



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

**Μελέτη, σχεδίαση και ανάπτυξη συστήματος ψηφιακής
υδατογράφησης εικόνων για την ασφαλή διαχείριση
ιατρικών δεδομένων**

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αγγελική Μ. Γιακουμάκη

Αθήνα, Οκτώβριος 2006



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Μελέτη, σχεδίαση και ανάπτυξη συστήματος ψηφιακής υδατογράφησης εικόνων για την ασφαλή διαχείριση ιατρικών δεδομένων

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αγγελική Μ. Γιακουμάκη

Συμβουλευτική Επιτροπή : Δημήτριος-Διονύσιος Κουτσούρης

Νικόλαος Κ. Ουζούνογλου

Κωνσταντίνα Σ. Νικήτα

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 16^η Οκτωβρίου 2006.

.....
Δ. Κουτσούρης
Καθηγητής Ε.Μ.Π.

.....
Ν. Ουζούνογλου
Καθηγητής Ε.Μ.Π.

.....
Κ. Νικήτα
Καθηγήτρια Ε.Μ.Π.

.....
Π. Τσανάκας
Καθηγητής Ε.Μ.Π.

.....
Σ. Κόλλιας
Καθηγητής Ε.Μ.Π.

.....
Γ. Στασινόπουλος
Καθηγητής Ε.Μ.Π.

.....
Μ. Ζερβάκης
Καθηγητής Πολυτεχνείου Κρήτης

Αθήνα, Οκτώβριος 2006

.....
Αγγελική Μ. Γιακουμάκη

Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Copyright © Αγγελική Μ. Γιακουμάκη, 2006.

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Στη μνήμη του πατέρα μου

Περίληψη

Το πεδίο έρευνας της παρούσας διατριβής είναι η αξιοποίηση της τεχνολογίας της ψηφιακής υδατογραφίας στον τομέα της ασφαλούς και αποδοτικής διαχείρισης της πληροφορίας σε συστήματα υπηρεσιών υγείας. Η ψηφιακή υδατογραφία αποτελεί ένα ερευνητικό πεδίο με ευρεία κλίμακα εφαρμογών και ειδικά τα τελευταία χρόνια αναδείχθηκε σε ένα πολύτιμο εργαλείο προστιθέμενης αξίας σε εφαρμογές ασφάλειας δεδομένων. Παρά τις λίγες προς το παρόν αναφορές στη βιβλιογραφία σχετικά με τη χρήση υδατογραφίας σε ιατρικές εφαρμογές, διαφαίνεται ήδη η αξία της συμβολής της σε πληθώρα ιατρικών εφαρμογών. Η ερευνητική εργασία επικεντρώνεται στη σχεδίαση και υλοποίηση ενός υδατογραφικού συστήματος, το οποίο στοχεύει στην επίλυση ποικίλων θεμάτων που αφορούν τα συστήματα διαχείρισης ιατρικής πληροφορίας. Συγκεκριμένα, το σύστημα εφαρμόζει πολλαπλή υδατογράφηση σε ιατρικές εικόνες, παρέχοντας εναλλακτικές ή/και συμπληρωματικές λύσεις για την προστασία του ιατρικού απορρήτου, τον έλεγχο πρόσβασης και ακεραιότητας των δεδομένων, την αποδοτική διαχείριση και ανάκτηση ιατρικής πληροφορίας, ικανοποιώντας παράλληλα την αυστηρή απαίτηση για διατήρηση της διαγνωστικής αξίας των ιατρικών εικόνων. Καθώς η υδατογραφία έχει την προοπτική να χρησιμοποιηθεί σε ιατρικές εφαρμογές με διαφορετικές και σε κάποιες περιπτώσεις αντιφατικές μεταξύ τους προδιαγραφές, η υλοποίηση ενός ενιαίου υδατογραφικού σχήματος που πληροί το σύνολο των προϋποθέσεων και στόχων, αποτελεί μια καινοτόμα προσέγγιση στην προσπάθεια αναβάθμισης της ασφάλειας και της διαχειριστικής ικανότητας των ιατρικών πληροφοριακών συστημάτων.

Abstract

The research field of this Ph.D thesis is the exploitation of digital watermarking technology in the field of secure and efficient information management in health data management systems. Digital watermarking is a research area with a wide range of applications, and has recently proved to be a value-added tool in data security. Despite the limited number of medical-oriented watermarking studies in the literature to date, digital watermarking has also the potential of being a valuable tool for a variety of medical applications. The Ph.D. thesis is mainly focused on the design and implementation of a watermarking system, which addresses a range of issues regarding medical data management systems. Specifically, the system applies multiple watermarking in medical images, in order to provide alternative and/or complementary solutions to medical confidentiality protection, data access and integrity control, and efficient health data management and retrieval, while satisfying the strict requirements concerning the preservation of the diagnostic value of medical images. Since digital watermarking has the potential to be applied in a number of medical applications having different and sometimes conflicting requirements, the design of a unified, multiple watermarking scheme that addresses the whole set of requirements and targets, is an innovative approach towards the enhancement of security and efficiency provided by health information management systems.

Ευχαριστίες

Η παρούσα διατριβή εκπονήθηκε στο Εργαστήριο Βιοϊατρικής Τεχνολογίας της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου και χρηματοδοτήθηκε από τη Γ.Γ.Ε.Τ. στα πλαίσια του Προγράμματος Ενίσχυσης Ερευνητικού Δυναμικού ΠΕΝΕΔ 2001.

Θα ήθελα καταρχάς να ευχαριστήσω θερμά τον Καθηγητή Ε.Μ.Π. Δημήτρη Κουτσούρη, επιβλέποντα της διατριβής μου, για την καθοδήγηση και τη συμπαράστασή του όλα αυτά τα χρόνια, καθώς και για την ευκαιρία που μου έδωσε να ασχοληθώ με το ιδιαίτερα ενδιαφέρον πεδίο της ασφαλούς διαχείρισης ιατρικών δεδομένων μέσω της αξιοποίησης νέων τεχνολογιών. Τον ευχαριστώ επίσης για το φιλικό κλίμα που δημιούργησε στο εργαστήριο, συμβάλλοντας στην αρμονική συνεργασία και δημιουργικότητα των μελών του.

Θερμές ευχαριστίες οφείλω στον Καθηγητή Ε.Μ.Π. Νικόλαο Ουζούνoglou και την Καθηγήτρια Ε.Μ.Π. Κωνσταντίνα Νικήτα, για τη συμμετοχή τους στην Τριμελή Συμβουλευτική Επιτροπή της διατριβής μου και τις χρήσιμες υποδείξεις και συμβουλές τους.

Θα ήθελα επίσης να ευχαριστήσω τον Καθηγητή Ε.Μ.Π. Παναγιώτη Τσανάκα, τον Καθηγητή Ε.Μ.Π. Στέφανο Κόλλια, τον Καθηγητή Ε.Μ.Π. Γεώργιο Στασινόπουλο και τον Καθηγητή Πολυτεχνείου Κρήτης Μιχάλη Ζερβάκη, για τη συμμετοχή τους στην Επταμελή Συμβουλευτική Επιτροπή της διατριβής μου.

Οφείλω να ευχαριστήσω τον Ερευνητή Β' ΕΠΙΣΕΥ Δρ. Σωτήρη Παυλόπουλο για την προτροπή του να διερευνήσω τις προοπτικές της ψηφιακής υδατογραφίας στη διαχείριση ιατρικών δεδομένων, για τις συμβουλές του και τη συνεργασία μας.

Θα ήθελα ακόμη να ευχαριστήσω όλους τους συναδέλφους και μέλη του εργαστηρίου για την άψογη συνεργασία και το φιλικό περιβάλλον στο οποίο συνέβαλαν, κάνοντας έτσι πιο εύκολη την πολύωρη παραμονή στο εργαστήριο σε περιόδους έντονου φόρτου εργασίας. Ιδιαίτερα θα ήθελα να ευχαριστήσω τον Κώστα Περάκη για τη στήριξη, τη συμπαράσταση και τη βοήθειά του. Ευχαριστώ θερμά τον Δρ. Τάσο Τάγαρη και την Ερευνήτρια Γ' ΕΠΙΣΕΥ Δρ. Ανδριάννα Πρέντζα, για τις πολύτιμες συμβουλές και τη φιλία τους όλα αυτά τα χρόνια. Ευχαριστώ επίσης τους Ελένη Σακκά, Ηλία Λαμπρινό, Γρηγόρη Βάσιο, Βιβή Νταλή, Κώστα Γκιόκα, Δήμητρα Ηλιοπούλου και Γιώργο Κόννη, για τη βοήθεια και τη συμπαράστασή τους. Θα ήθελα να ευχαριστήσω τρία παλαιότερα μέλη του εργαστηρίου, τον Μάριο Νεοφύτου, τη Δρ. Βάσω Γώγου και τη Δρ. Αθηνά Μπούρκα, που με βοήθησαν σημαντικά στα πρώτα μου βήματα στο εργαστήριο.

Ένα μεγάλο ευχαριστώ στη Δρ. Ειρήνη Καρανάσιου για τη φιλία, τη συμπαράσταση, τις συμβουλές και τη βοήθειά της.

Τέλος, ευχαριστώ ιδιαίτερα τη μητέρα και τον αδερφό μου για τη συμπαράστασή τους όλα αυτά τα χρόνια. Οφείλω ένα μεγάλο ευχαριστώ στον πατέρα μου, που αν και δεν πρόλαβε να δει την ολοκλήρωση αυτής μου της προσπάθειας, η στήριξη και η ενθάρρυνσή του στα πρώτα μου βήματα είναι σημείο αναφοράς για μένα όλο αυτό το διάστημα και πηγή δύναμης και έμπνευσης στα δύσκολα.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κεφάλαιο 1.....	21
ΕΙΣΑΓΩΓΗ.....	21
1.1 Γενικά.....	21
1.2 Κίνητρο και Συνεισφορά της Διδακτορικής Διατριβής.....	22
1.3 Δομή της Διδακτορικής Διατριβής	25
Βιβλιογραφικές Αναφορές.....	28
Κεφάλαιο 2.....	33
ΨΗΦΙΑΚΗ ΥΔΑΤΟΓΡΑΦΙΑ	33
2.1 Τεχνικές Απόκρυψης Δεδομένων (Data Hiding)	33
2.2 Εφαρμογές Ψηφιακής Υδατογραφίας	39
2.2.1 Προστασία Πνευματικών Δικαιωμάτων	40
2.2.2 Ανίχνευση Συναλλαγών (Fingerprinting).....	41
2.2.3 Δεικτοδότηση (Indexing).....	42
2.2.4 Επισημάνση Χαρακτηριστικών (Feature Tagging)	43
2.2.5 Μυστική Επικοινωνία (Data Hiding).....	44
2.2.6 Παρακολούθηση Μετάδοσης (Broadcast Monitoring)	44
2.2.7 Έλεγχος Αντιγράφων (Copy Control)	45
2.2.8 Πιστοποίηση Δεδομένων (Data Authentication)	47
2.3 Χαρακτηριστικά Υδατογραφήματων	49
2.3.1 Ανθεκτικότητα (Robustness).....	49
2.3.2 Χωρητικότητα (Capacity).....	50
2.3.3 Διαφάνεια (Perceptual Transparency)	51
2.3.4 Αποτελεσματικότητα Ενσωμάτωσης (Embedding Effectiveness)	52
2.3.5 «Ενημερωμένη» και «Τυφλή Ανίχνευση» (Informed and Blind Detection)	52
2.3.6 Ρυθμός Ψευδώς Θετικών (False Positive Rate)	54
2.3.7 Ασφάλεια	55
2.3.8 Υδατογραφικά Κλειδιά.....	56
2.3.9 Τροποποίηση Υδατογραφήματος και Πολλαπλά Υδατογραφήματα.....	59
2.4 Ταξινόμηση Τεχνικών Υδατογραφίας	60
2.5 Βιβλιογραφική Ανασκόπηση	69
Βιβλιογραφικές Αναφορές.....	75
Κεφάλαιο 3.....	81
ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΙΑΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	81
3.1 Εισαγωγή	81
3.2 Περιγραφή Νομικού Πλαισίου	82
3.2.1 Κανονισμοί σε Διεθνές Επίπεδο	82
3.2.2 Ευρωπαϊκή Νομοθεσία.....	86
3.2.2.1 Ιδιοκτησιακό καθεστώς.....	86
3.2.2.2 Διατάξεις και γνωμοδοτήσεις σε ευρωπαϊκό επίπεδο.....	87
3.2.3 Ελληνική Νομοθεσία	89
3.3 Βασικές Απαιτήσεις Ασφάλειας.....	90
3.4 Υπηρεσίες Ασφάλειας.....	92
3.4.1 Υπηρεσίες Ασφάλειας Ιατρικών Βάσεων Δεδομένων.....	92
3.4.2 Υπηρεσίες Ασφάλειας κατά τη Μετάδοση Ιατρικών Εικόνων	94
3.5 Ανασκόπηση Τεχνικών Μέτρων Ασφάλειας	96
3.6 Περιορισμοί Υφιστάμενων Μέτρων Ασφάλειας	99
Βιβλιογραφικές Αναφορές.....	101
Κεφάλαιο 4.....	105

ΠΡΟΟΠΤΙΚΕΣ ΨΗΦΙΑΚΗΣ ΥΔΑΤΟΓΡΑΦΙΑΣ ΣΤΗ ΔΙΑΧΕΙΡΙΣΗ ΙΑΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	105
4.1 Ιατρικές Εφαρμογές της Ψηφιακής Υδατογραφίας	105
4.2 Βιβλιογραφική Έρευνα	112
Βιβλιογραφικές Αναφορές	117
Κεφάλαιο 5	123
ΑΝΑΛΥΣΗ ΑΠΑΙΤΗΣΕΩΝ ΧΡΗΣΤΩΝ	123
5.1 Εισαγωγή	123
5.2 Απαιτήσεις Χρηστών	124
5.3 Τεχνικές Απαιτήσεις των Εφαρμογών	126
5.3.1 Λειτουργικές Απαιτήσεις	126
5.3.2 Μη Λειτουργικές Απαιτήσεις	132
5.3.2.1 Απαιτούμενη ανθεκτικότητα των πολλαπλών υδατογραφημάτων	132
5.3.2.2 Απαιτούμενη χωρητικότητα των πολλαπλών υδατογραφημάτων	132
5.3.2.3 Αλληλεπίδραση με το χρήστη	133
5.3.3 Εργαλεία Ανάπτυξης των Εφαρμογών	135
5.4 Προσδιορισμός Περιοχών Εφαρμογής του Υδατογραφικού Συστήματος	135
5.4.1 Εφαρμογές e-Health	137
5.4.2 Διαχείριση Ιατρικών Δεδομένων σε Πληροφοριακά Συστήματα Νοσοκομείων	140
Βιβλιογραφικές Αναφορές	143
Κεφάλαιο 6	145
ΠΕΡΙΓΡΑΦΗ ΥΔΑΤΟΓΡΑΦΙΚΟΥ ΣΧΗΜΑΤΟΣ	145
6.1 Εισαγωγή	145
6.2 Χαρακτηριστικά Πεδίου Μετασχηματισμού Κυματιδίων	146
6.3 Σύνοψη Προτεινόμενης Μεθόδου	151
6.4 Περιγραφή Αλγορίθμου	154
6.5 Επιλογή Συντελεστών για Υδατογράφιση	157
Βιβλιογραφικές Αναφορές	165
Κεφάλαιο 7	167
ΑΠΟΤΙΜΗΣΗ ΥΔΑΤΟΓΡΑΦΙΚΟΥ ΣΧΗΜΑΤΟΣ	167
7.1 Εισαγωγή	167
7.2 Δοκιμές του Υδατογραφικού Σχήματος	168
7.2.1 Δοκιμές σε Εικόνες Υπερήχων	169
7.2.2 Δοκιμές σε Εικόνες Αξονικής Τομογραφίας (CT)	178
7.2.3 Δοκιμές σε Εικόνες Μαγνητικής Τομογραφίας (MRI)	184
7.2.4 Δοκιμές σε Εικόνες Μαγνητικής Αγγειογραφίας (MRA)	188
7.2.5 Δοκιμές σε Εικόνες Τομογραφίας Εκπομπής Ποζιτρονίου (PET)	192
7.2.6 Εναλλακτικά Σχήματα Εφαρμογής Αλγορίθμου	195
7.2.6.1 Ενσωμάτωση τριών τύπων υδατογραφημάτων χωρίς επιλογή Περιοχής Ενδιαφέροντος	196
7.2.6.2 Ενσωμάτωση τεσσάρων τύπων υδατογραφημάτων χωρίς επιλογή Περιοχής Ενδιαφέροντος	200
7.2.6.3 Ενσωμάτωση τεσσάρων τύπων υδατογραφημάτων με επιλογή Περιοχής Ενδιαφέροντος	203
Βιβλιογραφικές Αναφορές	208
Κεφάλαιο 8	211
ΓΡΑΦΙΚΗ ΔΙΑΠΡΟΣΩΠΕΙΑ ΤΗΣ ΕΦΑΡΜΟΓΗΣ	211
8.1 Εισαγωγή	211
8.2 Γραφική Διαπροσωπεία Εισαγωγής και Εξαγωγής Υδατογραφημάτων	211
8.2.1 Φόρμα Καθορισμού Επιλογών	213

8.2.2	Φόρμα Εισαγωγής Υδατογραφημάτων.....	214
8.2.3	Φόρμα Εξαγωγής Υδατογραφημάτων	218
	Βιβλιογραφικές Αναφορές.....	220
Κεφάλαιο 9.....		221
	ΣΥΜΠΕΡΑΣΜΑΤΑ – ΣΥΖΗΤΗΣΗ - ΠΡΟΟΠΤΙΚΕΣ	221
9.1	Εισαγωγή	221
9.2	Σύνοψη Ερευνητικής Εργασίας	221
9.3	Αξιολόγηση Συστήματος – Καινοτομία και Συνεισφορά	225
9.4	Μελλοντικές Επεκτάσεις και Προοπτικές	228
	Βιβλιογραφικές Αναφορές.....	232
Κατάλογος Δημοσιεύσεων		237

ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ

Σχήμα 1: Ταξινόμηση τεχνικών απόκρυψης δεδομένων.....	38
Σχήμα 2: Γενικό μοντέλο ψηφιακής υδατογραφίας	61
Σχήμα 3: Ενσωμάτωση υπηρεσίας ψηφιακής υδατογραφίας σε σύστημα τηλεϊατρικής	137
Σχήμα 4: Χρήση υπηρεσίας ψηφιακής υδατογραφίας σε εφαρμογή e-Health.....	138
Σχήμα 5: Χρήση υπηρεσίας ψηφιακής υδατογραφίας στο τοπικό δίκτυο νοσοκομείου	141
Σχήμα 6: Ανάλυση εικόνας υπερήχων με εφαρμογή ΔΜΚ σε 2 επίπεδα.....	149
Σχήμα 7: Διαδικασία εισαγωγής πολλαπλών υδατογραφημάτων	152
Σχήμα 8: Διαδικασία εξαγωγής πολλαπλών υδατογραφημάτων	153
Σχήμα 9: Διαδικασία κβαντοποίησης	156
Σχήμα 10: Πολυδιακριτή ανάλυση εικόνας με εφαρμογή μετασχηματισμού κυματιδίων. (α) Πυραμιδική δομή ΔΜΚ 4 επιπέδων. (β) ΔΜΚ 4 επιπέδων σε εικόνα υπερήχων.....	159
Σχήμα 11: Εικόνα αξονικής τομογραφίας (CT)	160
Σχήμα 12: Αντιστοιχία των Πινάκων Περιοχής Ενδιαφέροντος ανά υποζώνη και επίπεδο ανάλυσης.....	164
Σχήμα 13: (α) Αρχική εικόνα υπερήχων με καθορισμένη Περιοχή Ενδιαφέροντος. (β) Προκύπτουσα υδατογραφημένη εικόνα.	172
Σχήμα 14: (α) Εικόνα υπερήχων με θολωμένη περιοχή. (β) Ανίχνευση αλλοίωσης μέσω της εικόνας διαφορών του υδατογραφήματος αναφοράς 1ου επιπέδου ανάλυσης	177
Σχήμα 15: Αντιστοιχία των Πινάκων Περιοχής Ενδιαφέροντος ανά υποζώνη και επίπεδο ανάλυσης εικόνας CT	179
Σχήμα 16: (α) Αρχική εικόνα CT με καθορισμένη Περιοχή Ενδιαφέροντος. (β) Προκύπτουσα υδατογραφημένη εικόνα	181
Σχήμα 17: (α) Αρχική εικόνα MRI με καθορισμένη Περιοχή Ενδιαφέροντος. (β) Προκύπτουσα υδατογραφημένη εικόνα	185
Σχήμα 18: Αντιστοιχία των Πινάκων Περιοχής Ενδιαφέροντος ανά υποζώνη και επίπεδο ανάλυσης εικόνας MRA.....	188
Σχήμα 19: (α) Αρχική εικόνα MRA με καθορισμένη Περιοχή Ενδιαφέροντος. (β) Προκύπτουσα υδατογραφημένη εικόνα	189
Σχήμα 20: (α) Αρχική εικόνα PET με καθορισμένη Περιοχή Ενδιαφέροντος. (β) Προκύπτουσα υδατογραφημένη εικόνα	193
Σχήμα 21: (α) Αρχική εικόνα υπερήχων. (β) Αντίστοιχη υδατογραφημένη εικόνα. .	199
Σχήμα 22: (α) Αρχική εικόνα υπερήχων. (β) Αντίστοιχη υδατογραφημένη εικόνα. .	202
Σχήμα 23: (α) Αρχική εικόνα υπερήχων. (β) Αντίστοιχη υδατογραφημένη εικόνα. .	202
Σχήμα 24: (α) Αρχική εικόνα υπερήχων με Περιοχή Ενδιαφέροντος. (β) Αντίστοιχη υδατογραφημένη εικόνα.	206
Σχήμα 25: Φόρμα καθορισμού επιλογών.....	213
Σχήμα 26: Φόρμα εισαγωγής υδατογραφημάτων	215
Σχήμα 27: Εισαγωγή δεδομένων για το υδατογράφημα υπογραφής από αρχείο κειμένου	216

Σχήμα 28: Εισαγωγή δεδομένων για το υδατογράφημα υπογραφής από το χρήστη	216
Σχήμα 29: Επιλογή δεδομένων για το υδατογράφημα δείκτη από τη λίστα ICD9/10	217
Σχήμα 30: Εισαγωγή δεδομένων για το υδατογράφημα επικεφαλίδας από το χρήστη	218
Σχήμα 31: Φόρμα εξαγωγής υδατογραφημάτων	219

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

Πίνακας 1: Μηχανισμοί παροχής υπηρεσιών ασφάλειας.....	99
Πίνακας 2: Ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών Διακριτού Μετασχηματισμού Κυματιδίων 4 επιπέδων εικόνας CT	159
Πίνακας 3: Κατανομή πολλαπλών υδατογραφημάτων στις υποζώνες βάσει απαιτήσεων ανθεκτικότητας και χωρητικότητας	163
Πίνακας 4: Σχήματα κωδικοποίησης BCH ανά υδατογράφημα.....	170
Πίνακας 5: Ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών Διακριτού Μετασχηματισμού Κυματιδίων 4 επιπέδων εικόνας υπερήχων	171
Πίνακας 6: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων υπερήχων ως προς το PNSR.....	174
Πίνακας 7: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων υπερήχων ως προς το wPNSR	174
Πίνακας 8: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες υπερήχων).....	175
Πίνακας 9: Ποσοστό εσφαλμένων bits σε υδατογραφήματα εξαχθέντα από εικόνες υπερήχων (%)	176
Πίνακας 10: Κατανομή πολλαπλών υδατογραφημάτων στις υποζώνες βάσει απαιτήσεων ανθεκτικότητας και χωρητικότητας	181
Πίνακας 11: Ποσοστό εσφαλμένων bits σε υδατογραφήματα εξαχθέντα από εικόνες CT (%).....	183
Πίνακας 12: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες CT)	183
Πίνακας 13: Ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών Διακριτού Μετασχηματισμού Κυματιδίων 4 επιπέδων εικόνας MRI.....	185
Πίνακας 14: Ποσοστό εσφαλμένων bits σε υδατογραφήματα εξαχθέντα από εικόνες MRI (%)	186
Πίνακας 15: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες MRI).....	187
Πίνακας 16: Ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών Διακριτού Μετασχηματισμού Κυματιδίων 4 επιπέδων εικόνας MRA	189
Πίνακας 17: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων MRA ως προς το PNSR.....	190
Πίνακας 18: Ποσοστό εσφαλμένων bits σε υδατογραφήματα εξαχθέντα από εικόνες MRA (%).....	191
Πίνακας 19: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες MRA).....	192
Πίνακας 20: Ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών Διακριτού Μετασχηματισμού Κυματιδίων 4 επιπέδων εικόνας PET	193
Πίνακας 21: Ποσοστό εσφαλμένων bits σε υδατογραφήματα εξαχθέντα από εικόνες PET (%).....	194
Πίνακας 22: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες PET)	195
Πίνακας 23: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων υπερήχων ως προς το PNSR.....	200

Πίνακας 24: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων υπερήχων ως προς το PNSR	203
Πίνακας 25: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων υπερήχων ως προς το PNSR	206
Πίνακας 26: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες υπερήχων)	207
Πίνακας 27: Συγκεντρωτικός πίνακας διαθέσιμων τύπων υδατογραφημάτων, της πληροφορίας που φέρουν και του ρόλου που εξυπηρετούν.....	224

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

1.1 ΓΕΝΙΚΑ

Τα τελευταία χρόνια παρατηρείται αλματώδης ανάπτυξη των πληροφοριακών συστημάτων και ευρεία χρήση του διαδικτύου σε πληθώρα εφαρμογών. Η υιοθέτηση και προσαρμογή των νέων τεχνολογιών σε ιατρικές εφαρμογές προσφέρει νέες δυνατότητες στη διαχείριση και μετάδοση των ιατρικών δεδομένων, βελτιώνοντας σημαντικά την ποιότητα της παρεχόμενης ιατρικής περίθαλψης. Τα νοσοκομειακά πληροφοριακά συστήματα (Hospital Information Systems - HIS) και τα συστήματα αρχειοθέτησης και μετάδοσης εικόνας (Picture Archiving and Communication Systems - PACS) αποτελούν βασικά δομικά συστατικά των σύγχρονων ολοκληρωμένων συστημάτων παροχής ιατρικής περίθαλψης, παρέχοντας εύκολη πρόσβαση, διαχείριση και μετάδοση των ψηφιακών ιατρικών δεδομένων. Το διαδίκτυο χρησιμοποιείται πλέον ευρέως για την πρόσβαση ηλεκτρονικών ιατρικών φακέλων κατανεμημένων σε διάφορους διακομιστές (servers). Η ευκολία στην πρόσβαση, διαχείριση και μετάδοση πληροφορίας, αποτέλεσμα των ραγδαίων τεχνολογικών εξελίξεων, καθιστά κρίσιμης σημασίας το ζήτημα της ασφάλειας. Ειδικά στις ιατρικές εφαρμογές, η ευαίσθητη φύση των προσωπικών δεδομένων των ασθενών επιβάλλει την προστασία τους από μη εξουσιοδοτημένη πρόσβαση και τη διασφάλιση του ιατρικού απορρήτου. Σε αυτό το πλαίσιο καθίσταται αναγκαία η λήψη πρόσθετων μέτρων προκειμένου να αντιμετωπιστούν οι αυξημένοι κίνδυνοι για την ασφάλεια. Απαιτείται επιπλέον

πιστοποίηση της πηγής προέλευσης, δηλαδή πιστοποίηση της ταυτότητας του γιατρού που διενεργεί την εξέταση και ελέγχει τα αποτελέσματα. Ζήτημα μείζονος σημασίας αποτελεί επίσης η προστασία της ακεραιότητας των ιατρικών δεδομένων, καθώς η τυχαία ή αθέμιτη αλλοίωσή τους ενδέχεται να οδηγήσει σε λανθασμένη διάγνωση και θεραπευτική αγωγή.

Υπάρχουν διάφορες μέθοδοι ασφαλείας που εφαρμόζονται στα σύγχρονα ιατρικά πληροφοριακά συστήματα για την προστασία των δεδομένων από μη εξουσιοδοτημένους χρήστες. Οι τεχνικές κρυπτογραφίας και η χρήση ψηφιακών υπογραφών, κωδικών πρόσβασης και έξυπνων καρτών αποτελούν κάποιες διαδεδομένες πρακτικές για την πιστοποίηση των εξουσιοδοτημένων χρηστών. Ωστόσο, για το κρίσιμο θέμα της ασφάλειας στα συστήματα διαχείρισης ιατρικής πληροφορίας αναζητούνται συνεχώς νέες αποτελεσματικές τεχνικές λύσεις, που θα συμπληρώσουν τις υπάρχουσες και θα προσφέρουν ένα πρόσθετο επίπεδο προστασίας, σύμφωνα και με τα νομικά μέτρα που έχουν θεσπιστεί σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο.

1.2 ΚΙΝΗΤΡΟ ΚΑΙ ΣΥΝΕΙΣΦΟΡΑ ΤΗΣ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

Η ψηφιακή υδατογραφία αποτελεί ένα σχετικά καινούριο ερευνητικό πεδίο που επικεντρώθηκε αρχικά στην κατοχύρωση των πνευματικών δικαιωμάτων των δημιουργών. Σύντομα όμως διαπιστώθηκε η δυνατότητα αξιοποίησης της συγκεκριμένης τεχνολογίας σε μια ευρεία κλίμακα εφαρμογών και ειδικά τα τελευταία χρόνια αναδείχθηκε σε ένα πολύτιμο εργαλείο προστιθέμενης αξίας σε εφαρμογές ασφάλειας δεδομένων. Παρά τις λίγες προς το παρόν αναφορές στη βιβλιογραφία σχετικά με τη χρήση υδατογραφίας σε ιατρικές εφαρμογές, διαφαίνεται ήδη η αξία της συμβολής της σε πληθώρα ιατρικών εφαρμογών λόγω της δυνατότητάς της να προσφέρει αυξημένη ασφάλεια και αποδοτικότερη διαχείριση κρίσιμης ιατρικής πληροφορίας [1]-[17]. Αξίζει να σημειωθεί ότι την τελευταία πενταετία εμπλουτίζεται συνεχώς η σχετική αρθρογραφία, γεγονός που φανερώνει τη δυναμική της ψηφιακής υδατογραφίας στον τομέα της ιατρικής πληροφορικής.

Η ψηφιακή υδατογράφηση είναι η ενσωμάτωση πρόσθετης πληροφορίας απευθείας στα δεδομένα, μέσω ανεπαίσθητης τροποποίησης είτε της αρχικής τους μορφής είτε κάποιας μετασχηματισμένης εκδοχής τους. Υπάρχουν διάφοροι τύποι υδατογραφημάτων, τα πεδία εφαρμογής των οποίων καθορίζονται από το βαθμό στον οποίο ικανοποιούν τις παραμέτρους της διαφάνειας, της ανθεκτικότητας και της χωρητικότητας [18]. Τα ανθεκτικά υδατογραφήματα σχεδιάζονται έτσι ώστε να μην αλλοιώνονται από τις συνηθισμένες τεχνικές επεξεργασίας, αλλά ούτε και από κακόβουλες επιθέσεις, γεγονός που τα καθιστά κατάλληλα για εφαρμογές κατοχύρωσης πνευματικής ιδιοκτησίας και πιστοποίησης ταυτότητας. Η ποσότητα της πληροφορίας που μπορεί να ενσωματωθεί στα αρχικά δεδομένα, η λεγόμενη χωρητικότητα, δεν αποτελεί βασική απαίτηση για τη συγκεκριμένη κατηγορία υδατογραφημάτων, καθώς το μήκος του αναγνωριστικού κώδικα περιορίζεται συνήθως στο ελάχιστο που χρειάζεται για την εξασφάλιση της μοναδικότητάς του. Αντιθέτως, για ένα υδατογράφημα που προορίζεται για εμπλουτισμό των αρχικών δεδομένων με πρόσθετη βοηθητική πληροφορία, πρέπει οπωσδήποτε να εξασφαλίζεται επαρκής χωρητικότητα, χωρίς όμως να αγνοείται η ανθεκτικότητα. Τα εύθραυστα υδατογραφήματα αλλοιώνονται από τροποποιήσεις στα αρχικά δεδομένα και επομένως μπορούν να χρησιμοποιηθούν για έλεγχο της ακεραιότητας δεδομένων και εντοπισμό των παραποιημένων τμημάτων. Λόγω του ότι διαφορετικοί τύποι υδατογραφημάτων χαρακτηρίζονται από διαφορετικό βαθμό ανθεκτικότητας, διαφάνειας και χωρητικότητας, ένα μόνο υδατογράφημα δεν μπορεί να καλύψει τις απαιτήσεις όλων των εφαρμογών και χρειάζεται αντιστάθμιση (trade-off) των παραπάνω παραμέτρων ανάλογα με την εφαρμογή. Η ενιαία προσέγγιση ποικίλων εφαρμογών απαιτεί την υιοθέτηση ενός σχήματος υδατογραφίας που να επιτρέπει την ταυτόχρονη ενσωμάτωση πολλαπλών υδατογραφημάτων, καθένα από τα οποία ικανοποιεί διαφορετικές απαιτήσεις, διαθέτει διαφορετικά χαρακτηριστικά και μπορεί να εισαχθεί και να εξαχθεί ανεξάρτητα από τα υπόλοιπα. Η βιβλιογραφία σχετικά με την ταυτόχρονη ενσωμάτωση πολλαπλών υδατογραφημάτων για διαφορετικούς σκοπούς παραμένει περιορισμένη μέχρι τώρα [19]-[25].

Στα πλαίσια της παρούσας διδακτορικής διατριβής διερευνήθηκαν οι τρόποι με τους οποίους μπορεί η υδατογραφία να συμβάλει στην υλοποίηση ενός ασφαλούς συστήματος διαχείρισης ιατρικών δεδομένων, με βάση το αυστηρό πλαίσιο που ορίζεται από τους νομικούς κανόνες στον τομέα της υγείας. Οι ιατρικές εφαρμογές της ψηφιακής υδατογραφίας περιλαμβάνουν μεταξύ άλλων την προστασία του ιατρικού απορρήτου, τον έλεγχο της ακεραιότητας των κρίσιμων ιατρικών δεδομένων, την πιστοποίηση της πηγής προέλευσης και την αποδοτικότερη διαχείριση της ιατρικής πληροφορίας. Παρακάτω θα γίνει αναλυτική παρουσίαση του συνόλου των πιθανών ιατρικών εφαρμογών της υδατογραφίας, οι οποίες μπορούν να συντελέσουν στην ουσιαστική αναβάθμιση της ποιότητας της παρεχόμενης ιατρικής περίθαλψης.

Η υδατογραφία έχει διεισδύσει τα τελευταία χρόνια σε μια ευρεία κλίμακα εφαρμογών, λόγω των ποικίλων δυνατοτήτων που προσφέρει. Οι απαιτήσεις και τα χαρακτηριστικά των εφαρμογών αυτών διαφέρουν σε μεγάλο βαθμό και συχνά έρχονται σε αντίθεση μεταξύ τους, γεγονός που οδηγεί στην υιοθέτηση υδατογραφικών τεχνικών προσαρμοσμένων στην εκάστοτε περίπτωση. Για κάθε εφαρμογή αναζητείται η τεχνική εκείνη που ικανοποιεί τις ιδιαίτερες απαιτήσεις της, καθώς δεν υπάρχει μια μέθοδος υδατογραφίας που να συνδυάζει ταυτόχρονα τα διάφορα αντιφατικά χαρακτηριστικά που απαιτούνται από το σύνολο των εφαρμογών. Στα πλαίσια της διδακτορικής διατριβής σχεδιάστηκε και αναπτύχθηκε ένα σύστημα πολλαπλής υδατογράφησης ιατρικών εικόνων που ανταποκρίνεται στις ανάγκες και απαιτήσεις των ιατρικών εφαρμογών που ανέκυψαν τα τελευταία χρόνια, ως αποτέλεσμα της τεχνολογικής προόδου και των νέων δυνατοτήτων που παρουσιάζονται στον τομέα της υγείας. Το σύστημα αυτό αξιοποιεί τα πλεονεκτήματα της ψηφιακής υδατογραφίας, επιδιώκοντας την παροχή συμπληρωματικών λύσεων ασφάλειας και υπηρεσιών προστιθέμενης αξίας σε ιατρικά πληροφοριακά συστήματα. Καθώς η υδατογραφία έχει την προοπτική να χρησιμοποιηθεί σε ιατρικές εφαρμογές με διαφορετικές και σε κάποιες περιπτώσεις αντιφατικές μεταξύ τους προδιαγραφές, η υλοποίηση ενός ενιαίου υδατογραφικού σχήματος που πληροί το σύνολο των προϋποθέσεων και στόχων, αποτελεί μια καινοτόμα προσέγγιση στην προσπάθεια αναβάθμισης της ασφάλειας και της

διαχειριστικής ικανότητας των ιατρικών πληροφοριακών συστημάτων. Η συνεισφορά της παρούσας διδακτορικής διατριβής στον τομέα της ασφαλούς και αποδοτικής διαχείρισης ιατρικής πληροφορίας μέσω της καινοτομικής σχεδίασης και εφαρμογής ενός συστήματος πολλαπλής υδατογράφησης ιατρικών εικόνων, πιστοποιείται από μια σειρά δημοσιεύσεων σε περιοδικά και πρακτικά συνεδρίων [26]-[38], καθώς και από αναφορές στις δημοσιεύσεις αυτές σε πρόσφατα άρθρα άλλων ερευνητών [39]-[46].

1.3 ΔΟΜΗ ΤΗΣ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

Το γενικότερο πεδίο ενδιαφέροντος της διατριβής είναι η διερεύνηση των προοπτικών της ψηφιακής υδατογραφίας στον τομέα της ασφαλούς και αποδοτικής διαχείρισης της πληροφορίας σε συστήματα υπηρεσιών υγείας. Η ερευνητική εργασία επικεντρώνεται στη σχεδίαση και υλοποίηση ενός υδατογραφικού συστήματος, το οποίο στοχεύει στην επίλυση ποικίλων θεμάτων που αφορούν τα συστήματα διαχείρισης ιατρικής πληροφορίας. Συγκεκριμένα, το σύστημα εφαρμόζει πολλαπλή υδατογράφηση σε ιατρικές εικόνες, παρέχοντας εναλλακτικές ή / και συμπληρωματικές λύσεις για την προστασία του ιατρικού απορρήτου, τον έλεγχο πρόσβασης και ακεραιότητας των δεδομένων, την αποδοτική διαχείριση και ανάκτηση ιατρικής πληροφορίας, ικανοποιώντας παράλληλα την αυστηρή απαίτηση για διατήρηση της διαγνωστικής αξίας των ιατρικών εικόνων. Η ανάλυση της σχεδίασης, ανάπτυξης και αξιολόγησης του συστήματος πολλαπλής υδατογράφησης ιατρικών εικόνων, που αποτελεί το θέμα της παρούσας διατριβής, ολοκληρώνεται σε εννέα κεφάλαια.

Στο **Κεφάλαιο 2** παρουσιάζονται αναλυτικά η έννοια και οι εφαρμογές της ψηφιακής υδατογραφίας. Περιγράφονται τα χαρακτηριστικά των υδατογραφημάτων και στη συνέχεια γίνεται ταξινόμηση των τεχνικών υδατογραφίας που έχουν προταθεί στη βιβλιογραφία. Τέλος, παρατίθεται η ανασκόπηση της σχετικής βιβλιογραφίας μέσω της παρουσίασης βασικών και αντιπροσωπευτικών σχημάτων.

Στο **Κεφάλαιο 3** περιγράφονται οι βασικές απαιτήσεις ασφάλειας ως προς τη διαχείριση της παραγόμενης και διακινούμενης πληροφορίας σε συστήματα

υπηρεσιών υγείας και παρουσιάζονται σχετικές οδηγίες και πρότυπα που αφορούν τη διαχείριση και αποθήκευση των ιατρικών δεδομένων. Γίνεται επίσης αναφορά στα κύρια μέτρα αντιμετώπισης των προβλημάτων και απειλών σε πληροφοριακά συστήματα υγείας, καθώς και στους περιορισμούς που διέπουν τις παρούσες τεχνολογίες και οδηγούν στην ανάγκη εύρεσης συμπληρωματικών λύσεων ασφάλειας.

Στο **Κεφάλαιο 4** παρουσιάζονται οι προοπτικές της ψηφιακής υδατογραφίας στη διαχείριση πληροφορίας σε συστήματα υπηρεσιών υγείας. Παρατίθενται επίσης τα αποτελέσματα της βιβλιογραφικής έρευνας σχετικά με τις προσπάθειες που έχουν γίνει προς την κατεύθυνση της αξιοποίησης της ψηφιακής υδατογραφίας στο χώρο της υγείας, οι οποίες λόγω της καινοτομίας του θέματος είναι προς το παρόν περιορισμένες.

Στο **Κεφάλαιο 5** αναλύονται οι απαιτήσεις των χρηστών ως προς τις προδιαγραφές στις οποίες καλείται να ανταποκριθεί ένα λειτουργικό υδατογραφικό σύστημα που προορίζεται για ιατρικές εφαρμογές. Παρουσιάζονται οι απαιτήσεις των χρηστών και τα απαιτούμενα λειτουργικά χαρακτηριστικά του συστήματος και στη συνέχεια δίνονται τα προβλεπόμενα σενάρια χρήσης του. Τέλος, περιγράφονται κάποιες περιπτώσεις εφαρμογής του υδατογραφικού συστήματος και δίνονται πληροφορίες ως προς την ολοκλήρωση ενός τέτοιου συστήματος στα πλαίσια των προτεινόμενων εφαρμογών.

Στο **Κεφάλαιο 6** περιγράφεται το υδατογραφικό σχήμα που σχεδιάστηκε και υλοποιήθηκε στα πλαίσια της διατριβής, με βάση τις προδιαγραφές που προέκυψαν από την ανάλυση απαιτήσεων των χρηστών. Παρατίθενται κάποια στοιχεία σχετικά με το πεδίο μετασχηματισμού που επιλέχθηκε για την ανάπτυξη του αλγορίθμου και δίνεται αναλυτική περιγραφή του υδατογραφικού σχήματος που αναπτύχθηκε για την εισαγωγή και εξαγωγή των πολλαπλών υδατογραφημάτων. Τέλος, εξηγείται διεξοδικά η διαδικασία επιλογής των συντελεστών μετασχηματισμού που κρίθηκαν κατάλληλοι για υδατογράφιση.

Στο **Κεφάλαιο 7** παρουσιάζονται τα αποτελέσματα των δοκιμών που έγιναν στον υδατογραφικό αλγόριθμο προκειμένου να αξιολογηθεί η αποδοτικότητά του. Γίνεται αναλυτική παρουσίαση των δοκιμών που έγιναν σε διαφορετικά είδη

ιατρικών εικόνων, συγκεκριμένα σε εικόνες υπερήχων (ultrasound), αξονικής τομογραφίας (CT), μαγνητικής τομογραφίας (MRI), μαγνητικής αγγειογραφίας (MRA) και τομογραφίας εκπομπής ποζιτρονίου (PET). Επίσης παρατίθενται τα αποτελέσματα των δοκιμών που έγιναν σε διαφορετικά σενάρια εφαρμογής του σχήματος, που περιλάμβαναν καθορισμό ή μη μιας Περιοχής Ενδιαφέροντος και χρήση κώδικα διόρθωσης σφαλμάτων για αύξηση της ανθεκτικότητας των υδατογραφημάτων. Τα αποτελέσματα περιλαμβάνουν αξιολόγηση της αλλοίωσης που προκαλείται στις εικόνες – με έμφαση στις διαγνωστικά σημαντικές περιοχές – λόγω υδατογράφησης και αποτίμηση της ανθεκτικότητας των υδατογραφημάτων και της ικανότητας του σχήματος να ελέγξει την ακεραιότητα των εικόνων.

Το **Κεφάλαιο 8** παρουσιάζει τις γραφικές διαπροσωπείες που αποτυπώνουν τη λειτουργικότητα του υδατογραφικού συστήματος που αναπτύχθηκε στα πλαίσια της διατριβής. Συγκεκριμένα παρουσιάζονται οι γραφικές διαπροσωπείες που παρέχουν τη δυνατότητα εισαγωγής και εξαγωγής πολλαπλών υδατογραφημάτων από ιατρικές εικόνες και περιγράφονται οι επιλογές που προσφέρονται στο χρήστη του συστήματος.

Στο **Κεφάλαιο 9** ολοκληρώνεται η διδακτορική διατριβή με την παράθεση των συμπερασμάτων που προκύπτουν από την αξιολόγηση του συστήματος. Παρουσιάζονται επίσης τα ανοιχτά θέματα και οι προτάσεις για μελλοντικές επεκτάσεις και βελτιώσεις του.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

- [1] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, "Relevance of watermarking in medical imaging," in *Proc. 3rd Conf. Information Technology Applications in Biomedicine, ITAB'00*, Arlington, USA, pp. 250-255.
- [2] A. Wakatani, "Digital watermarking for ROI medical images by using compressed signature image," presented at the 35th Annu. Hawaii Intern. Conf. System Sciences, HICSS'02, Big Island, HI, USA.
- [3] G. Coatrieux, H. Maitre, B. Sankur, "Strict integrity control of biomedical images," in *Proc. SPIE Security and Watermarking of Multimedia Contents III, SPIE2001*, San Jose, USA, vol. 4314, pp. 229-240, Jan. 2001.
- [4] H. M. Chao, C. M. Hsu, S. G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Trans. Inf. Technol. Biomed.*, vol. 6, no. 1, pp. 46-53, March 2002.
- [5] S. G. Miaou, C. M. Hsu, Y. S. Tsai, H. M. Chao, "A secure data hiding technique with heterogeneous data combining capability for electronic patient records," in *Proc. 22nd Annu. Intern. Conf. IEEE Engineering in Medicine and Biology Society, EMBS'00*, Chicago, USA, vol. 1, pp. 280-283.
- [6] U. Rajendra Acharya, D. Anand, P. Subbanna Bhat, U.C. Niranjan, "Compact storage of medical images with patient information," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 4, pp. 320-323, Dec. 2001.
- [7] R. U. Acharya, P. S. Bhat, S. Kumar, L. Choo Min, "Transmission and storage of medical images with patient information," *Computers in Biology and Medicine*, no. 33, pp. 303-310, 2003.
- [8] R. U. Acharya, U.C. Niranjan, S.S. Iyengar, N. Kannathal, L. C. Min, "Simultaneous storage of patient information with medical images in the frequency domain," *Computer Methods and Programs in Biomedicine*, no. 76, pp.13-19, 2004.
- [9] Jagadish Nayak, Subbanna P. Bhat, Rajendra U. Acharya, Niranjan U. Cholaayya, "Simultaneous storage of medical images in the spatial and frequency domain: A comparative study," *BioMedical Engineering OnLine*, Jun 05, 2004, 3(1):17.

- [10] X. Q. Zhou, H. K. Huang, S. L. Lou, "Authenticity and integrity of digital mammography images," *IEEE Trans. Medical Imaging*, vol. 20, no. 8, pp. 784-791, Aug. 2001.
- [11] B. Macq, F. Dewey, "Trusted Headers for Medical Images," *Proc. DFG VIII-DII Watermarking Workshop*, Erlangen, Germany, Oct. 1999.
- [12] H. Trichili, M. Boubel, N. Derbel, L. Kamoun, "A new medical image watermarking scheme for a better telediagnosis," *Proc. IEEE International Conference on Systems, Man and Cybernetics*, vol. 1, pp. 556-559, Oct. 6-9, 2002.
- [13] X. Kong, R. Feng, "Watermarking medical signals for telemedicine," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 3, pp. 195-201, Sept. 2001.
- [14] Y. Yang, F. Bao, "An invertible watermarking scheme for authentication of Electronic Clinical Brain Atlas", *Proc. IEEE Intern. Conf. on Acoustics, Speech, and Signal Processing (ICASSP '03)*, vol. 3, pp. 533-536, April 6-10, 2003.
- [15] W. Puech, J. M. Rodrigues, "A new crypto-watermarking method for medical images safe transfer", *Proc. 12th Europ. Signal Processing Conf. (EUSIPCO'04)*, pp. 1481-1484, Vienna, Austria, Sept. 6-10, 2004.
- [16] D. Osborne, D. Abbott, M. Sorell, D. Rogers, "Multiple embedding using robust watermarks for wireless medical images," *Proc. 3rd Intern. Conf. Mobile and Ubiquitous Multimedia*, College Park, Maryland, USA, pp. 245-250, 2004.
- [17] F. Bao, R.H. Deng, B. Chin Ooi, Y. Yang, "Tailored reversible watermarking schemes for authentication of Electronic Clinical Atlas", *IEEE Trans. Information Technology in Biomedicine*, vol. 9, no. 4, Dec. 2005, pp. 554-563.
- [18] G. C. Langelaar, I. Setyawan, R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Sig. Proc. Mag.*, vol. 17, no. 5, pp. 20-46, Sept. 2000.
- [19] F. Mintzer, G. W. Braudaway, "If one watermark is good, are more better?" in *Proc. Intern. Conf. Acoustics, Speech, and Signal Processing, ICASSP'99*, Phoenix, AZ, March 15-19, 1999, pp. 2067-2070.
- [20] X. S. Hua, J. F. Feng, Q. Y. Shi, "Public multiple watermarking resistant to cropping," presented at the 6th Intern. Conf. Pattern Recognition and Information Processing, PRIP'2001, Minsk, Belarus.

- [21] X. S. Hua, J. F. Feng, Q. Y. Shi, "Public multiple watermarking resistant to cropping for digital images," 5th Workshop on Modern Electr. Techn. & Applic., 165-173, Kyungpook National University, Taegu, Korea. Nov. 9-12, 2000.
- [22] C. S. Lu, H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Proc.*, vol. 10, no. 10, pp. 1579-1592, Oct. 2001.
- [23] C.S. Lu, H.-Y. Mark Liao, C.J. Sze, "Combined watermarking for image authentication and protection," *Proc. 1st IEEE Int. Conf. on Multimedia and Expo*, USA, 2000.
- [24] C.S. Lu, H.Y. Mark Liao, S.K. Huang, C.J. Sze, "Cocktail Watermarking," *3rd International Workshop on Information Hiding*, LNCS 1768, pp. 333-347, Sept. 29-Oct. 1, 1999.
- [25] Gwo-Jong Yu, Chun-Shien Lu, Hong-Yuan Mark Liao, "A message-based cocktail watermarking system," *Pattern Recognition*, no, 36, pp. 957 – 968, 2003.
- [26] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple Image Watermarking Applied to Health Information Management", *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. 722-732, Oct. 2006.
- [27] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images", *Medical & Biological Engineering & Computing*, vol. 44, no. 8, pp. 619-631, Springer Berlin / Heidelberg, August 2006. Available: <http://dx.doi.org/10.1007/s11517-006-0081-x>
- [28] A. Giakoumaki, A. Tagaris, D. Koutsouris, "Implementation of a User-friendly GUI for a Multiple Image Watermarking Tool Addressing Healthcare Applications", to appear in *Proceedings of 2006 IEEE EMBS International Conference on Information Technology Applications in Biomedicine (ITAB 2006)*, Ioannina, Greece, October 26-28, 2006.
- [29] A. Giakoumaki, K. Perakis, A. Tagaris, D. Koutsouris, "Digital Watermarking in Telemedicine Applications – Towards Enhanced Data Security and Accessibility", *Proc. 28th IEEE Annual Intern. Conf. of the Engineering in Medicine and Biology Society (EMBC'06)*, pp. 6328-6331, New York, USA, Aug. 30 – Sept. 3, 2006.
- [30] A. Tagaris, A. Giakoumaki, L. Karle, D. Koutsouris, "Watermarking SDK Implementation to Facilitate Integration in a Secure Healthcare Environment", *Proc.*

- 28th IEEE Annual Intern. Conf. of the Engineering in Medicine and Biology Society (EMBC'06)*, pp. 3262-3265, New York, USA, Aug. 30 – Sept. 3, 2006.
- [31] Kostas Perakis, Aggeliki Giakoumaki, Tassos Tagaris, Dimitris Koutsouris, “Enhancement of security and accessibility in telemedical applications using digital watermarking”, *Proceedings of the 4th International Conference on Information Communication Technologies in Health, ICICTH'06*, Samos Island, Greece, July 13-15, 2006.
- [32] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, “Health Data Management through Multiple Watermarking of Medical Images”, in *IFMBE Proc. 3rd European Medical and Biological Engineering Conf., EMBEC'05*, vol. 11, pp. 3093-3096, Prague, Czech Republic, November 20-25, 2005.
- [33] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, “Multiple Digital Watermarking Applied to Medical Imaging”, *Proceedings of the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS)*, pp. 3444-3447, Shanghai, China, September 1-4, 2005.
- [34] Aggeliki Giakoumaki, Sotiris Pavlopoulos, Dimitris Koutsouris, “Digital Watermarking Perspectives in Health Information Management,” *Proceedings of the 3rd International Conference on Information Communication Technologies in Health, ICICTH'05*, pp. 316-321, Samos Island, Greece, July 7-9, 2005.
- [35] Aggeliki Giakoumaki, Sotiris Pavlopoulos, Dimitris Koutsouris, “Digital Watermarking Perspectives in Health Information Management,” *Journal for Quality of Life Research*, volume 3, issue 2, supplement 1, pp. 145-149, May-June 2005.
- [36] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, “A Multiple Watermarking Scheme Applied to Medical Image Management”, *Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS)*, pp. 3241-3244, San Francisco, CA, USA, September 1-5, 2004.
- [37] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, “A Medical Image Watermarking Scheme Based on Wavelet Transform”, *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS)*, pp. 856-859, Cancun, Mexico, September 17-21, 2003.

- [38] Giakoumaki A., Pavlopoulos S., Koutsouris D., "A wavelet-based watermarking scheme appropriate for medical images", *Proceedings of the 1st International Conference on Information Communication Technologies in Health*, Samos, Greece, July 11-13, 2003.
- [39] H.-K. Lee, H.-J. Kim, K.-R. Kwon, J.-K. Lee, "Digital watermarking of medical image using ROI information", *Proc. 7th Intern. Workshop Enterprise Networking and Computing in Healthcare Industry (HEALTHCOM)*, 2005.
- [40] C.-S. Woo, J. Du, B. Pham, "Multiple watermark method for privacy control and tamper detection in medical images", *Proc. APRS Workshop on Digital Image Computing, Pattern Recognition and Imaging for Medical Applications*, Brisbane, Queensland, Australia, February 21, 2005.
- [41] B. Planitz, A. Maeder, "Medical image watermarking: a study on image degradation", *Proc. APRS Workshop on Digital Image Computing, Pattern Recognition and Imaging for Medical Applications*, February 21, 2005, Brisbane, Queensland, Australia.
- [42] H.-K. Lee, H.-J. Kim, K.-R. Kwon, J.-K. Lee, "ROI medical image watermarking using DWT and bit-plane", *Proc. Asia-Pacific Conference on Communications*, pp. 512-515, Perth, Western Australia, Oct. 3-5, 2005.
- [43] B. M. Planitz, A. J. Maeder, "A Study of block-based medical image watermarking using a perceptual similarity metric", *Proc. IEEE Digital Imaging Computing: Techniques and Applications (DICTA 2005)*, Cairns, Queensland, Australia, Dec. 6-8, 2005.
- [44] H. M. Desai, M. S. Raval, A. I. Trivedi, "Correlation-based reversible watermarking technique for medical images", *Proc. National Conference on Image Processing*, Bangalore, India, March 23-25, 2005.
- [45] G. Coatrieux, L. Lecornu, B. Sankur, Ch. Roux, "A review of image watermarking applications in healthcare", *Proc. 28th IEEE Annual Intern. Conf. of the Engineering in Medicine and Biology Society (EMBC'06)*, pp. 4691-4694, New York City, USA, Aug. 30-Sept. 3, 2006.
- [46] G. Boato, F. G. B. De Natale, C. Fontanari, "Digital image tracing by sequential multiple watermarking", *IEEE Transactions on Multimedia*, to be published.

ΚΕΦΑΛΑΙΟ 2

ΨΗΦΙΑΚΗ ΥΔΑΤΟΓΡΑΦΙΑ

2.1 ΤΕΧΝΙΚΕΣ ΑΠΟΚΡΥΨΗΣ ΔΕΔΟΜΕΝΩΝ (DATA HIDING)

Οι τεχνικές απόκρυψης δεδομένων αποτελούν μια ευρεία κατηγορία τεχνικών που επιτρέπουν απευθείας ενσωμάτωση κρυφής πληροφορίας στα αρχικά δεδομένα. Οι τεχνικές αυτές συνδυάζουν γνώσεις από ποικίλα ερευνητικά πεδία όπως την κρυπτογραφία, την επεξεργασία σήματος και εικόνας, τις θεωρίες επικοινωνίας, κωδικοποίησης και ανθρώπινης αντιληπτικότητας.

Η στεγανογραφία και η ψηφιακή υδατογραφία αποτελούν βασικές υποκατηγορίες της «απόκρυψης δεδομένων», οι οποίες αλληλεπικαλύπτονται σε αρκετά σημεία και παρουσιάζουν κάποιες κοινές τεχνικές προσέγγισης. Υπάρχουν ωστόσο θεμελιώδεις διαφορές ως προς τη φιλοσοφία τους, γεγονός που επηρεάζει τις απαιτήσεις και κατά συνέπεια τη σχεδίαση μιας τεχνικής λύσης. Ο όρος «στεγανογραφία» προέρχεται από τις ελληνικές λέξεις «στεγανός» και «γράφειν» και ουσιαστικά δηλώνει την επίτευξη κρυφής επικοινωνίας μέσω της απόκρυψης κάποιου μηνύματος σε δεδομένα. Αναφέρεται κυρίως σε μεθόδους ενσωμάτωσης μυστικής πληροφορίας σε δεδομένα που δεν προκαλούν υποψία και τα οποία δεν έχουν καμία σχέση με τη διακινούμενη πληροφορία, αλλά χρησιμοποιούνται μόνο για συγκαλύψη της μυστικής επικοινωνίας. Σε αυτήν την κατηγορία τεχνικών δεν ενδιαφέρει η προστασία των δεδομένων που χρησιμεύουν ως μέσο μετάδοσης της κρυφής πληροφορίας, παρά μόνο η διατήρησή τους σε μια μορφή που δε θα κινεί

υποψίες για την ύπαρξη κρυμμένου μηνύματος. Οι στεγανογραφικές μέθοδοι επομένως δε στοχεύουν στην ανθεκτικότητα σε επιθέσεις, αλλά στο να παραμείνει κρυφή η επικοινωνία. Σε περίπτωση που η επικοινωνία γίνει αντιληπτή, θεωρείται ότι το στεγανογραφικό σχήμα έχει αποτύχει στο σκοπό του [1].

Σε αντίθεση με τη στεγανογραφία, στην ψηφιακή υδατογραφία απαιτείται η ανθεκτικότητα σε ενδεχόμενες επιθέσεις. Στα υδατογραφικά σχήματα τα δεδομένα που χρησιμοποιούνται για τη μετάδοση της κρυφής πληροφορίας έχουν αξία – σε αντίθεση με ό,τι συμβαίνει στην περίπτωση της στεγανογραφίας – και άρα ενδιαφέρει η διατήρηση της ποιότητάς τους. Τα υδατογραφήματα που ενσωματώνονται έχουν σχέση με τα αρχικά δεδομένα και σε κάποιες εφαρμογές δεν υπάρχει καν η απαίτηση να μη γίνονται αντιληπτά. Για παράδειγμα, είναι επιθυμητή η αναγνωσιμότητα ενός υδατογραφήματος από όλους όταν αυτό προορίζεται για την προστασία των πνευματικών δικαιωμάτων του δημιουργού. Το υδατογράφημα είναι μόνιμα συνδεδεμένο με τα αρχικά δεδομένα και κάθε απόπειρα εξάλειψής του θα πρέπει να συνεπάγεται αλλοίωσή τους σε τέτοιο βαθμό, ώστε να χάνουν την αξία τους και να μην μπορούν πλέον να χρησιμοποιηθούν.

Όπως προαναφέρθηκε, ένα βασικό σημείο στο οποίο διαφέρει η ψηφιακή υδατογραφία από τη στεγανογραφία είναι το γεγονός ότι στην πρώτη περίπτωση δε χρειάζεται απαραίτητα να παραμείνει κρυφή η μετάδοση μυστικής πληροφορίας. Ακόμη και αν γίνει γνωστή η ύπαρξη κρυφού μηνύματος, το σημαντικό στην ψηφιακή υδατογραφία είναι το μήνυμα αυτό να μην μπορεί να προσπελαστεί ούτε να αφαιρεθεί από μη εξουσιοδοτημένο χρήστη. Η ψηφιακή υδατογραφία υιοθέτησε μια αρχή που εφαρμόζεται στην κρυπτογραφία, τη λεγόμενη «αρχή του Kerckhoff» («Kerckhoff's principle»), σύμφωνα με την οποία «ένα κρυπτογραφικό σύστημα πρέπει να παραμένει ασφαλές ακόμη και όταν ο επιτιθέμενος γνωρίζει τις κρυπτογραφικές αρχές και μεθόδους που χρησιμοποιούνται, αλλά όχι το κατάλληλο κλειδί». Εφαρμόζοντας την αρχή του Kerckhoff στην υδατογραφία, η ανθεκτικότητα σε επιθέσεις ερμηνεύεται ως αδυναμία του επιτιθέμενου να εντοπίσει, να διαβάσει ή να καταστρέψει το κρυμμένο μήνυμα, ακόμη και όταν γνωρίζει την υδατογραφική μέθοδο που έχει χρησιμοποιηθεί. Αποτέλεσμα της απαίτησης για ανθεκτικότητα στην υδατογραφία είναι ο περιορισμένος – σε σχέση με τη στεγανογραφία – όγκος

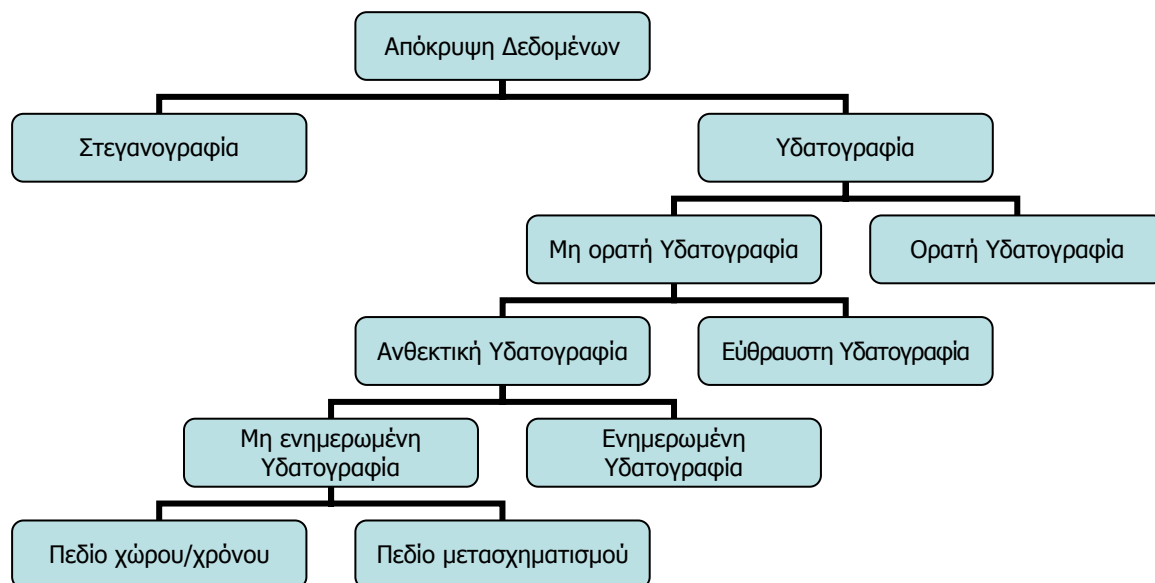
πληροφορίας που μπορεί να ενσωματωθεί («χωρητικότητα») [2]. Όπως θα φανεί σαφέστερα σε επόμενες ενότητες, οι απαιτήσεις ως προς την ανθεκτικότητα, τη διαφάνεια και τη χωρητικότητα εξαρτώνται από την εφαρμογή και παρουσιάζουν ακόμη και μεγάλες διαφοροποιήσεις, ανάλογα με την περίπτωση.

Οι τεχνικές απόκρυψης δεδομένων προσφέρουν συμπληρωματικές ή εναλλακτικές λύσεις σε περιπτώσεις όπου η κρυπτογραφία είτε δεν αρκεί, είτε είναι ακατάλληλη. Η κρυπτογραφία αποτελεί στις μέρες μας μια ευρέως χρησιμοποιούμενη μέθοδο προστασίας ψηφιακών δεδομένων μέσω της κωδικοποίησής τους, που τα καθιστά ακατάληπτα χωρίς το κλειδί αποκωδικοποίησης. Το περιεχόμενο κρυπτογραφείται πριν από τη μετάδοσή του και το κλειδί αποκρυπτογράφησης παρέχεται μόνο σε όσους διαθέτουν νόμιμα αντίγραφα των δεδομένων. Στη συνέχεια το κρυπτογραφημένο αρχείο μπορεί να διανεμηθεί μέσω του διαδικτύου, καθώς είναι ακατάληπτο χωρίς τη γνώση του κατάλληλου κλειδιού. Η κρυπτογραφία όμως δεν παρέχει τη δυνατότητα στον αποστολέα να παρακολουθήσει πώς διαχειρίζεται ο νόμιμος παραλήπτης τα δεδομένα μετά την αποκρυπτογράφησή τους. Υπάρχει πάντα το ενδεχόμενο να λάβει ο εξουσιοδοτημένος παραλήπτης το κρυπτογραφημένο υλικό, να χρησιμοποιήσει το κλειδί αποκρυπτογράφησης για να αποκτήσει μια μη προστατευμένη έκδοση του περιεχομένου και στη συνέχεια να προχωρήσει σε διανομή παράνομων αντιγράφων. Κατά συνέπεια η πληροφορία είναι προστατευμένη μόνο όταν είναι σε κρυπτογραφημένη μορφή, ενώ από τη στιγμή που αποκρυπτογραφείται είναι προσπελάσιμη από όλους και ευάλωτη σε επιθέσεις. Αυτή η αδυναμία της κρυπτογραφίας αντιμετωπίζεται με χρήση υδατογραφίας, που επιτρέπει την προστασία του περιεχομένου ακόμη και μετά την αποκρυπτογράφησή του, καθώς η πληροφορία ενσωματώνεται απευθείας στα δεδομένα, από τα οποία δεν αφαιρείται ποτέ υπό συνθήκες κανονικής χρήσης. Σε αντίθεση με την κρυπτογραφία, που προστατεύει μεν την πληροφορία κατά τη μετάδοση, αλλά δεν παρέχει κάποιον τρόπο εξέτασης των αρχικών δεδομένων στην «προστατευμένη» μορφή τους, το υδατογράφημα παρέχει μια μόνιμη σύνδεση της πληροφορίας με τα δεδομένα στα οποία έχει ενσωματωθεί και υφίσταται τις ίδιες τροποποιήσεις με αυτά. Ο συνδυασμός των δύο τεχνικών, η χρήση δηλαδή υδατογραφίας για την

απόκρυψη ενός κρυπτογραφημένου μηνύματος, προσφέρει ένα επιπλέον επίπεδο προστασίας: ακόμη και αν καταφέρει ένας μη εξουσιοδοτημένος χρήστης να ανιχνεύσει το υδατογράφημα, θα χρειαστεί το κατάλληλο κλειδί αποκωδικοποίησης προκειμένου να αποκρυπτογραφήσει το μήνυμα [2]-[4].

Λόγω της παράλληλης μελέτης και ανάπτυξης υδατογραφικών σχημάτων από ερευνητικές ομάδες προερχόμενες από διαφορετικούς τομείς, παρατηρούνται στη βιβλιογραφία διαφοροποιήσεις ως προς τη σχετική ορολογία, οι οποίες συχνά δημιουργούν σύγχυση [1]. Τα συστήματα ενσωμάτωσης πρόσθετης πληροφορίας σε δεδομένα μπορούν να διακριθούν σε «υδατογραφικά» και «μη υδατογραφικά». Στην πρώτη κατηγορία το μήνυμα έχει άμεση σχέση με το αντικείμενο στο οποίο ενσωματώνεται, ενώ στη δεύτερη κατηγορία τα αρχικά δεδομένα χρησιμεύουν απλώς ως μέσο απόκρυψης και δεν έχουν καμία σχέση με το μεταφερόμενο μήνυμα. Στη βιβλιογραφία συναντάται και η διάκριση ανάμεσα στα «στεγανογραφικά» συστήματα – όπου αποκρύπτεται το γεγονός της ενσωμάτωσης μηνύματος – και τα «μη στεγανογραφικά», στα οποία δεν είναι μυστική η ύπαρξή του. Οι όροι «fingerprinting» και «labeling» αναφέρονται στις εφαρμογές της υδατογραφίας σε θέματα προστασίας πνευματικών δικαιωμάτων και πιο συγκεκριμένα στην εισαγωγή πληροφορίας σχετικής με την πηγή προέλευσης και το νόμιμο παραλήπτη των δεδομένων. Τα υδατογραφήματα σε αυτές τις εφαρμογές περιέχουν αναγνωριστικούς κωδικούς (serial numbers) διαφορετικούς για κάθε παραλήπτη και συχνά καλούνται «αποτυπώματα» (fingerprints) ή «ετικέτες» (labels) [1]. Τα «ορατά υδατογραφήματα» τέλος, είναι ειδικά σχέδια, όπως λογότυπα, που ενσωματώνονται σε εικόνες ή βίντεο και έχουν χρησιμότητα αντίστοιχη με αυτήν των υδατογραφημάτων που τυπώνονται σε χαρτί. Συνήθως χρησιμοποιούνται σε εικόνες που διατίθενται στο διαδίκτυο ή σε βάσεις δεδομένων, προκειμένου να αποτρέψουν την εμπορική τους χρήση χωρίς άδεια [5]. Προς αποφυγή σύγχυσης, στην παρούσα διατριβή θα χρησιμοποιείται ο όρος «υδατογραφία» για να περιγράψει τις τεχνικές που ενσωματώνουν σε κάποιο ψηφιακό αντικείμενο πρόσθετη πληροφορία, η οποία έχει άμεση σχέση με το αντικείμενο αυτό και είναι προσπελάσιμη μόνο από εξουσιοδοτημένους χρήστες. Στο Σχήμα 1 δίνεται η κατηγοριοποίηση των τεχνικών απόκρυψης δεδομένων. Όπως φαίνεται και στο διάγραμμα, τα μη ορατά

υδατογραφήματα διακρίνονται σε ανθεκτικά και εύθραυστα. Τα εύθραυστα υδατογραφήματα δεν επιβιώνουν από ανεπιθύμητους μετασχηματισμούς στα αρχικά δεδομένα και επιτρέπουν τον έλεγχο ακεραιότητάς τους και την ανίχνευση των μεταβολών. Αντίθετα, τα ανθεκτικά υδατογραφήματα διατηρούνται τόσο μετά από κοινές ενέργειες επεξεργασίας σήματος / εικόνας όσο και μετά από κακόβουλες επιθέσεις. Τα ανθεκτικά υδατογραφικά σχήματα διακρίνονται περαιτέρω σε «*ενημερωμένα*» (non-blind watermarking schemes) και «*μη ενημερωμένα*» (blind). Τα «*ενημερωμένα*» σχήματα [6]-[9] προϋποθέτουν τη γνώση των αρχικών δεδομένων (original host signal) για την εξαγωγή του υδατογραφήματος και χαρακτηρίζονται γενικά από μεγαλύτερη ανθεκτικότητα σε επιθέσεις. Η απαίτηση όμως για γνώση του αρχικού σήματος στη φάση εξαγωγής του υδατογραφήματος περιορίζει δραστικά τις πρακτικές εφαρμογές της συγκεκριμένης κατηγορίας. Στα «*μη ενημερωμένα*» ή «*τυφλά*» υδατογραφικά σχήματα η εξαγωγή του υδατογραφήματος δεν απαιτεί πρόσβαση στα αρχικά, μη υδατογραφημένα δεδομένα, παρόλο μόνο γνώση ενός κλειδιού. Οι τεχνικές αυτές ταξινομούνται σε δύο κατηγορίες [10], τις τεχνικές που εφαρμόζονται στο πεδίο του χώρου/χρόνου (spatial/time domain) [11] και εκείνες που χρησιμοποιούν κάποιο πεδίο μετασχηματισμού (transform domain) [12], [13]. Η πρώτη κατηγορία ενσωματώνει το υδατογράφημα στο πεδίο του χώρου (pixels) ή του χρόνου στην περίπτωση εικόνας ή σήματος ήχου αντιστοίχως, ενώ η δεύτερη κατηγορία χρησιμοποιεί μετασχηματισμένες μορφές των αρχικών δεδομένων, που προκύπτουν από τους διακριτούς μετασχηματισμούς Fourier (DFT), συνημιτόνου (DCT), wavelet (DWT) κ.λπ. Αξίζει να σημειωθεί ότι κάποια από τα «*ενημερωμένα*» υδατογραφικά σχήματα μπορούν να τροποποιηθούν έτσι ώστε να μην απαιτείται γνώση του αρχικού σήματος για την εξαγωγή του υδατογραφήματος, με κάποιο κόστος όμως ως προς την απόδοση (performance) [6], [8].



Σχήμα 1: Ταξινόμηση τεχνικών απόκρυψης δεδομένων

Στη βιβλιογραφία υπάρχει πληθώρα μελετών που επικεντρώνονται στην υδατογράφιση εικόνων. Όπως προαναφέρθηκε, η εισαγωγή του υδατογραφήματος γίνεται είτε απευθείας στα αρχικά δεδομένα, είτε σε μια μετασχηματισμένη μορφή τους [10]. Η απευθείας ενσωμάτωση του υδατογραφήματος στις τιμές των pixels της εικόνας, που εφαρμόζεται από τις τεχνικές χωρικού πεδίου (spatial domain), χαρακτηρίζεται από χαμηλή πολυπλοκότητα και κόστος, αλλά από την άλλη παρουσιάζει σχετικά χαμηλή ανθεκτικότητα. Οι τεχνικές σε πεδίο μετασχηματισμού είναι ιδιαίτερα δημοφιλείς στις μέρες μας καθώς πλεονεκτούν ως προς τη διαφάνεια και την προστασία του υδατογραφήματος, μέσω της αξιοποίησης ιδιοτήτων ανθρώπινης αντιληπτικότητας (perceptual properties) που επιτρέπει την αύξηση της ανθεκτικότητας χωρίς αλλοίωση του οπτικού αποτελέσματος [2], [7], [14], [15]. Σε επόμενη ενότητα παρατίθεται λεπτομερής ταξινόμηση των υδατογραφικών τεχνικών και ανασκόπηση της πλούσιας βιβλιογραφίας μέσω της παρουσίασης κάποιων αντιπροσωπευτικών σχημάτων.

Μέχρι πρόσφατα οι ερευνητικές προσπάθειες πάνω σε τεχνικές απόκρυψης δεδομένων ήταν σαφώς ελάχιστες σε σχέση με τις αντίστοιχες μελέτες για την κρυπτογραφία, ωστόσο το σκηνικό αλλάζει ραγδαία τα τελευταία χρόνια. Από το πρώτο σχετικό συνέδριο που διοργανώθηκε το 1996 μέχρι σήμερα, έχουν σημειωθεί εκτεταμένες έρευνες με αντίστοιχο εντυπωσιακό εμπλουτισμό της παγκόσμιας

βιβλιογραφίας. Το πρωταρχικό μέλημα των ερευνητών που ασχολήθηκαν με το πεδίο αυτό ήταν η κατοχύρωση των πνευματικών δικαιωμάτων των δημιουργών. Σε μια εποχή που οι τεχνολογικές εξελίξεις έχουν ως αποτέλεσμα τη διαθεσιμότητα τεράστιου όγκου δεδομένων σε ψηφιακή μορφή και την εξαιρετικά εύκολη δημιουργία πιστών αντιγράφων, ζητήματα προστασίας της πνευματικής ιδιοκτησίας αποκτούν ιδιαίτερη σημασία και γίνεται επιτακτική η εύρεση αποτελεσματικών λύσεων. Ήταν εύλογη επομένως η εκδήλωση έντονου ερευνητικού ενδιαφέροντος για τη χρήση των τεχνικών απόκρυψης δεδομένων στην υπηρεσία της κατοχύρωσης πνευματικής ιδιοκτησίας. Όμως, η ψηφιακή υδατογραφία έχει αποδειχθεί κατάλληλη και για πληθώρα άλλων εφαρμογών, όπως για παρακολούθηση μετάδοσης (broadcast monitoring), ανίχνευση συναλλαγών (transaction tracking), πιστοποίηση (authentication) και έλεγχο αντιγραφής (copy control) [16].

2.2 ΕΦΑΡΜΟΓΕΣ ΨΗΦΙΑΚΗΣ ΥΔΑΤΟΓΡΑΦΙΑΣ

Οι τεχνολογικές εξελίξεις που σημειώθηκαν τα τελευταία χρόνια και η ευρεία χρήση του διαδικτύου για διαχείριση ψηφιακών δεδομένων διευκόλυναν την πρόσβαση κατανεμημένης πληροφορίας, εγείροντας όμως παράλληλα πρόσθετα ζητήματα ασφάλειας [17]. Στα πλαίσια αυτά επιβάλλεται η ανάπτυξη νέων μηχανισμών για τον αποτελεσματικό έλεγχο πρόσβασης στα δεδομένα, ώστε μόνο εξουσιοδοτημένα άτομα να έχουν τη δυνατότητα ανάκτησης και εγκεκριμένης τροποποίησης της παρεχόμενης πληροφορίας. Η ψηφιακή υδατογραφία αποτελεί μια τεχνολογία που έκανε την εμφάνισή της στα μέσα της δεκαετίας του '90 και οι πρώτες σχετικές ερευνητικές προσπάθειες στόχευαν στην κατοχύρωση των πνευματικών δικαιωμάτων για τα δεδομένα που διατίθενται μέσω του διαδικτύου. Η ωρίμανση της τεχνολογίας αυτής που σημειώθηκε τα τελευταία χρόνια συνοδεύτηκε από πληθώρα ερευνητικών μελετών, οι οποίες ανέδειξαν τις ποικίλες προοπτικές της σε μια ευρεία κλίμακα εφαρμογών. Παρόλο που η ψηφιακή υδατογραφία και οι τεχνικές απόκρυψης δεδομένων παραμένουν ιδιαίτερα δημοφιλείς στην προσπάθεια κατοχύρωσης της πνευματικής ιδιοκτησίας (copyright), η κλίμακα των εφαρμογών τους διαρκώς διευρύνεται, περιλαμβάνοντας μεταξύ άλλων τον έλεγχο

ακεραιότητας δεδομένων, την πιστοποίηση αποστολέα και παραλήπτη και την παρακολούθηση μετάδοσης δεδομένων (data monitoring). Στη συνέχεια παρατίθενται οι εφαρμογές της υδατογραφίας που έχουν ήδη παρουσιαστεί στη βιβλιογραφία.

2.2.1 Προστασία Πνευματικών Δικαιωμάτων

Η κατοχύρωση των πνευματικών δικαιωμάτων των δημιουργών ψηφιακών δεδομένων αποτέλεσε το βασικό κίνητρο για την ανάπτυξη της ψηφιακής υδατογραφίας. Το γεγονός αυτό είχε ως αποτέλεσμα να υπάρχει στις μέρες μας εκτενής σχετική βιβλιογραφία και ευρεία χρήση υδατογραφημάτων για την ενσωμάτωση στοιχείων πνευματικής ιδιοκτησίας ή/και συνθηκών χρήσης σε ψηφιακά δεδομένα. Μέχρι πρόσφατα, ο μοναδικός τρόπος προστασίας των πνευματικών δικαιωμάτων ήταν η χρήση κρυπτογραφίας, η οποία έχει το βασικό μειονέκτημα ότι δεν παρέχει προστασία στα δεδομένα από τη στιγμή της αποκρυπτογράφησης τους. Οι τεχνικές υδατογραφίας συμπληρώνουν την κρυπτογραφία, καθώς ενσωματώνουν στα αρχικά δεδομένα ένα υδατογράφημα που κατοχυρώνει την πνευματική ιδιοκτησία και το οποίο δεν μπορεί να αποσπαστεί εύκολα [17], ή του οποίου η αφαίρεση προκαλεί την υποβάθμιση της ποιότητας των αρχικών δεδομένων σε τέτοιο βαθμό, ώστε να χάνουν πλέον την αξία τους και να μην μπορούν να χρησιμοποιηθούν από επίδοξους «πειρατές» [16]. Στις εικόνες η χρήση μη αντιληπτού υδατογραφήματος πλεονεκτεί σε σχέση με μια γραπτή επισήμανση πνευματικών δικαιωμάτων, καθώς το υδατογράφημα αφήνει αναλλοίωτο το αισθητικό αποτέλεσμα και επιπλέον εξαλείφεται δύσκολα, σε αντίθεση με τη γραπτή επισήμανση που συνήθως καλύπτει ένα άκρο της εικόνας και μπορεί εύκολα να αφαιρεθεί. Στην περίπτωση δεδομένων ήχου η γραπτή επισήμανση πνευματικής ιδιοκτησίας είναι ακόμη πιο ανεπαρκής, καθώς τοποθετείται πάνω στο φυσικό μέσο (δίσκος, κασέτα, CD) που περιέχει τα αρχεία ήχου και δεν αντιγράφεται μαζί με τα αρχεία αυτά. Η μόνιμη σύνδεση του υδατογραφήματος με τα δεδομένα προσφέρει ένα σαφώς βελτιωμένο επίπεδο προστασίας των πνευματικών δικαιωμάτων του δημιουργού. Σε αυτήν την

κατηγορία εφαρμογών το υδατογράφημα ταυτοποιεί τον πνευματικό δημιουργό των δεδομένων (owner identification) και αποτελεί ουσιαστικά μια μορφή υπογραφής. Η πληροφορία που περιέχεται στο υδατογράφημα μπορεί στη συνέχεια να χρησιμοποιηθεί από το χρήστη ώστε να αποκτήσει νόμιμα δικαιώματα αντιγραφής ή χρήσης του περιεχομένου και στο μέλλον δεν αποκλείεται να χρησιμοποιηθεί και για την επίλυση αντιδικιών ιδιοκτησίας [18]. Για να λειτουργήσει όμως η υδατογραφία ως μέσο επίλυσης αντιδικιών στα δικαστήρια, δεν αρκεί η απλή ταυτοποίηση του δημιουργού. Η μεγάλη πρόκληση είναι να αποδειχθεί ότι ο δημιουργός που αναγνωρίζεται από το υδατογράφημα είναι ο πραγματικός κάτοχος των πνευματικών δικαιωμάτων και όχι κάποιος επιδέξις λογοκλόπος (proof of ownership), θέμα όμως που ξεφεύγει από το αντικείμενο της παρούσας διατριβής και δεν αναλύεται περισσότερο.

2.2.2 Ανίχνευση Συναλλαγών (Fingerprinting)

Μια άλλη εφαρμογή της υδατογραφίας που έχει άμεση σχέση με την πάταξη της πειρατείας είναι η ταυτοποίηση του παραλήπτη μέσω της εμφύτευσης ειδικών αναγνωριστικών κωδικών και χρονικής σφραγίδας (time-stamp) στα ψηφιακά δεδομένα που προορίζονται για πώληση ή διανομή. Η παρεχόμενη πληροφορία σχετικά με το νόμιμο παραλήπτη επιτρέπει τον εντοπισμό μεμονωμένων αντιγράφων του υλικού που έχουν διανεμηθεί παράνομα και την αναγνώριση του νόμιμου αγοραστή που ευθύνεται για την πειρατεία [19]. Σε αυτού του είδους τις εφαρμογές το υδατογράφημα είναι αντίστοιχο με τους σειριακούς αριθμούς (serial numbers) που αναγράφονται στα προϊόντα και καλείται συχνά «αποτύπωμα» (fingerprint), καθώς ο ρόλος του είναι να προσδιορίσει μοναδικά την ταυτότητα του παραλήπτη.

Οι τεχνικές που προορίζονται για αυτό το πεδίο εφαρμογής δεν αποτρέπουν τη δημιουργία αντιγράφων, αλλά παρέχουν τη δυνατότητα στο νόμιμο ιδιοκτήτη να ανιχνεύσει τους εξουσιοδοτημένους χρήστες που διένειμαν παράνομα τα αντίγραφα αυτά. Στη μετάδοση κωδικοποιημένου τηλεοπτικού σήματος για παράδειγμα, οι χρήστες έχουν στην κατοχή τους ένα σύνολο κλειδιών για την αποκωδικοποίηση του

σήματος. Στην περίπτωση που ο σταθμός εισαγάγει «αποτυπώματα» στα πακέτα μετάδοσης, μπορεί να εντοπίσει τους εξουσιοδοτημένους χρήστες που παραχώρησαν παράνομα τα κλειδιά αποκωδικοποίησης. Η διαδικασία εισαγωγής «αποτυπωμάτων» (fingerprinting) χρησιμοποιείται επομένως για την ανίχνευση παρανομίας (traitor tracing). Σε πολλές εφαρμογές εισαγωγής «αποτυπωμάτων» απαιτείται εύκολη και χαμηλής πολυπλοκότητας εξαγωγή του υδατογραφήματος, όπως για παράδειγμα σε διαδικτυακές εφαρμογές όπου ειδικές μηχανές αναζήτησης (web crawlers) ανιχνεύουν παράνομα διανεμημένες υδατογραφημένες εικόνες. Τα υδατογραφήματα που χρησιμοποιούνται σε αυτήν την κατηγορία εφαρμογών απαιτούν επίσης μεγάλη ανθεκτικότητα σε συνηθισμένες ενέργειες επεξεργασίας των δεδομένων, αλλά και σε εσκεμμένες απόπειρες αλλοίωσής τους (malicious attacks). Μια βασική κατηγορία «επιθέσεων» που πρέπει να αποτραπούν σε αυτές τις περιπτώσεις είναι οι λεγόμενες «επιθέσεις συννομωσίας» (collusion attacks), οι οποίες στοχεύουν στην εξαγωγή της αρχικής, μη υδατογραφημένης έκδοσης του αντικειμένου μέσω της σύγκρισης πολλαπλών υδατογραφημένων εκδοχών του [16].

2.2.3 Δεικτοδότηση (Indexing)

Ένα άλλο πεδίο εφαρμογής της υδατογραφίας αποτελεί η ταχεία αναζήτηση σε βάσεις δεδομένων. Η διαδικασία αυτή συνήθως βασίζεται σε συναρτήσεις σύνοψης (hash functions) που εξάγουν μοναδικά χαρακτηριστικά των αντικειμένων της βάσης, τα οποία τα διαφοροποιούν από άλλα ομοειδή τους και επιτρέπουν την ανάκτηση σχετικών δεδομένων [20]. Η αναζήτηση εικόνων γίνεται συχνά με χρήση καταλλήλων λέξεων-κλειδιών, ενώ τα τελευταία χρόνια προτείνεται στη βιβλιογραφία η ανάκτηση εικόνων με βάση το περιεχόμενό τους (content-based image retrieval) [21]-[24]. Τα υδατογραφήματα που χρησιμοποιούνται σε αυτές τις εφαρμογές αναφέρονται συχνά στη βιβλιογραφία ως «δείκτες» (markers, indices) και είναι είτε ειδικοί αναγνωριστικοί κωδικοί (π.χ. λέξεις-κλειδιά), είτε εγγενή (intrinsic) χαρακτηριστικά του αντικειμένου που προκύπτουν από κατάλληλη επεξεργασία του. Η χρήση υδατογραφημάτων σε εφαρμογές δεικτοδότησης παρέχει έναν αποδοτικό τρόπο αρχειοθέτησης, διαχείρισης και εύκολης ανάκτησης δεδομένων

από μηχανισμούς αναζήτησης (querying mechanisms). Προσφέρει επίσης το πλεονέκτημα των μειωμένων απαιτήσεων μνήμης αποθήκευσης και εύρους μετάδοσης, σε σχέση με τη χρήση μεταδεδομένων για τον ίδιο σκοπό [25]. Εκτός από την ταχεία ανάκτηση πληροφορίας από βάσεις δεδομένων, υδατογραφήματα μπορούν να χρησιμοποιηθούν και σε εφαρμογές βίντεο για την ενσωμάτωση σχολίων και δεικτών στο περιεχόμενο [26]. Επιπλέον η εισαγωγή χρονικών δεικτών (time markers) στα καρέ (frames) μιας βιντεοταινίας επιτρέπει το συγχρονισμό των καρέ με τον ήχο. Τέλος, η δεικτοδότηση μέσω υδατογραφημάτων είναι χρήσιμη και σε εφαρμογές θέασης επί πληρωμή (pay-per-view), όπου είναι δυνατή η ενσωμάτωση σε εικόνα ενός αριθμού που αντιστοιχεί στο πόσες φορές έχει προσπελάσει κάποιος χρήστης τη συγκεκριμένη εικόνα [17].

2.2.4 Επισήμανση Χαρακτηριστικών (Feature Tagging)

Η υδατογραφία επιτρέπει την ενσωμάτωση περιγραφικής πληροφορίας, όπως επικεφαλίδων, σχολίων, ονομάτων απεικονιζόμενων αντικειμένων ή τοποθεσιών χαρτών, σε συγκεκριμένες περιοχές στην εικόνα [17]. Η επισήμανση των χαρακτηριστικών επιτρέπει να δοθεί έμφαση στα σημαντικά στοιχεία της εικόνας και παρέχει πρόσθετη βοηθητική πληροφορία στους εξουσιοδοτημένους χρήστες. Η προσθήκη επικεφαλίδων (captioning) και σχολίων (annotation) απευθείας στις εικόνες εξασφαλίζει τη μόνιμη σύνδεση των απεικονιζόμενων αντικειμένων με τη σχετική πληροφορία, χωρίς τον κίνδυνο απώλειας της τελευταίας σε περίπτωση αλλαγής μορφοποίησης (format) του αρχείου και χωρίς περιττές απαιτήσεις σε μνήμη αποθήκευσης και εύρος μετάδοσης.

Αντίθετα, η χρήση μεταδεδομένων και η χωριστή μετάδοσή τους συνεπάγεται πρόσθετες απαιτήσεις σε κανάλια μετάδοσης και μνήμη αποθήκευσης. Επίσης, ακόμη και μια απλή αλλαγή στη μορφοποίηση του αρχείου ενδέχεται να οδηγήσει στην απώλεια των μεταδεδομένων που αποθηκεύονται στην επικεφαλίδα (header) του, όπως για παράδειγμα συμβαίνει στην περίπτωση μετατροπής μιας εικόνας TIF (Tagged Image File Format) σε μορφή GIF (Graphic Interchange Format) [11].

Αξίζει να σημειωθεί ότι λόγω της χρησιμότητάς τους, τα υδατογραφήματα επισήμανσης χαρακτηριστικών δεν απειλούνται συνήθως από εσκεμμένες απόπειρες αλλοίωσής τους, υπάρχει όμως πάντα ο κίνδυνος τροποποίησής τους από τετριμμένες ενέργειες επεξεργασίας των εικόνων, όπως για παράδειγμα από αλλαγή κλίμακας ή cropping.

2.2.5 Μυστική Επικοινωνία (Data Hiding)

Σε πολλές περιπτώσεις όπου είναι ανεπιθύμητη η γνωστοποίηση της ύπαρξης επικοινωνίας μεταξύ δύο μερών η κρυπτογραφία αντενδείκνυται, καθώς η μετάδοση κρυπτογραφημένου μηνύματος εφιστά την προσοχή και δημιουργεί υποψίες σχετικά με τη φύση της διακινούμενης πληροφορίας. Η στεγανογραφία αντίθετα επιτρέπει τη μυστική επικοινωνία προστατεύοντας τα επικοινωνούντα μέρη και τα μηνύματά τους από ανεπιθύμητο έλεγχο. Επαγγελματικά μυστικά, προσχέδια εργασιών ή άλλες «ευαίσθητες» πληροφορίες μπορούν με αυτόν τον τρόπο να μεταδοθούν χωρίς να κινήσουν υποψίες σε επίδοξους υποκλοπείς. Το ενσωματωμένο σήμα χρησιμοποιείται για την ανταλλαγή μυστικής πληροφορίας μεταξύ δύο ατόμων, χωρίς να γνωρίζει κανείς άλλος το γεγονός της μετάδοσής της. Η απόκρυψη άλλωστε μιας πληροφορίας μέσα σε μια άλλη αποτελεί τη βασική αρχή της στεγανογραφίας, αλλά και μια τακτική που εφαρμόστηκε ήδη από την αρχαιότητα, όπως προκύπτει από διάφορα παραδείγματα στην ιστορία [27].

2.2.6 Παρακολούθηση Μετάδοσης (Broadcast Monitoring)

Το υδατογράφημα μπορεί να ανιχνευτεί από αυτόματα συστήματα που παρακολουθούν τις τηλεοπτικές και ραδιοφωνικές μεταδόσεις, τα δίκτυα υπολογιστών και άλλα κανάλια ροής πληροφορίας, προκειμένου να καταγράψουν πότε και πού εμφανίζονται τα δεδομένα. Αυτή η εφαρμογή είναι ιδιαίτερα χρήσιμη στους κατόχους πνευματικών δικαιωμάτων, καθώς τους δίνεται η δυνατότητα να αποτρέψουν την παράνομη διανομή του υλικού τους ή/και να διασφαλίσουν αποζημίωση για τη χρήση των πνευματικών τους δημιουργημάτων. Επίσης η εφαρμογή αυτή εξυπηρετεί τους διαφημιστές που επιθυμούν να εξασφαλίσουν τη

μετάδοση των διαφημίσεών τους στις ώρες και στα μέσα για τα οποία έχουν πληρώσει.

Η προσθήκη των αναγνωριστικών στοιχείων σε ξεχωριστό τμήμα του σήματος προς μετάδοση, καθιστά δύσκολη τη διατήρηση της συνημμένης πληροφορίας μετά από αλλαγές στη μορφοποίηση (format). Αντίθετα, η υδατογραφία αποτελεί μια αποδοτική λύση κωδικοποίησης της πληροφορίας αναγνώρισης μέσα στα δεδομένα, εξασφαλίζοντας τη διατήρησή της στην περίπτωση αλλαγής μορφοποίησης. Ένα ζήτημα βέβαια που προκύπτει είναι το εάν και πόσο επιδρά η ενσωματωμένη πληροφορία στην ποιότητα των αρχικών δεδομένων. Πάντως υπάρχουν ήδη αρκετές εταιρείες που παρέχουν υπηρεσίες παρακολούθησης της μετάδοσης δεδομένων με χρήση υδατογραφημάτων [16].

2.2.7 Έλεγχος Αντιγραφών (Copy Control)

Εκτός από την κατοχύρωση των δικαιωμάτων τους, ένα βασικό ζήτημα που απασχολεί τους πνευματικούς δημιουργούς αποτελεί η δυνατότητα ελέγχου της αναπαραγωγής αντιγράφων. Υδατογραφήματα που περιέχουν κανόνες χρήσης / αντιγραφής και καθορίζουν το εάν και πόσες φορές επιτρέπεται η αντιγραφή του περιεχομένου (π.χ. «never copy», «copy once»), μπορούν να αποτελέσουν τη βάση ενός μηχανισμού προστασίας από παράνομη αντιγραφή του υλικού. Για το σκοπό αυτό η συνήθης πρακτική μέχρι σήμερα είναι η κρυπτογράφηση του περιεχομένου με χρήση μυστικού κλειδιού, η οποία παρέχει προστασία από μη εξουσιοδοτημένους χρήστες που δεν έχουν υπό την κατοχή τους το κατάλληλο κλειδί αποκωδικοποίησης. Το κλειδί αυτό πρέπει να παρέχεται στους νόμιμους κατόχους του με τέτοιο τρόπο ώστε να καθίσταται εξαιρετικά δύσκολη η αντιγραφή ή διανομή του. Για παράδειγμα, τα κρυπτογραφημένα δορυφορικά τηλεοπτικά σήματα αποκρυπτογραφούνται με κλειδιά τα οποία συνήθως παρέχονται στους αγοραστές μέσω έξυπνων καρτών (smart cards) που εισάγονται στον τηλεοπτικό ψηφιακό αποκωδικοποιητή / δέκτη (television set-top box). Υπάρχουν τρεις τρόποι με τους οποίους ενδέχεται να επιχειρήσει κάποιος την εξουδετέρωση ενός κρυπτογραφικού συστήματος. Ο πρώτος και πιο δύσκολος τρόπος είναι η αποκρυπτογράφηση των

δεδομένων χωρίς τη γνώση του κλειδιού, που συνήθως προϋποθέτει διεξοδική έρευνα, κατά την οποία ο επίδοξος «παραβιαστής» επιχειρεί να αποκρυπτογραφήσει το σήμα χρησιμοποιώντας εκατομμύρια κλειδιά. Σε ένα καλά σχεδιασμένο κρυπτογραφικό σύστημα θα χρειαστεί η δοκιμή κάθε πιθανού κλειδιού, κάτι που είναι εξαιρετικά δύσκολο στην πράξη εάν τα κλειδιά αποτελούνται από περισσότερα από 50 bits. Μια άλλη μέθοδος είναι η προσπάθεια υποκλοπής του κλειδιού, που μπορεί να γίνει μέσω αντίστροφης μηχανικής (reverse engineering) στο υλικό ή λογισμικό που το περιέχει. Τον απλούστερο τρόπο παράκαμψης του κρυπτογραφικού συστήματος αποτελεί η νόμιμη απόκτηση ενός κλειδιού και η δημιουργία αντιγράφων μετά την αποκρυπτογράφηση του υλικού. Είναι φανερό επομένως η αδυναμία της κρυπτογραφίας όσον αφορά τον έλεγχο της παράνομης αντιγραφής, καθώς τα δεδομένα πρέπει να αποκρυπτογραφηθούν προκειμένου να χρησιμοποιηθούν και από τη στιγμή που θα γίνει αυτό δεν μπορεί πλέον να αποφευχθεί η παράνομη δημιουργία αντιτύπων.

Τα υδατογραφήματα αντιθέτως, ενσωματώνονται απευθείας στο ψηφιακό αντικείμενο και παραμένουν σε αυτό ανεξάρτητα από τυχόν αλλαγές στη μορφοποίησή του, προσφέροντας έτσι καλύτερο έλεγχο αναπαραγωγής αντιγράφων. Συσκευές αντιγραφής που διαθέτουν ανιχνευτές υδατογραφημάτων μπορούν με τις κατάλληλες ρυθμίσεις να ελέγξουν τη δημιουργία αντιτύπων (record control) βάσει των ανιχνευόμενων υδατογραφημάτων. Τέτοια συστήματα έχουν οραματιστεί οι οργανισμοί Copy Protection Technical Working Group (CPTWG) και Secure Digital Music Initiative (SDMI) για χρήση σε DVD και μουσικά αρχεία αντίστοιχα. Ανακύπτει όμως ένα ουσιαστικό πρόβλημα μη τεχνικής φύσης σχετικά με την ανάπτυξη τέτοιων συστημάτων ελέγχου, που αφορά τον τρόπο με τον οποίο θα εξασφαλιστεί η ενσωμάτωση ανιχνευτή υδατογραφημάτων στις συσκευές αντιγραφής. Όχι μόνο δεν υπάρχει ισχυρό κίνητρο για τους κατασκευαστές ώστε να επιβαρυνθούν το κόστος ενσωμάτωσης ανιχνευτών στα προϊόντα τους, αντίθετα μια τέτοια κίνηση μειώνει στην πραγματικότητα την αξία της συσκευής από την οπτική γωνία του πελάτη. Είναι αναμενόμενο ότι ο πελάτης θα προτιμήσει να αγοράσει μια συσκευή που θα του επιτρέπει τη δημιουργία αντιγράφων χωρίς περιορισμούς. Η λύση που εξετάζεται για το πρόβλημα αυτό είναι να απαιτείται ρητά από το νόμο ή

την άδεια (patent license) η ενσωμάτωση ανιχνευτή υδατογραφημάτων στις συσκευές αντιγραφής.

2.2.8 Πιστοποίηση Δεδομένων (Data Authentication)

Ο έλεγχος της ακεραιότητας των δεδομένων μέσω της χρήσης των λεγόμενων «εύθραυστων υδατογραφημάτων» αποτελεί μια δημοφιλή εφαρμογή της υδατογραφίας τα τελευταία χρόνια. Τα υδατογραφήματα αυτά κωδικοποιούν πληροφορία απαραίτητη για τον έλεγχο της αυθεντικότητας του περιεχομένου και δίνουν πληροφορίες σχετικά με το εάν και ποια τμήματα έχουν υποστεί μεταβολές, παρουσιάζοντας μικρή έως και καθόλου ανθεκτικότητα σε τυχόν τροποποιήσεις των δεδομένων που τα εμπεριέχουν. Οι απαιτήσεις ως προς την ανθεκτικότητα ποικίλλουν ανάλογα με το είδος των δεδομένων και την εφαρμογή. Πάντως, από όλες τις κατηγορίες εφαρμογών της υδατογραφίας, τα υδατογραφήματα ελέγχου ακεραιότητας δεδομένων απαιτούν εξ ορισμού το μικρότερο βαθμό ανθεκτικότητας.

Η πιστοποίηση των δεδομένων γίνεται μέχρι σήμερα κυρίως με χρήση κρυπτογραφίας. Μια συνηθισμένη προσέγγιση του προβλήματος είναι η δημιουργία ψηφιακής υπογραφής που αποτελεί ουσιαστικά μια κρυπτογραφημένη περίληψη των δεδομένων. Χρησιμοποιείται ένας αλγόριθμος κρυπτογράφησης ασύμμετρου κλειδιού, ώστε τα κλειδιά που απαιτούνται για την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος να είναι διαφορετικά. Μόνο ο εξουσιοδοτημένος αποστολέας των μηνυμάτων γνωρίζει το κατάλληλο κλειδί για τη δημιουργία των υπογραφών, επομένως εάν κάποιος τροποποιήσει το μήνυμα, δε θα είναι σε θέση να δημιουργήσει μια νέα υπογραφή που να αντιστοιχεί σε αυτό. Η σύγκριση στη συνέχεια της αρχικής υπογραφής με αυτή που προκύπτει από το ληφθέν μήνυμα φανερώνει την παραποίηση. Έχει προταθεί από τον Friedman η σχεδίαση μιας «αξιόπιστης κάμερας» («trustworthy camera») που διαθέτει ενσωματωμένο κλειδί, με το οποίο δημιουργεί ψηφιακές υπογραφές στις φωτογραφίες [28]. Η σύγκριση της υπογραφής που εξάγεται από ένα αντίγραφο εικόνας με εκείνη που αντιστοιχεί στο πρωτότυπο επιτρέπει τον έλεγχο ταυτοποίησης. Εάν δηλαδή από τη σύγκριση προκύψει ότι οι δύο υπογραφές είναι ίδιες, πιστοποιείται η ταυτοποίηση του

αντιγράφου με το πρωτότυπο. Οι υπογραφές αυτές όμως αποτελούν μεταδεδομένα (metadata) που συνοδεύουν την πληροφορία που επικυρώνουν και τα οποία μπορούν εύκολα να εξαλειφθούν. Για παράδειγμα, σε ένα σύστημα πιστοποίησης εικόνων που αποθηκεύει τα μεταδεδομένα στο πεδίο επικεφαλίδας, η μετατροπή μιας εικόνας σε μορφή (format) που δεν υποστηρίζει την ενσωμάτωση υπογραφής στην επικεφαλίδα, θα έχει ως αποτέλεσμα την απώλεια της υπογραφής και κατά συνέπεια την αδυναμία πιστοποίησης της εικόνας.

Μια αποδοτικότερη λύση αποτελεί η ενσωμάτωση της υπογραφής απευθείας στα αρχικά δεδομένα με χρήση υδατογραφίας. Η υπογραφή αυτή αναφέρεται συχνά στη βιβλιογραφία ως «σημάδι πιστοποίησης» (authentication mark). Η εισαγωγή των «σημαδιών πιστοποίησης» εξασφαλίζει τη μόνιμη σύνδεση της υπογραφής με τα αντίστοιχα δεδομένα. Πρέπει βέβαια η τροποποίηση που υφίστανται τα δεδομένα λόγω υδατογράφησης να είναι τέτοιας φύσης και έκτασης, ώστε η υπογραφή να εξακολουθεί να τους αντιστοιχεί. Αυτό επιτυγχάνεται με το διαχωρισμό τους σε δύο τμήματα, ένα από τα οποία χρησιμοποιείται για την εξαγωγή της υπογραφής, ενώ το άλλο για την ενσωμάτωσή της. Για παράδειγμα, έχει προταθεί στη βιβλιογραφία η εξαγωγή μιας υπογραφής από τα bits μεγάλης τάξης της εικόνας και η μετέπειτα ενσωμάτωσή της στα bits χαμηλής τάξης.

Η τροποποίηση δεδομένων που εμπεριέχουν κάποιο υδατογράφημα πιστοποίησης προκαλεί ταυτόχρονα και την αλλοίωση του υδατογραφήματος, από την εξέταση του οποίου προκύπτουν πληροφορίες σχετικά με τον τρόπο παραποίησης των δεδομένων. Για παράδειγμα, εάν τμηματοποιηθεί μια εικόνα σε τετραγωνίδια (blocks) και σε κάθε ένα από αυτά ενσωματωθεί το υδατογράφημα πιστοποίησης που του αντιστοιχεί, από τη σύγκρισή του αρχικού με το τοπικά εξαγόμενο υδατογράφημα αντλείται πληροφορία ως προς το ποια τμήματα της εικόνας είναι αυθεντικά και ποια έχουν αλλοιωθεί («localized authentication»). Σημειώνεται ότι το υδατογράφημα πιστοποίησης που ενσωματώνεται στα τετραγωνίδια μπορεί να περιγράφει εγγενή (intrinsic) χαρακτηριστικά των δεδομένων. Μια πληροφορία που μπορεί να προκύψει από την εξέταση τροποποιημένων υδατογραφημάτων πιστοποίησης είναι σχετικά με το εάν έχουν υποστεί τα δεδομένα συμπίεση με απώλειες. Η κβαντοποίηση που εφαρμόζεται από

τους περισσότερους αλγορίθμους συμπίεσης με απώλειες προκαλεί χαρακτηριστικές στατιστικές μεταβολές στο υδατογράφημα που μπορούν να ανιχνευτούν εύκολα. Αντίθετα, σε εφαρμογές όπου ενδιαφέρει το αν έγιναν πιο ουσιαστικές αλλαγές, όπως προσθήκη ή αφαίρεση κάποιου αντικειμένου από την εικόνα, ενδείκνυται η χρήση των λεγόμενων «ημι-εύθραυστων» (semi-fragile) υδατογραφημάτων, τα οποία αντιστέκονται σε μικρές αλλαγές (π.χ. συμπίεση με απώλειες) αλλά αλλοιώνονται από μεγαλύτερες παραποιήσεις.

2.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΥΔΑΤΟΓΡΑΦΗΜΑΤΩΝ

Τα υδατογραφικά σχήματα μπορούν να χαρακτηριστούν από διάφορες παραμέτρους. Οι τρεις βασικές παράμετροι είναι η ανθεκτικότητα, η διαφάνεια και η χωρητικότητα, αλλά υπάρχει και μία σειρά άλλων που συμπληρώνουν το χαρακτηρισμό των υδατογραφικών σχημάτων. Η σημασία κάθε ιδιότητας εξαρτάται από τις απαιτήσεις της εφαρμογής και το ρόλο του υδατογραφήματος σε αυτήν και ενδέχεται μάλιστα να αλλάζει ακόμη και η ερμηνεία της ανάλογα με την εφαρμογή. Τα πλεονεκτήματα και οι αδυναμίες μιας υδατογραφικής μεθόδου αποτιμώνται βάσει του βαθμού στον οποίο καλύπτει το σύνολο των απαιτήσεων, σε συνάρτηση πάντα με τη σχετική βαρύτητα που έχει κάθε απαίτηση για μια συγκεκριμένη εφαρμογή [17]. Παρακάτω παρουσιάζονται οι βασικές παράμετροι που χαρακτηρίζουν τα υδατογραφικά σχήματα.

2.3.1 Ανθεκτικότητα (Robustness)

Η ανθεκτικότητα αναφέρεται στη δυνατότητα ανίχνευσης του υδατογραφήματος μετά από κακόβουλες «επιθέσεις» αλλά και μετά από συνηθισμένες ενέργειες επεξεργασίας των δεδομένων, που περιλαμβάνουν στην περίπτωση των εικόνων προσθήκη τυχαίου θορύβου, γραμμικό και μη γραμμικό φιλτράρισμα, cropping, μετατροπή από ψηφιακή σε αναλογική μορφή και αντίστροφα, συμπίεση με απώλειες και γεωμετρικές μεταβολές (περιστροφή, μετάθεση, αλλαγή κλίμακας κ.λπ.).

Η ανθεκτικότητα είναι μείζονος σημασίας στα υδατογραφήματα προστασίας πνευματικών δικαιωμάτων. Όμως, αρκετές εφαρμογές δεν απαιτούν ανθεκτικότητα σε όλες τις πιθανές ενέργειες επεξεργασίας των δεδομένων. Αντίθετα, το υδατογράφημα που χρησιμοποιείται σε μια εφαρμογή πρέπει να είναι ανθεκτικό στο σύνολο των διαδικασιών επεξεργασίας που είναι πιθανό να μεσολαβήσουν από την εισαγωγή του μέχρι την ανίχνευσή του στα πλαίσια της συγκεκριμένης εφαρμογής. Σε κάποιες περιπτώσεις μάλιστα η ανθεκτικότητα μπορεί να μην έχει καμιά αξία ή ακόμη και να είναι ανεπιθύμητη. Στην πραγματικότητα, ένα σημαντικό τμήμα της έρευνας στο πεδίο της υδατογραφίας εστιάζεται στα λεγόμενα «εύθραυστα υδατογραφήματα», που σχεδιάζονται με σκοπό να μην είναι ανθεκτικά. Για παράδειγμα, τα υδατογραφήματα που προορίζονται για εφαρμογές ελέγχου ακεραιότητας δεδομένων επιβάλλεται να είναι εύθραυστα. Από την άλλη πλευρά, υπάρχουν εφαρμογές στις οποίες επιβάλλεται η χρήση υδατογραφημάτων που είναι ανθεκτικά σε οποιαδήποτε παραποίηση του σήματος, με την προϋπόθεση όμως ότι διατηρείται η αξία του έργου. Πρόκειται για περιπτώσεις όπου δεν μπορεί να προβλεφθεί η επεξεργασία που θα υποστεί το σήμα από την εισαγωγή του υδατογραφήματος μέχρι την ανίχνευσή του, ή όπου ενδέχεται να σημειωθούν κακόβουλες «επιθέσεις».

2.3.2 Χωρητικότητα (Capacity)

Η χωρητικότητα, ή αλλιώς «φορτίο» (payload), αναφέρεται στην ποσότητα της πληροφορίας που μπορεί να ενσωματωθεί στο μέσο και πιο συγκεκριμένα στον αριθμό των bits που κωδικοποιεί ένα υδατογράφημα στη μονάδα του χρόνου ή ανά πακέτο δεδομένων. Προκειμένου για εικόνες, η χωρητικότητα αναφέρεται στον αριθμό των bits του υδατογραφήματος που μπορεί να ενσωματωθεί στην εικόνα. Όσον αφορά τον ήχο, η χωρητικότητα εκφράζει τον αριθμό των ενσωματωμένων bits που μεταδίδονται ανά δευτερόλεπτο, ενώ στην περίπτωση του βίντεο αναφέρεται στο πλήθος των bits ανά καρέ (frame) ή ανά δευτερόλεπτο. Ένα υδατογραφικό σύστημα που ενσωματώνει στα δεδομένα υδατογράφημα μήκους N bits, παρέχει τη δυνατότητα κωδικοποίησης 2^N διαφορετικών μηνυμάτων. Η μεγαλύτερη

χωρητικότητα επιτρέπει τη χρήση ενός ψηφιακού αντικειμένου μικρότερου μεγέθους για την ενσωμάτωση συγκεκριμένου μηνύματος, γεγονός που συνεπάγεται μείωση του απαιτούμενου εύρους μετάδοσης.

2.3.3 Διαφάνεια (Perceptual Transparency)

Η ενσωμάτωση ενός υδατογραφήματος είναι μια διαδικασία που προσθέτει θόρυβο στα αρχικά δεδομένα και είναι σημαντικό να γίνεται χωρίς σημαντική υποβάθμιση της ποιότητας του υδατογραφούμενου μέσου [17]. Σε μια στεγανογραφική εφαρμογή όπου το ζητούμενο είναι η διεξαγωγή μυστικής επικοινωνίας μεταξύ δύο μερών, το σύστημα αποτυγχάνει στο σκοπό του εάν κάποιος τρίτος διαπιστώσει την ύπαρξη κρυφής πληροφορίας στα διακινούμενα δεδομένα, ακόμη και εάν εκείνος δεν είναι σε θέση να εξαγάγει το μήνυμα. Η απαίτηση για διαφάνεια των υδατογραφημάτων είναι πολύ σημαντική και σε πολλές κατεχοχίν υδατογραφικές εφαρμογές, όπως σε περιπτώσεις κατοχύρωσης πνευματικών δικαιωμάτων, όπου η εισαγωγή υδατογραφήματος δεν πρέπει να υποβαθμίζει στο ελάχιστο την ποιότητα του αντικειμένου. Η διαφάνεια αποδίδεται κάποιες φορές στη βιβλιογραφία με τον όρο «πιστότητα» (fidelity), που δηλώνει την ομοιότητα – όπως την αντιλαμβάνονται οι αισθήσεις – ανάμεσα στα αρχικά και τα υδατογραφημένα δεδομένα.

Η ανθεκτικότητα, η χωρητικότητα και η διαφάνεια αποτελούν τρεις αντικρουόμενες παραμέτρους που χρειάζεται να αντισταθμιστούν (trade-off) ανάλογα με τις ιδιαιτερότητες της εφαρμογής. Για παράδειγμα σε εφαρμογές όπου δεν είναι ιδιαίτερα κρίσιμη η διαφάνεια του υδατογραφήματος, υπάρχει περιθώριο αύξησης της χωρητικότητας ή / και της ανθεκτικότητας, λόγω του ότι είναι ανεκτή η παραποίηση των αρχικών δεδομένων ως ένα βαθμό. Ενδέχεται επομένως σε τέτοιες περιπτώσεις να προτιμηθούν ελαφρώς αντιληπτά υδατογραφήματα σε αντάλλαγμα μεγαλύτερης ανθεκτικότητας ή χαμηλότερου κόστους. Αντίθετα, σε εφαρμογές όπου τα αρχικά δεδομένα πρέπει να διατηρήσουν ακέραια την ποιότητά τους, είναι βασική η απαίτηση για υδατογραφήματα που δεν επηρεάζουν αισθητά την πιστότητα.

2.3.4 Αποτελεσματικότητα Ενσωμάτωσης (Embedding Effectiveness)

Ένα ψηφιακό αντικείμενο χαρακτηρίζεται υδατογραφημένο όταν η έξοδος του ανιχνευτή είναι θετική (positive detection). Βάσει του ορισμού αυτού η αποτελεσματικότητα της ενσωμάτωσης είναι η πιθανότητα ανίχνευσης του ενσωματωμένου υδατογραφήματος, που παίρνει τιμές μικρότερες από το 100%. Παρόλο που η 100% αποτελεσματικότητα είναι πάντοτε επιθυμητή, συνήθως αυτός ο στόχος έχει κόστος όσον αφορά τις άλλες απαιτήσεις. Ανάλογα με την εφαρμογή, ενδέχεται να προτιμηθεί η μείωση της αποτελεσματικότητας σε κάποιο βαθμό προκειμένου να επιτευχθεί καλύτερη απόδοση ως προς άλλες παραμέτρους. Για παράδειγμα, όταν υπάρχει η ανάγκη εισαγωγής υδατογραφημάτων κατοχύρωσης πνευματικών δικαιωμάτων σε χιλιάδες εικόνες επί καθημερινής βάσης, το υδατογραφικό σύστημα που χρησιμοποιείται πρέπει να εξασφαλίζει υψηλή πιστότητα στις υδατογραφημένες εικόνες. Σε αυτήν την περίπτωση επομένως δικαιολογείται η αδυναμία επιτυχούς υδατογράφησης περιορισμένου πλήθους εικόνων στο πλαίσιο των αυστηρών περιορισμών ως προς την ποιότητα. Το δίλημμα εάν προτιμάται η αδυναμία κατοχύρωσης της πνευματικής ιδιοκτησίας κάποιων εικόνων ή η πρόκληση μεγαλύτερης αλλοίωσης προκειμένου να εξασφαλιστεί 100% αποτελεσματικότητα ενσωμάτωσης, συνήθως καταλήγει σε επιλογή της πρώτης λύσης. Η αποτελεσματικότητα ενός υδατογραφικού σχήματος μπορεί να αποτιμηθεί αναλυτικά, καθώς επίσης και εμπειρικά, με την ενσωμάτωση ενός υδατογραφήματος σε πληθώρα εικόνων. Το ποσοστό των εικόνων που καταλήγουν σε «θετική ανίχνευση» προσεγγίζει την πιθανότητα αποτελεσματικότητας, εφόσον το πλήθος των εικόνων στο δείγμα είναι αρκετά μεγάλο και έχει την ίδια στατιστική κατανομή με τις αναμενόμενες εικόνες εφαρμογής.

2.3.5 «Ενημερωμένη» και «Τυφλή Ανίχνευση» (Informed and Blind Detection)

Τα υδατογραφικά σχήματα διακρίνονται σε δύο κατηγορίες, ανάλογα με το αν χρησιμοποιούνται ή όχι τα αρχικά δεδομένα κατά τη διαδικασία ανίχνευσης του υδατογραφήματος. Στην περίπτωση που τα αρχικά, μη υδατογραφημένα δεδομένα

απαιτούνται για την εξαγωγή του, πρόκειται για «ενημερωμένη ανίχνευση» (informed detection) και ο αντίστοιχος ανιχνευτής υδατογραφημάτων καλείται «ενημερωμένος ανιχνευτής» (informed detector). Αυτός ο όρος χρησιμοποιείται και για το χαρακτηρισμό ανιχνευτών που δεν απαιτούν πρόσβαση στο σύνολο των αρχικών δεδομένων, παρόλο που σε κάποιες πληροφορίες που προκύπτουν από αυτά. Αντιθέτως, οι ανιχνευτές που δε χρειάζονται καμία πληροφορία σχετική με τα αρχικά δεδομένα ονομάζονται «τυφλοί ανιχνευτές» (blind detectors) και η αντίστοιχη διαδικασία εξαγωγής του υδατογραφήματος καλείται «τυφλή ανίχνευση» (blind detection). Μια βασική παράμετρος που καθορίζει εάν ένα υδατογραφικό σύστημα είναι κατάλληλο για μια συγκεκριμένη εφαρμογή, είναι το εάν εφαρμόζει «τυφλή» ή «ενημερωμένη ανίχνευση». Η «ενημερωμένη ανίχνευση» μπορεί να εφαρμοστεί μόνο σε περιπτώσεις όπου είναι διαθέσιμα τα αρχικά δεδομένα, οι οποίες σαφώς μειοψηφούν σε σχέση με τις εφαρμογές όπου δεν υπάρχει καμία πληροφορία για το μη υδατογραφημένο υλικό. Σε εφαρμογές ανίχνευσης συναλλαγών (transaction tracking) είναι σύνηθες να χρησιμοποιεί τον ανιχνευτή ο πνευματικός ιδιοκτήτης των δεδομένων, προκειμένου να εντοπίσει αυτόν που διένειμε παράνομα κάποιο αντίγραφο της δουλειάς του. Προφανώς ο κάτοχος των πνευματικών δικαιωμάτων έχει στη διάθεσή του μια μη υδατογραφημένη έκδοση του έργου του, την οποία και χρησιμοποιεί στον ανιχνευτή μαζί με το παράνομο αντίγραφο. Σε μια εφαρμογή ελέγχου αντιγράφων (copy control) όμως, ο ανιχνευτής πρέπει να διανεμηθεί σε όλους τους πελάτες μαζί με τη συσκευή αντιγραφής. Σε μια τέτοια εφαρμογή η διανομή του μη υδατογραφημένου υλικού σε όλους τους ανιχνευτές όχι μόνο δε θα ήταν πρακτική, αλλά ουσιαστικά θα ακύρωνε το στόχο του υδατογραφικού συστήματος.

Στη σχετική βιβλιογραφία, τα συστήματα που χρησιμοποιούν «ενημερωμένη» ή «τυφλή ανίχνευση» ονομάζονται «ιδιωτικά» ή «δημόσια υδατογραφικά συστήματα» (private/public watermarking systems) αντίστοιχα. Αυτή η ορολογία αναφέρεται στη χρησιμότητα των συστημάτων σε εφαρμογές όπου το υδατογράφημα ανιχνεύεται μόνο από ένα περιορισμένο σύνολο ατόμων («ιδιωτική υδατογραφία») ή από τον καθένα χωρίς περιορισμό («δημόσια υδατογραφία»). Εφόσον τα αρχικά δεδομένα είναι διαθέσιμα μόνο σε «ιδιωτικές εφαρμογές», δεν

μπορούν να χρησιμοποιηθούν «ενημερωμένοι ανιχνευτές» σε «δημόσιες εφαρμογές». Πρέπει πάντως να σημειωθεί ότι στη βιβλιογραφία αποφεύγονται συνήθως οι όροι «δημόσιος» και «ιδιωτικός», λόγω της σύγχυσης που προκαλείται από τη χρήση τους και στη διάκριση των κρυπτογραφικών συστημάτων.

2.3.6 Ρυθμός Ψευδώς Θετικών (False Positive Rate)

Ο όρος «ψευδώς θετικό» (false positive) περιγράφει την ανίχνευση ενός υδατογραφήματος σε δεδομένα, χωρίς αυτό στην πραγματικότητα να υπάρχει. Ο ρυθμός ψευδώς θετικών (false positive rate) αναφέρεται στο πλήθος των ψευδών θετικών που αναμένονται σε δεδομένο αριθμό δοκιμών του ανιχνευτή. Υπάρχουν δύο διαφορετικοί ορισμοί για την «πιθανότητα ψευδώς θετικού» σε μια δοκιμή του ανιχνευτή, ανάλογα με το αν θεωρείται ως τυχαία μεταβλητή το υδατογράφημα ή το αρχικό υλικό (cover object).

Στον πρώτο ορισμό, η «πιθανότητα ψευδώς θετικού» είναι η πιθανότητα ανίχνευσης υδατογραφήματος για ένα συγκεκριμένο έργο και τυχαία επιλεγμένα υδατογραφήματα. Τα υδατογραφήματα έχουν μια κατανομή που καθορίζεται από τη σχεδίαση του συστήματος δημιουργίας υδατογραφημάτων. Συνήθως τα υδατογραφήματα προκύπτουν είτε από έναν αλγόριθμο κωδικοποίησης bit (bit-encoding algorithm), είτε από μια ανεξάρτητη γεννήτρια τυχαίων αριθμών, κατανομής Gauss. Σε πολλές περιπτώσεις η πιθανότητα ψευδώς θετικού - σύμφωνα με αυτόν τον πρώτο ορισμό - είναι στην πραγματικότητα ανεξάρτητη από το έργο και εξαρτάται μόνο από τη μέθοδο εισαγωγής του υδατογραφήματος.

Στο δεύτερο ορισμό, η πιθανότητα ψευδώς θετικού είναι η πιθανότητα ανίχνευσης υδατογραφήματος σε ένα έργο για ένα συγκεκριμένο υδατογράφημα και τυχαία επιλεγμένα έργα. Η κατανομή από την οποία επιλέγεται το έργο εξαρτάται σε πολύ μεγάλο βαθμό από την εφαρμογή. Οι φυσικές εικόνες (natural images), τα γραφικά, οι ιατρικές εικόνες, τα μουσικά βίντεο και τα βίντεο παρακολούθησης (surveillance videos) έχουν πολύ διαφορετικά στατιστικά χαρακτηριστικά μεταξύ τους. Το ίδιο ισχύει για τα διάφορα είδη μουσικής μεταξύ τους αλλά και σε σχέση με τις ραδιοφωνικές ομιλίες. Οι κατανομές αυτές είναι

πιθανό να διαφέρουν πολύ και από τα στατιστικά χαρακτηριστικά του συστήματος δημιουργίας υδατογραφήμάτων, με ενδεχόμενο αποτέλεσμα τη σημαντική διαφορά ανάμεσα στις πιθανότητες ψευδώς θετικού που προκύπτουν από τους δύο ορισμούς.

Στις περισσότερες εφαρμογές χρησιμοποιείται συνήθως ο δεύτερος ορισμός. Σε κάποιες περιπτώσεις ωστόσο είναι εξίσου σημαντικός ο πρώτος ορισμός, όπως για παράδειγμα στην περίπτωση της παρακολούθησης συναλλαγών, όπου η ανίχνευση τυχαίου υδατογραφήματος σε ένα έργο μπορεί να οδηγήσει σε εσφαλμένη κατηγορία για κλοπή. Η κατάλληλη πιθανότητα ψευδώς θετικού εξαρτάται από την εφαρμογή. Στην περίπτωση της κατοχύρωσης πνευματικών δικαιωμάτων (copyright), ο ανιχνευτής χρησιμοποιείται τόσο σπάνια που μια πιθανότητα 10^{-6} θα επαρκούσε για να θεωρηθεί το πλήθος των «ψευδώς θετικών» αμελητέο. Σε μια εφαρμογή ελέγχου αντιγράφων αντιθέτως, όπου εκτελούνται διαρκώς εκατομμύρια ανιχνεύσεις υδατογραφήμάτων σε πληθώρα έργων, η ανίχνευση πολλών «ψευδώς θετικών» σε ένα μη υδατογραφημένο έργο θα δημιουργούσε μεγάλο πρόβλημα. Για αυτόν το λόγο απαιτείται σε τέτοιες εφαρμογές να είναι απειροελάχιστος ο ρυθμός ψευδώς θετικών.

2.3.7 Ασφάλεια

Η ασφάλεια του υδατογραφικού σχήματος αναφέρεται στην ικανότητά του να αντιστέκεται στις κακόβουλες επιθέσεις, δηλαδή σε διαδικασίες προορισμένες να αποτρέψουν την υλοποίηση του στόχου του. Οι επιθέσεις εμπίπτουν σε τρεις βασικές κατηγορίες: α) μη εξουσιοδοτημένη αφαίρεση, β) μη εξουσιοδοτημένη ενσωμάτωση, γ) μη εξουσιοδοτημένη ανίχνευση. Η μη εξουσιοδοτημένη αφαίρεση και ενσωμάτωση αποτελούν τις λεγόμενες «ενεργές επιθέσεις» καθώς τροποποιούν τα δεδομένα, σε αντίθεση με τη μη εξουσιοδοτημένη ανίχνευση η οποία δεν αλλοιώνει τα δεδομένα και καλείται «παθητική επίθεση».

Η σημασία των παραπάνω επιθέσεων εξαρτάται από την εφαρμογή. Στην πραγματικότητα υπάρχουν περιπτώσεις, ελάχιστες βέβαια σε σχέση με το σύνολο των δυνατών εφαρμογών, όπου λόγω της βελτιωμένης λειτουργικότητας που προσφέρουν τα υδατογραφήματα στους – εξουσιοδοτημένους και μη – χρήστες, δεν

υπάρχει η απειλή επιθέσεων. Προκειμένου όμως για εφαρμογές που απαιτούν κάποιο επίπεδο ασφαλείας, η διάκριση ανάμεσα στους παραπάνω τύπους επιθέσεων είναι σημαντική.

Η «μη εξουσιοδοτημένη αφαίρεση» περιγράφει επιθέσεις που στοχεύουν στο να καταστήσουν ένα υδατογράφημα μη ανιχνεύσιμο. Συνήθως γίνεται διάκριση ανάμεσα σε δύο κατηγορίες μη εξουσιοδοτημένης αφαίρεσης υδατογραφήματος: τις «επιθέσεις εξάλειψης» (elimination attacks) και τις «επιθέσεις κάλυψης» (masking attacks). Η εξάλειψη του υδατογραφήματος έχει ως αποτέλεσμα να θεωρείται το έργο μη υδατογραφημένο, δηλαδή να μην είναι δυνατή η ανίχνευση του υδατογραφήματος ακόμη και από έναν πολύ καλό ανιχνευτή. Η εξάλειψη του όμως δε συνδέεται απαραίτητα με την αναπαραγωγή των αρχικών, μη υδατογραφημένων δεδομένων, αλλά με τη μετατροπή του υλικού σε μια εκδοχή που μοιάζει με το αρχικό και στην οποία δεν μπορεί να ανιχνευτεί το υδατογράφημα. Οι «επιθέσεις κάλυψης» από την άλλη μεριά, έχουν ως αποτέλεσμα να θεωρείται μεν το έργο υδατογραφημένο, αλλά να μην ανιχνεύεται το υδατογράφημα από τα υπάρχοντα συστήματα, χωρίς όμως να αποκλείεται το ενδεχόμενο ανίχνευσής του από κάποιο σύστημα με βελτιωμένα χαρακτηριστικά.

2.3.8 Υδατογραφικά Κλειδιά

Η κρυπτογραφία παρέχει ασφάλεια μέσω της χρήσης μυστικών κλειδιών· τα κλειδιά αυτά μπορούν να θεωρηθούν ως αυθαίρετες ακολουθίες bits που καθορίζουν τον τρόπο με τον οποίο κρυπτογραφούνται τα μηνύματα. Στα πιο απλά κρυπτογραφικά συστήματα τα μηνύματα μπορούν να αποκρυπτογραφηθούν μόνο με το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφησή τους («συμμετρικά κρυπτογραφικά συστήματα»). Σε πολλά υδατογραφικά συστήματα γίνεται αντίστοιχα χρήση κλειδιών για την εισαγωγή και ανίχνευση των υδατογραφημάτων.

Πριν από την ευρεία χρήση κλειδιών στην κρυπτογραφία, η ασφάλεια των περισσότερων κρυπτογραφικών αλγορίθμων βασιζόταν στο να μείνουν μυστικοί οι ίδιοι οι αλγόριθμοι, γεγονός που προκάλούσε δύο κύρια προβλήματα. Το πρώτο ήταν ότι εάν παραβιαζόταν η ασφάλεια ενός αλγορίθμου, έπρεπε να αναπτυχθεί ένας

εντελώς νέος αλγόριθμος. Το δεύτερο ήταν ότι λόγω της ανάγκης για μυστικότητα, δεν ήταν δυνατό να αποκαλυφθεί ο αλγόριθμος σε άλλους ερευνητές για μελέτη. Αυτό είχε ως αποτέλεσμα να μην επισημανθούν πολλές αδυναμίες ως προς την ασφάλεια προτού εφαρμοστούν οι αλγόριθμοι αυτοί στην πράξη. Τα παραπάνω προβλήματα έχουν πλέον αντιμετωπιστεί δραστικά με τη χρήση μυστικών κλειδιών, καθώς στις μέρες μας οι κρυπτογραφικοί αλγόριθμοι παρέχουν ασφάλεια μέσω της προστασίας του κλειδιού μόνο και όχι ολόκληρου του αλγορίθμου. Έτσι, οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης μπορούν να δημοσιοποιηθούν και να αποτιμηθούν με χρήση ενός συγκεκριμένου κλειδιού. Κάποιο άλλο κλειδί μπορεί να χρησιμοποιηθεί στη συνέχεια κατά τη χρήση του αλγορίθμου στην πράξη. Στην περίπτωση που το κλειδί αυτό διαρρεύσει, αρκεί η επιλογή ενός νέου κλειδιού, χωρίς να απαιτείται αλλαγή όλου του αλγορίθμου. Επομένως, ένας καλά σχεδιασμένος κρυπτογραφικός αλγόριθμος πρέπει να καλύπτει τις παρακάτω απαιτήσεις:

- η γνώση των αλγορίθμων κρυπτογράφησης και αποκρυπτογράφησης δεν απειλεί την ασφάλεια του συστήματος
- η ασφάλεια βασίζεται στη χρήση κλειδιών
- τα κλειδιά πρέπει να επιλέγονται από ένα μεγάλο σύνολο, ώστε να είναι πρακτικά αδύνατη η δοκιμή όλων των πιθανών επιλογών

Είναι επιθυμητή η εφαρμογή των ίδιων περιορισμών και στους υδατογραφικούς αλγορίθμους, όμως οι απαιτήσεις ως προς την ασφάλεια των υδατογραφήματων συχνά διαφέρουν από αυτές των κρυπτογραφήματων (cipher). Για αυτόν το λόγο δεν αρκεί μια απλή προσαρμογή των κρυπτογραφικών μεθόδων στην υδατογραφία. Η κρυπτογραφία χρησιμοποιείται για την αποτροπή της μη εξουσιοδοτημένης ανάγνωσης και παραποίησης των μηνυμάτων. Επομένως μπορεί να χρησιμοποιηθεί στην υδατογραφία για την αποτροπή συγκεκριμένων μορφών παθητικής επίθεσης και παραποίησης, αλλά δεν καλύπτει το θέμα της αφαίρεσης του υδατογραφήματος. Αυτό το πρόβλημα είναι αντίστοιχο με το θέμα των παρεμβολών στην επικοινωνία για στρατιωτικούς σκοπούς. Προκειμένου να αντιμετωπιστεί το πρόβλημα των παρεμβολών και παραστίτων σε στρατιωτικές

εφαρμογές, εφαρμόστηκε επικοινωνία διασποράς φάσματος (spread spectrum communications), κατά την οποία ένα σήμα στενής ζώνης (narrow-band signal) «απλώνεται» σε πολύ μεγαλύτερο εύρος. Ο ακριβής τρόπος διασποράς είναι γνωστός μόνο στον πομπό και το δέκτη. Χωρίς γνώση της συνάρτησης διασποράς είναι μάλλον απίθανο να καταφέρει κάποιος να παρέμβει ή έστω να ανιχνεύσει κάποια μετάδοση. Η συνάρτηση αυτή βασίζεται σε μια μυστική πληροφορία που αναλογεί στο κλειδί που χρησιμοποιείται στην κρυπτογραφία (αν και σπάνια αναφέρεται ως τέτοιο). Οι αλγόριθμοι υδατογραφίας μπορούν να σχεδιαστούν έτσι ώστε να χρησιμοποιούν μυστικά κλειδιά με τρόπο παρόμοιο με αυτόν που συναντάται στη διασπορά φάσματος. Για παράδειγμα, ένας απλός υδατογραφικός αλγόριθμος προσθέτει μια μορφή ψευδοτυχαίου θορύβου (PN pattern) σε εικόνες. Σε αυτήν την περίπτωση το ρόλο του μυστικού κλειδιού μπορεί να θεωρηθεί ότι έχει η μορφή του ψευδοτυχαίου θορύβου (PN pattern) ή ο «σπόρος» (seed) που χρησιμοποιήθηκε για τη δημιουργία του.

Στην ιδανική περίπτωση είναι αδύνατη η ανίχνευση της παρουσίας ενός υδατογραφήματος σε κάποιο έργο χωρίς γνώση του κλειδιού, ακόμη και όταν ο αλγόριθμος υδατογράφησης είναι γνωστός. Επίσης ιδανικά είναι εξαιρετικά δύσκολη, αν όχι αδύνατη, η αφαίρεση ενός υδατογραφήματος χωρίς σημαντική αλλοίωση στην ποιότητα του έργου, ακόμη και στην περίπτωση που το κλειδί έχει γνωστοποιηθεί σε μια έμπιστη ομάδα ανθρώπων.

Καθώς τα κλειδιά που χρησιμοποιούνται κατά την ενσωμάτωση και ανίχνευση των υδατογραφημάτων παρέχουν διαφορετικού τύπου ασφάλεια από αυτήν που προσφέρουν τα κρυπτογραφικά κλειδιά, συχνά είναι επιθυμητός ο συνδυασμός των δύο τύπων στα υδατογραφικά συστήματα για την εξασφάλιση μεγαλύτερης προστασίας. Πιο συγκεκριμένα, τα μηνύματα κρυπτογραφούνται σε πρώτη φάση με χρήση ενός κρυπτογραφικού κλειδιού (cipher key) και στη συνέχεια ενσωματώνονται στα δεδομένα με χρήση υδατογραφικού κλειδιού (watermark key).

2.3.9 Τροποποίηση Υδατογραφήματος και Πολλαπλά Υδατογραφήματα

Σε κάποιες εφαρμογές είναι επιθυμητή ή/και απαραίτητη η δυνατότητα τροποποίησης υδατογραφημάτων που έχουν ήδη ενσωματωθεί στα δεδομένα. Για παράδειγμα, η αμερικανική νομοθεσία δίνει στους τηλεθεατές το δικαίωμα να δημιουργήσουν ένα μόνο αντίγραφο των μεταδιδόμενων προγραμμάτων για λόγους μετάθεσης ώρας (time-shifting purposes), ενώ απαγορεύει τη δημιουργία επιπλέον αντιγράφων. Σε εφαρμογές ελέγχου αντιτύπων επομένως, πρέπει να υπάρχει η δυνατότητα χαρακτηρισμού του μεταδιδόμενου υλικού με την ένδειξη «ένα αντίγραφο» (copy once) και μετά την πρώτη αντιγραφή η ένδειξη να μετατρέπεται σε «κανένα αντίγραφο» (copy-no-more). Αυτή η τροποποίηση του καταγεγραμμένου βίντεο μπορεί να γίνει με διάφορους τρόπους. Ο πιο προφανής τρόπος είναι η απλή αλλαγή του ενσωματωμένου υδατογραφήματος ώστε από «copy once» να δείχνει «copy-no-more». Εάν όμως ένα υδατογράφημα είναι σχεδιασμένο ώστε να επιδέχεται εύκολα τροποποίηση, υπάρχει αυξημένος κίνδυνος για εκτεταμένες παράνομες αλλοιώσεις, όπως για παράδειγμα μετατροπή ενός υδατογραφήματος «copy once» σε «copy freely». Αντί για την τροποποίηση του υφιστάμενου υδατογραφήματος, υπάρχει η εναλλακτική λύση της πρόσθετης ενσωμάτωσης ενός δεύτερου, με την παρουσία και των δύο να δηλώνει ότι δεν επιτρέπεται η δημιουργία άλλου αντιγράφου (copy-no-more state). Αντίστροφα, η αρχική κατάσταση «ένα αντίγραφο» (copy once) μπορεί να δηλωθεί με δύο υδατογραφήματα, ένα βασικό και ένα δευτερεύον. Το δευτερεύον υδατογράφημα μπορεί να είναι ένα σχετικά εύθραυστο υδατογράφημα σε σχέση με το βασικό, και ενδεχόμενη αφαίρεσή του να δηλώνει «κανένα αντίγραφο» (copy-no-more). Αυτές οι δύο μέθοδοι εμφανίζονται να είναι ισοδύναμες εκ πρώτης όψεως, αλλά στην πραγματικότητα έχουν πολύ διαφορετικές μεταξύ τους συμπεριφορές «ψευδώς θετικού» (false positive). Η εφαρμογή τους εγείρει τεχνικές προκλήσεις, όπως την ανάγκη ενσωμάτωσης υδατογραφημάτων σε συμπίεσμένα μέσα χωρίς μεταβολή του ρυθμού μετάδοσης δεδομένων (bit rate).

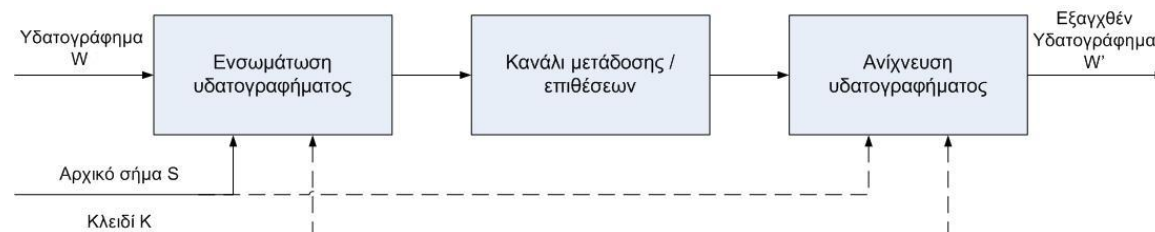
Ένα άλλο παράδειγμα για τη χρησιμότητα των πολλαπλών υδατογραφημάτων είναι αυτό των υδατογραφημάτων παρακολούθησης

συναλλαγών (transactional watermarks). Η διανομή υλικού συνήθως περιλαμβάνει πλήθος μεσαζόντων πριν από τον τελικό χρήστη. Επομένως, μια ετικέτα καταγραφής μπορεί καταρχάς να περιλαμβάνει ένα υδατογράφημα που να προσδιορίζει τον κάτοχο των πνευματικών δικαιωμάτων. Στη συνέχεια ενδέχεται να σταλεί το υλικό σε πλήθος δικτυακών τόπων. Η ενσωμάτωση ενός δεύτερου υδατογραφήματος, μοναδικού για κάθε αντίγραφο, επιτρέπει τη διάκριση των διανομέων. Τέλος, ο δικτυακός τόπος μπορεί να εισαγάγει ένα μοναδικό υδατογράφημα (fingerprint) στο υλικό που πουλάει, προκειμένου να έχει τη δυνατότητα αναγνώρισης κάθε αγοραστή.

2.4 ΤΑΞΙΝΟΜΗΣΗ ΤΕΧΝΙΚΩΝ ΥΔΑΤΟΓΡΑΦΙΑΣ

Τα τελευταία χρόνια η βιβλιογραφία εμπλουτίζεται συνεχώς με νέες υδατογραφικές τεχνικές, οι οποίες παρουσιάζουν διαφορετικά χαρακτηριστικά και προορίζονται για ποικίλες εφαρμογές. Η πλειοψηφία των προτεινόμενων μεθόδων επικεντρώνονται στην υδατογράφιση εικόνων, αν και πολλές από αυτές μπορούν να τροποποιηθούν ώστε να εφαρμοστούν και σε άλλα πολυμεσικά δεδομένα. Όλες οι τεχνικές, ανεξάρτητα από το πεδίο εφαρμογών και τα χαρακτηριστικά τους, ακολουθούν ένα γενικό υδατογραφικό μοντέλο που περιλαμβάνει τα στάδια ενσωμάτωσης και εξαγωγής του υδατογραφήματος και παρουσιάζεται στο Σχήμα 2. Όπως φαίνεται και στο σχήμα, το υδατογράφημα W ενσωματώνεται στο αρχικό σήμα S (original host signal) με προαιρετική χρήση ενός μυστικού κλειδιού K . Στην περίπτωση των εικόνων, το αρχικό σήμα S μπορεί να είναι η ένταση των pixels (spatial domain) ή οι συντελεστές κάποιου μετασχηματισμού τους (transform domain), ενώ το κλειδί K μπορεί να έχει διάφορες χρήσεις: α) να αποτελεί το «σπόρο» (seed) για τη δημιουργία ψευδοτυχαίας ακολουθίας με συγκεκριμένη κατανομή (συνήθως ομοιόμορφη ή Gauss), η οποία και θα αποτελέσει το υδατογράφημα, β) να καθορίζει τις θέσεις στις οποίες θα εισαχθεί το υδατογράφημα, γ) να αποτελεί το κλειδί με το οποίο θα κρυπτογραφηθούν τα δεδομένα προτού ενσωματωθούν, με σκοπό την αύξηση της ασφάλειας. Στη φάση εξαγωγής του υδατογραφήματος απαιτείται η γνώση του κλειδιού που χρησιμοποιήθηκε κατά την ενσωμάτωσή του,

ενώ όπως προαναφέρθηκε, η χρήση της αρχικής εικόνας είναι προαιρετική. Λόγω των περιορισμένων εφαρμογών των συστημάτων που απαιτούν γνώση της αρχικής εικόνας για την εξαγωγή του υδατογραφήματος, η μελέτη μας επικεντρώνεται στα λεγόμενα «μη ενημερωμένα» ή «τυφλά» υδατογραφικά συστήματα (blind watermarking schemes).



Σχήμα 2: Γενικό μοντέλο ψηφιακής υδατογραφίας

Οι ποικίλες υδατογραφικές τεχνικές που έχουν προταθεί μέχρι σήμερα στη βιβλιογραφία μπορούν να ταξινομηθούν με βάση το πεδίο στο οποίο πραγματοποιούνται η εισαγωγή και η εξαγωγή του υδατογραφήματος. Σύμφωνα με αυτό το κριτήριο, στην περίπτωση των εικόνων γίνεται διάκριση ανάμεσα στις τεχνικές στο πεδίο του χώρου (spatial domain techniques) και σε αυτές που εφαρμόζονται σε κάποιο πεδίο μετασχηματισμού (transform domain techniques). Οι τεχνικές στο πεδίο του χώρου ενσωματώνουν το υδατογράφημα κατευθείαν στις τιμές των pixels της εικόνας και χαρακτηρίζονται από μικρή πολυπλοκότητα και χαμηλό κόστος, αλλά και από εξαιρετικά περιορισμένη ανθεκτικότητα σε επιθέσεις. Οι τεχνικές εισαγωγής υδατογραφημάτων σε πεδίο μετασχηματισμού εφαρμόζουν κάποιο μετασχηματισμό στην αρχική εικόνα, τροποποιούν τους προκύπτοντες συντελεστές προκειμένου να ενσωματώσουν το υδατογράφημα και στη συνέχεια εφαρμόζουν τον αντίστροφο μετασχηματισμό ώστε να προκύψει η τελική, υδατογραφημένη εικόνα. Οι μετασχηματισμοί που χρησιμοποιούνται περιλαμβάνουν τους Διακριτούς Μετασχηματισμούς Συνημιτόνου (DCT), wavelet (DWT), Fourier (DFT), αλλά και λιγότερο δημοφιλείς μετασχηματισμούς, όπως Fresnel, Fourier-Mellin, fractal κ.λπ.

Τα τελευταία χρόνια παρατηρείται έντονη στροφή των ερευνητών στη σχεδίαση υδατογραφικών σχημάτων μετασχηματισμένου πεδίου, τα οποία

πλεονεκτούν σε σχέση με του χωρικού πεδίου ως προς την ανθεκτικότητα και τη διαφάνεια, λόγω μιας σειράς χαρακτηριστικών που διαθέτουν. Για παράδειγμα, ένα υδατογράφημα που ενσωματώνεται σε συντελεστές μετασχηματισμού DCT κατανέμεται σε ολόκληρη την εικόνα, γεγονός που καθιστά δύσκολο τον εντοπισμό των υδατογραφημένων περιοχών από μη εξουσιοδοτημένο χρήστη. Στην περίπτωση βέβαια εφαρμογής μετασχηματισμού κυματιδίων ή DCT σε τετραγωνίδια (block-based DCT), το υδατογράφημα επηρεάζει μόνο τη συγκεκριμένη περιοχή όπου ενσωματώθηκε.

Ο μετασχηματισμός DCT σε τετραγωνίδια αποτέλεσε δημοφιλή επιλογή για την υδατογράφιση εικόνων τα τελευταία χρόνια, καθώς σε αυτόν βασίζονται αρκετά πρότυπα συμπίεσης εικόνας και βίντεο (JPEG, MPEG κ.λπ.). Ωστόσο, νέες απαιτήσεις όπως σταδιακή και χαμηλού ρυθμού bit μετάδοση (progressive and low-bit rate transmission), διαβάθμιση ποιότητας (quality scalability) και κωδικοποίηση Περιοχής Ενδιαφέροντος (Region of Interest – ROI), οδήγησαν στην αναζήτηση πιο αποδοτικής και προσαρμόσιμης κωδικοποίησης εικόνας. Το νέο πρότυπο συμπίεσης JPEG2000 βασίζεται στο μετασχηματισμό κυματιδίων (wavelets) και στοχεύει στην πλήρωση των παραπάνω απαιτήσεων [29]. Το γεγονός αυτό, σε συνδυασμό με μια σειρά πλεονεκτημάτων του συγκεκριμένου μετασχηματισμού, έδωσαν ώθηση στη σχεδίαση υδατογραφικών σχημάτων που εφαρμόζουν Διακριτό Μετασχηματισμό Κυματιδίων (DWT). Η επιλογή πεδίων μετασχηματισμού που είναι συμβατά με τα πρότυπα συμπίεσης έχει ως αποτέλεσμα τη σχεδίαση αλγορίθμων ανθεκτικών στη συμπίεση, μέσω της αποφυγής υδατογράφισης των συντελεστών που εξαλείφονται ή κβαντοποιούνται κατά την εφαρμογή των συγκεκριμένων προτύπων [30]. Ένας πρόσθετος λόγος για τη χρήση συμβατού πεδίου μετασχηματισμού είναι το γεγονός ότι σε αρκετές εφαρμογές είναι επιθυμητή η εισαγωγή υδατογραφήματος κατευθείαν στη συμπίεσμένη μορφή των δεδομένων. Σε μια εφαρμογή βίντεο για παράδειγμα, όπου πιθανότατα έχει προηγηθεί συμπίεση με χρήση κάποιου προτύπου όπως το MPEG-2, ενδέχεται να είναι επιθυμητή η εισαγωγή υδατογραφήματος απευθείας στη συμπίεσμένη ακολουθία bit.

Με δεδομένη την απαίτηση για όσο το δυνατό πιο ανθεκτικό και διαφανές υδατογράφημα στην πλειοψηφία των εφαρμογών, ένα αποδοτικό υδατογραφικό

σύστημα δεν μπορεί παρά να εκμεταλλεύεται, άμεσα ή έμμεσα, τα χαρακτηριστικά της ανθρώπινης αντιληπτικότητας. Έχουν αναπτυχθεί κάποια «οπτικά μοντέλα» (visual models) που στηρίζονται στην ιδιότητα του ανθρώπινου οπτικού συστήματος να επεξεργάζεται ανεξάρτητα συγκεκριμένες ζώνες συχνοτήτων. Οι μετασχηματισμένες μορφές των εικόνων, με την ανάλυση σε επίπεδο συχνότητας που παρέχουν, αποτελούν πρόσφορο πεδίο για την αξιοποίηση των οπτικών μοντέλων και διευκολύνουν βάσει αυτών την επιλογή των κατάλληλων για υδατογράφιση περιοχών συχνοτήτων. Οι συνιστώσες χαμηλών και μεσαίων συχνοτήτων αντιπροσωπεύουν το τμήμα της εικόνας που γίνεται κυρίως αντιληπτό από το μάτι. Αυτός είναι και ο λόγος που οι αλγόριθμοι συμπίεσης και οι διάφορες ενέργειες επεξεργασίας εικόνας δεν μπορούν να τροποποιήσουν σε μεγάλο βαθμό αυτό το κομμάτι χωρίς να αλλοιώσουν το αισθητικό αποτέλεσμα. Επομένως, η προσθήκη του υδατογραφήματος στους σημαντικούς συντελεστές μετασχηματισμού αυξάνει την ανθεκτικότητά του. Σημειώνεται ότι προκειμένου για μεθόδους στο πεδίο του χώρου, χρειάζεται έμμεση μοντελοποίηση των συνιστωσών χαμηλών συχνοτήτων της αρχικής εικόνας, που είναι αρκετά δύσκολη διαδικασία.

Πολλές υδατογραφικές τεχνικές μετασχηματισμένου πεδίου βασίζονται στο διαχωρισμό των σημαντικών από άποψη αισθητικού αποτελέσματος συνιστωσών (perceptually significant coefficients) από αυτές που δεν επηρεάζουν αισθητά το οπτικό αποτέλεσμα. Ο Cox και οι συνεργάτες του για παράδειγμα, πρότειναν την εισαγωγή του υδατογραφήματος στους αισθητικά σημαντικούς συντελεστές της εικόνας, λόγω της αυξημένης πιθανότητας που έχουν να διατηρηθούν αναλλοίωτοι μετά από συνηθισμένη επεξεργασία [6]. Στην ιδανική περίπτωση οι σημαντικοί από άποψη αισθητικού αποτελέσματος συντελεστές μεταβάλλονται μόνο όταν η εικόνα υποστεί επεξεργασία που να προκαλεί ορατή αλλοίωσή της. Όπως προαναφέρθηκε, οι πιο συνηθισμένες ενέργειες επεξεργασίας εικόνων – που αφορούν τη συμπίεση, μετάδοση και απεικόνισή τους – σχεδιάζονται με τέτοιο τρόπο ώστε να διατηρούν αναλλοίωτους τους αισθητικά σημαντικούς συντελεστές, δικαιώνοντας έτσι το χαρακτηρισμό τους ως αξιόπιστη επιλογή για υδατογράφιση. Από την άλλη μεριά, στις περισσότερες εφαρμογές απαιτείται το υδατογράφημα να παραμένει αναλλοίωτο στην εικόνα μόνο εφόσον η ίδια εικόνα δεν έχει αλλοιωθεί σε τέτοιο

βαθμό ώστε να χάνει τη χρηστική ή αισθητική της αξία. Επομένως στην πράξη δεν ενδιαφέρει συνήθως η διατήρηση του υδατογραφήματος όταν οι αισθητικά σημαντικοί συντελεστές έχουν υποστεί σοβαρές αλλοιώσεις. Σε μια εφαρμογή κατοχύρωσης πνευματικής ιδιοκτησίας για παράδειγμα, το υδατογράφημα χάνει την αξία του όταν η εικόνα αλλοιωθεί σε τέτοιο βαθμό ώστε να μην τίθεται πλέον θέμα πνευματικών δικαιωμάτων [16].

Μια κρίσιμη παράμετρος που πρέπει να ληφθεί υπόψη κατά την υδατογράφιση των αισθητικά σημαντικών συντελεστών είναι η διαφάνεια του υδατογραφήματος, καθώς η χρήση τους αυξάνει τον κίνδυνο πρόκλησης ορατής αλλοίωσης στην τελική εικόνα. Υπάρχουν εξάλλου στη βιβλιογραφία τεχνικές οι οποίες υδατογραφούν τους υψίσυχνους συντελεστές που αντιστοιχούν σε ακμές και λεπτομέρειες, αξιοποιώντας το γεγονός ότι οι μεταβολές τους δε γίνονται εύκολα αντιληπτές από το ανθρώπινο μάτι [9], [31], [32], [33]. Είναι σαφές επομένως ότι απαιτείται προσεκτική επιλογή των υδατογραφούμενων συντελεστών προκειμένου να επιτευχθεί εξισορρόπηση μεταξύ των αντιφατικών παραμέτρων της ανθεκτικότητας και της διαφάνειας του υδατογραφήματος.

Στο προαναφερθέν υδατογραφικό σχήμα του Cox και των συνεργατών του, ο συνδυασμός ανθεκτικότητας και διαφάνειας επιδιώκεται μέσω διαμόρφωσης *ευρέος φάσματος* (spread spectrum coding), που επιτρέπει την κατανομή του υδατογραφήματος σε ένα μεγάλο πλήθος αισθητικά σημαντικών συντελεστών στο πεδίο της συχνότητας [6]. Πιο συγκεκριμένα η τεχνική περιλαμβάνει την εφαρμογή Διακριτού Μετασχηματισμού Συνημιτόνου (DCT) σε ολόκληρη την εικόνα και την ενσωμάτωση του υδατογραφήματος – μιας ακολουθίας Gauss – στους χαμηλόσυχνους συντελεστές DCT. Η διαδικασία αυτή επιτρέπει την κατανομή χαμηλού ποσοστού από την ενέργεια του υδατογραφήματος σε κάθε συχνότητα, προκαλώντας έτσι μικρή και άρα μη αντιληπτή μεταβολή σε κάθε συντελεστή.

Μια εναλλακτική προσέγγιση αποτελεί η υδατογράφιση συντελεστών που έχουν μέτρια συμβολή στο αισθητικό αποτέλεσμα της εικόνας. Λόγω του περιορισμένου βαθμού επίδρασής τους στην εικόνα, οι συντελεστές αυτοί μπορούν να ενσωματώσουν υδατογραφήματα που πληρούν το κριτήριο της διαφάνειας. Επιπλέον χαρακτηρίζονται από σχετική ανθεκτικότητα, καθώς είναι αρκετά

σημαντικοί από αισθητικής άποψης ώστε να μην εξαλείφονται από τις συνηθισμένες ενέργειες επεξεργασίας των εικόνων. Πολλές τεχνικές χρησιμοποιούν τις μεσαίες συχνότητες για την υδατογράφιση εικόνων, αποφεύγοντας τόσο τις χαμηλές συχνότητες που επηρεάζουν έντονα το αισθητικό αποτέλεσμα, όσο και τις αναξιόπιστες από άποψη ανθεκτικότητας υψηλές συχνότητες [34], [35].

Υπάρχει όμως και η δυνατότητα εφαρμογής πιο σύνθετων μοντέλων αντίληψης (perceptual models) προκειμένου να καθοριστεί η μέγιστη δυνατή ένταση (strength) του υδατογραφήματος που δεν προκαλεί ορατές αλλοιώσεις. Η ένταση του υδατογραφήματος μπορεί να είναι σταθερή σε ολόκληρη την εικόνα ή να μεταβάλλεται σε διαφορετικές θέσεις στο χωρικό ή μετασχηματισμένο πεδίο. Αποτελεί για παράδειγμα συνήθη πρακτική να καθορίζεται η ένταση του υδατογραφήματος που θα ενσωματωθεί σε ένα συντελεστή μετασχηματισμού βάσει του μεγέθους του συγκεκριμένου συντελεστή. Πολλές είναι οι τεχνικές που προτείνουν τον καθορισμό της έντασης του υδατογραφήματος ως ποσοστού της έντασης του αρχικού σήματος στη συγκεκριμένη θέση, έτσι ώστε ένα ισχυρό σήμα να ενσωματώνει επίσης ισχυρό υδατογράφημα. Η επιλογή της έντασης του υδατογραφήματος βάσει χαρακτηριστικών τοπικών ή από ολόκληρη την εικόνα οδηγεί σε υδατογραφικά σχήματα που εξαρτώνται από τις εικόνες (image-adaptive schemes). Τα σχήματα αυτά ενσωματώνουν σε εικόνες με χαμηλή υφή (texture) και λίγες λεπτομέρειες ασθενέστερα υδατογραφήματα από ό,τι στην περίπτωση εικόνων υψηλών λεπτομερειών και σύνθετης υφής, όπου μπορεί να αποκρυφτεί αποτελεσματικά ένα πιο ισχυρό υδατογράφημα [30].

Είναι εφικτή η εφαρμογή μοντέλων αντίληψης και σε τεχνικές χωρικού πεδίου, με μεγαλύτερη δυσκολία ωστόσο σε σχέση με τις τεχνικές σε πεδίο μετασχηματισμού. Στο πεδίο του χώρου, η επιλογή των κατάλληλων για υδατογράφιση θέσεων μπορεί να γίνει βάσει κριτηρίων ανθρώπινης αντιληπτικότητας, εξετάζοντας για παράδειγμα την τοπική δραστηριότητα της εικόνας. Ενδεικτικά αναφέρεται ο υπολογισμός της διασποράς (variance) σε επίπεδο τετραγωνιδίων (local blocks) και η υδατογράφιση των τετραγωνιδίων εκείνων για τα οποία η διασπορά υπερβαίνει μια συγκεκριμένη εμπειρική τιμή κατωφλίου. Με αυτόν τον τρόπο αποκλείονται από τη διαδικασία υδατογράφισης οι περιοχές της

εικόνας με σχετικά χαμηλή δραστηριότητα (smooth blocks), καθώς μια μεταβολή σε αυτές θα μπορούσε να γίνει εύκολα αντιληπτή. Άλλες τεχνικές χωρικού πεδίου χρησιμοποιούν ως υδατογράφημα ένα πρότυπο υφής (textured pattern) που προσεγγίζει την υφή της περιοχής όπου ενσωματώνεται [30].

Εκτός όμως από την επιλογή του πεδίου μετασχηματισμού στο οποίο θα γίνει η υδατογράφιση, βασικά στοιχεία ενός υδατογραφικού σχήματος είναι επίσης η **μορφή** του υδατογραφήματος και φυσικά ο **κανόνας ενσωμάτωσής** του (embedding rule).

Η μορφή του υδατογραφήματος εξαρτάται από την εκάστοτε εφαρμογή και σε πολλές περιπτώσεις εξυπηρετεί η χρήση μιας ψευδοτυχαίας ακολουθίας ανεξάρτητων και ομοιόμορφα κατανεμημένων δειγμάτων. Η επιλογή μιας τέτοιας ακολουθίας είναι συμβατή με την προσέγγιση της υδατογραφίας από τη σκοπιά των επικοινωνιών, σύμφωνα με την οποία η υδατογράφιση θεωρείται ως μετάδοση ενός ασθενούς σήματος πάνω από ένα κανάλι με πολύ θόρυβο, όπου εφαρμόζονται κυρίως τεχνικές «διασποράς φάσματος» (spread spectrum techniques). Η ψευδοτυχαία ακολουθία συνήθως δημιουργείται με χρήση μυστικού κλειδιού για την ασφάλεια του συστήματος. Σε κάποιες εφαρμογές το υδατογράφημα αντιστοιχεί σε μια εικόνα που περιέχει στοιχεία πνευματικής ιδιοκτησίας, λογότυπα, σειριακούς αριθμούς κ.λπ. Σε αυτές τις περιπτώσεις μπορεί να εφαρμοστεί μια συνάρτηση κωδικοποίησης βάσει κλειδιού (key-dependent scrambling function) στο υδατογράφημα πριν από την εισαγωγή του, ώστε τελικά το σήμα που θα ενσωματωθεί να προσεγγίζει μια ψευδοτυχαία ακολουθία.

Οι περισσότερες υδατογραφικές τεχνικές εμπίπτουν σε δύο κατηγορίες, τις λεγόμενες *αθροιστικές* και *πολλαπλασιαστικές τεχνικές*. Οι αθροιστικές ενσωματώνουν στο αρχικό σήμα f μια ακολουθία αριθμών w_i μήκους N σύμφωνα με την Εξίσωση (2.1):

$$f'(m, n) = f(m, n) + a \cdot w_i \quad (2.1)$$

όπου a είναι η παράμετρος που καθορίζει την ένταση του υδατογραφήματος και f' το υδατογραφημένο σήμα.

Στις *πολλαπλασιαστικές τεχνικές* η διαδικασία υδατογράφισης περιγράφεται από την εξίσωση:

$$f'(m, n) = f(m, n) \cdot (1 + a \cdot w_i) \quad (2.2)$$

Η παραπάνω εξίσωση έχει τη χρήσιμη ιδιότητα ότι επιτρέπει την εύκολη εξαγωγή του υδατογραφήματος w^* από το υδατογραφημένο σήμα f εν γνώσει του αρχικού σήματος f μέσω της εξίσωσης:

$$w_i^* = \frac{f^*(m, n) - f(m, n)}{a \cdot f(m, n)} \quad (2.3)$$

Μετά την εξαγωγή του υδατογραφήματος w^* ακολουθεί η σύγκρισή του με το αρχικό υδατογράφημα w χρησιμοποιώντας την κανονικοποιημένη συσχέτιση ως κριτήριο ομοιότητας:

$$\delta = \frac{w^* \cdot w}{\|w^*\| \cdot \|w\|} \quad (2.4)$$

Η ομοιότητα δ κυμαίνεται στο διάστημα $[-1, 1]$ και μια τιμή κοντά στο 1 δηλώνει ότι το εξαχθέν υδατογράφημα w^* προσεγγίζει το υδατογράφημα αναφοράς w και άρα ότι η εικόνα έχει υδατογραφηθεί με το w . Η απόφαση για την ανίχνευση ή μη του υδατογραφήματος λαμβάνεται συνήθως βάσει μια τιμής κατωφλίου τ , την οποία και θα πρέπει να υπερβαίνει η παράμετρος δ προκειμένου να θεωρηθεί ότι το υδατογράφημα έχει ενσωματωθεί. Η τιμή του κατωφλίου τ μπορεί να προκύψει είτε πειραματικά παρατηρώντας τη συσχέτιση τυχαίων ακολουθιών, είτε αναλυτικά. Η επιλογή του κατωφλίου επηρεάζει τις πιθανότητες ψευδώς θετικού (false positive) και ψευδώς αρνητικού (false negative) και υπάρχουν στη βιβλιογραφία αρκετές μελέτες για αξιόπιστο υπολογισμό κατωφλίων συσχέτισης και αποδοτικά συστήματα ανίχνευσης υδατογραφήματος [36], [37]. Πρέπει πάντως να σημειωθεί ότι η διαδικασία που περιγράφηκε παραπάνω βρίσκει εφαρμογή σε «ενημερωμένα» (non-blind) υδατογραφικά σχήματα που εξετάζουν την ύπαρξη ή μη ενός συγκεκριμένου υδατογραφήματος στα δεδομένα.

Το βασικό πλεονέκτημα των αθροιστικών υδατογραφικών μεθόδων (εξ. 2.1) αποτελεί η χαμηλή πολυπλοκότητά τους. Τα αθροιστικά υδατογραφήματα χρησιμοποιούνται κυρίως στο πεδίο του χώρου, όπου ένα υδατογράφημα ενσωματώνεται χωρίς να γίνει αντιληπτό προσαρμόζοντας κατάλληλα την ένταση a στα τοπικά χαρακτηριστικά της αρχικής εικόνας.

Αντίθετα, οι τεχνικές που εφαρμόζονται σε πεδία μετασχηματισμού υιοθετούν συνήθως πολλαπλασιαστικό κανόνα υδατογράφησης. Αυτό οφείλεται κυρίως στο χαρακτηριστικό «επικάλυψης» (masking) του ανθρώπινου οπτικού συστήματος, δηλαδή στο γεγονός ότι το μάτι διακρίνει δύσκολα μια διαταραχή σε συγκεκριμένη συχνότητα, όταν η εικόνα περιέχει ήδη συνιστώσα της ίδιας συχνότητας. Επομένως η εισαγωγή υδατογραφήματος που έχει ενέργεια ανάλογη με αυτήν της εικόνας σε συγκεκριμένη συχνότητα, δε γίνεται εύκολα αντιληπτή από τον άνθρωπο. Ένα άλλο πλεονέκτημα του πολλαπλασιαστικού τύπου είναι το γεγονός ότι το υδατογράφημα εξαρτάται από την εικόνα, με αποτέλεσμα την αυξημένη προστασία του συστήματος από επιθέσεις που στοχεύουν στον υπολογισμό του υδατογραφήματος μέσω της σύγκρισης (averaging) ενός συνόλου υδατογραφημένων εικόνων.

Υπάρχει και μια τρίτη κατηγορία υδατογραφικών αλγορίθμων, οι οποίοι αντικαθιστούν ένα υποσύνολο των αρχικών δεδομένων με νέες τιμές. Στην πράξη όμως αυτή η κατηγορία προσεγγίζει αρκετά τον αθροιστικό τύπο που προαναφέρθηκε. Ενδεικτικό παράδειγμα αποτελούν οι αλγόριθμοι που εφαρμόζονται στο πεδίο DCT σε επίπεδο τετραγωνιδίων (block-based DCT domain), όπου κάποιοι DCT συντελεστές τροποποιούνται ανάλογα με την τιμή του υδατογραφήματος. Έχουν για παράδειγμα προταθεί ιδέες όπως η αντικατάσταση συντελεστών μετασχηματισμού ή η τροποποίησή τους έτσι ώστε να προκύψει μια συγκεκριμένη σχέση στη σειρά ταξινόμησή τους. Το τελευταίο διάστημα κερδίζουν έδαφος τα σχήματα κβαντοποίησης, τα οποία εφαρμόζουν μη γραμμικές τροποποιήσεις στην εικόνα και επιτρέπουν την ανίχνευση του υδατογραφήματος μέσω κβαντοποίησης των συντελεστών και απεικόνισής τους στο κοντινότερο σημείο ανακατασκευής (reconstruction point).

Πρέπει να σημειωθεί ότι οι τρεις γενικοί τύποι υδατογράφησης που προαναφέρθηκαν αντιπροσωπεύουν την πλειοψηφία των υδατογραφικών μεθόδων, αλλά σαφώς δεν καλύπτουν όλο το φάσμα.

Γενικά τα ποικίλα υδατογραφικά σχήματα που έχουν παρουσιαστεί μπορούν να ταξινομηθούν, με βάση και τα παραπάνω, ανάλογα με:

α) το πεδίο εισαγωγής / εξαγωγής του υδατογραφήματος:

- σχήματα χωρικού πεδίου
- σχήματα μετασχηματισμένου πεδίου (DCT, DFT, DWT, Fourier-Mellin κ.λπ.)

β) τη διαθεσιμότητα ή μη κάποιων δεδομένων αναφοράς (π.χ. της αρχικής εικόνας) στη φάση εξαγωγής του υδατογραφήματος:

- «μη ενημερωμένα» ή «τυφλά» (blind) σχήματα
- «ημι-ενημερωμένα» (semi-blind) σχήματα
- «ενημερωμένα» σχήματα

γ) τη μέθοδο ενσωμάτωσης του υδατογραφήματος στα αρχικά δεδομένα

- αθροιστικού τύπου
- πολλαπλασιαστικού τύπου
- μη γραμμικής κβαντοποίησης και αντικατάστασης

δ) την προσέγγιση της μοντελοποίησης των αισθήσεων (perceptual modeling strategy)

- χωρίς μοντελοποίηση
- έμμεση μοντελοποίηση μέσω ιδιοτήτων μετασχηματισμένου πεδίου
- άμεση μοντελοποίηση των ιδιοτήτων του ανθρώπινου οπτικού συστήματος (ή γενικότερα του συστήματος ανθρώπινης αντίληψης, προκειμένου για πολυμεσικά δεδομένα)

ε) το σκοπό της υδατογραφικής εφαρμογής

- προστασία πνευματικών δικαιωμάτων, ανίχνευση συναλλαγών
- έλεγχος αυθεντικότητας δεδομένων, ανίχνευση μεταβολών
- απόκρυψη δεδομένων, εισαγωγή επικεφαλίδων και σχολίων κ.λπ.

στ) τον τύπο των αρχικών δεδομένων (εικόνα, βίντεο, ήχος κ.λπ.)

2.5 ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

Στην ενότητα αυτή επιχειρείται η ανασκόπηση της πλούσιας σχετικής βιβλιογραφίας μέσω της παρουσίασης κάποιων βασικών και αντιπροσωπευτικών υδατογραφικών σχημάτων.

Δύο από τα κλασικά πλέον σχήματα της βιβλιογραφίας είναι αυτά που προτάθηκαν από τις ερευνητικές ομάδες των Cox και Koch, τα οποία εφαρμόζονται στο πεδίο του Διακριτού Μετασχηματισμού Συνημιτόνου και βασίζονται σε αλγορίθμους προσθετικού τύπου και κβαντοποίησης αντίστοιχα.

Στις τεχνικές διασποράς φάσματος (spread spectrum techniques), ένα σήμα στενής ζώνης που αντιπροσωπεύει το μήνυμα που θα μεταδοθεί, διαμορφώνεται από ένα φέρον ευρείας ζώνης, με αποτέλεσμα τη «διεύρυνση» του αρχικού φάσματος. Το σχήμα του Cox και των συνεργατών του αποτελεί την πιο γνωστή υδατογραφική τεχνική ευρέος φάσματος [6] και κατανέμει το υδατογράφημα σε ένα μεγάλο πλήθος αισθητικά σημαντικών συντελεστών στο πεδίο της συχνότητας. Πιο συγκεκριμένα, οι ερευνητές προτείνουν την εφαρμογή Διακριτού Μετασχηματισμού Συνημιτόνου (DCT) σε ολόκληρη την εικόνα και την ενσωμάτωση του υδατογραφήματος, που αποτελείται από μια ακολουθία Gauss 1000 bits, σε ισάριθμους συντελεστές DCT χαμηλής συχνότητας. Η ανίχνευση του υδατογραφήματος προκύπτει από τη συσχέτιση της ακολουθίας Gauss με τους υδατογραφημένους συντελεστές DCT, από τους οποίους αφαιρούνται προηγουμένως οι αντίστοιχοι συντελεστές της αρχικής εικόνας. Η προτεινόμενη διαμόρφωση ευρέος φάσματος (spread spectrum coding) επιτρέπει την κατανομή χαμηλού ποσοστού από την ενέργεια του υδατογραφήματος σε κάθε συχνότητα και κατά συνέπεια προκαλεί αρκετά μικρή και άρα μη αντιληπτή μεταβολή σε κάθε συντελεστή.

Η μέθοδος που προτάθηκε από τους Koch και Zhao [12] ήταν μία από τις πρώτες που εφάρμοσαν υδατογράφιση στο πεδίο μετασχηματισμού του Διακριτού Μετασχηματισμού Συνημιτόνου (DCT). Στη συγκεκριμένη μέθοδο εφαρμόζεται σε τυχαία τετραγωνίδια (blocks) 8x8 pixels της εικόνας μετασχηματισμός DCT και κβαντοποίηση κατά το πρότυπο JPEG και από καθένα από αυτά επιλέγεται ένα ζεύγος συντελεστών DCT μεσαίων συχνοτήτων για ενσωμάτωση 1 bit υδατογραφήματος. Η χρήση των μεσαίων συχνοτήτων στοχεύει στην ανθεκτικότητα ως προς τη συμπίεση JPEG, ενώ οι συντελεστές DC εξαιρούνται από τη διαδικασία υδατογράφισης προκειμένου να αποφευχθούν ορατές αλλοιώσεις. Η υδατογράφιση γίνεται με βάση τη διαφορά μεταξύ των επιλεχθέντων ανά μπλοκ συντελεστών: για

κάθε bit υδατογραφήματος, το αντίστοιχο ζεύγος συντελεστών τροποποιείται βάσει μιας προσέγγισης ελαχιστοποίησης του μέσου τετραγωνικού σφάλματος, ώστε από τη διαφορά τους να προκύπτει η τιμή του bit σύμφωνα με τη σχέση:

$$\Delta = \begin{cases} > p & \text{εάν } w_i = 1 \\ < -p & \text{εάν } w_i = 0 \end{cases} \quad (2.5)$$

όπου p η παράμετρος που καθορίζει την ένταση του υδατογραφήματος. Σε μεταγενέστερο άρθρο τους οι ερευνητές αποκλείουν από τη διαδικασία υδατογράφησης κάποια τετραγωνίδια ή συντελεστές βάσει συγκεκριμένων κριτηρίων ανθεκτικότητας και διαφάνειας [38]. Στην ίδια εργασία παρουσιάζουν μια παραλλαγή της παραπάνω τεχνικής που χρησιμοποιεί τρεις συντελεστές ανά μπλοκ αντί για δύο και όπου χρησιμοποιείται η σειρά ταξινόμησης (rank ordering) των συντελεστών για την αναπαράσταση των τιμών των bits του υδατογραφήματος.

Ο Swanson κ.ά. προτείνουν δύο υδατογραφικά σχήματα που αξιοποιούν τα χαρακτηριστικά του ανθρώπινου οπτικού συστήματος προκειμένου να ενσωματώσουν ανθεκτικά και ταυτόχρονα μη αντιληπτά υδατογραφήματα [39]. Στο πρώτο σχήμα επιλέγονται για υδατογράφηση τετραγωνίδια (blocks) ποικίλων διαστάσεων της εικόνας. Η ενσωμάτωση του υδατογραφήματος μπορεί να γίνει είτε σε ολόκληρη την εικόνα είτε σε συγκεκριμένες περιοχές ή αντικείμενα, παρέχοντας έτσι τη δυνατότητα προσθήκης επεξηγήσεων σε τοπικά χαρακτηριστικά. Το σχήμα περιλαμβάνει χρήση ψευδοτυχαίας ακολουθίας για διαμόρφωση ευρέος φάσματος (spread spectrum) του υδατογραφήματος και αξιοποίηση της «χωρικής επικάλυψης» (spatial mask) στον υπολογισμό της μέγιστης επιτρεπόμενης αλλαγής στα τετραγωνίδια. Το δεύτερο σχήμα χρησιμοποιεί επίσης τετραγωνίδια ποικίλων διαστάσεων και διαμόρφωση ευρέος φάσματος, αλλά σε αυτήν την περίπτωση εφαρμόζεται μετασχηματισμός DCT και τροποποιούνται οι προκύπτοντες συντελεστές αξιοποιώντας το χαρακτηριστικό «επικάλυψης συχνοτήτων» (frequency masking) του ανθρώπινου ματιού.

Οι Wu και Liu προτείνουν ένα «τυφλό» υδατογραφικό σχήμα που στοχεύει στην πιστοποίηση εικόνας, ενσωματώνοντας σε αυτήν ένα λογότυπο και κάποια βασικά χαρακτηριστικά της [40]. Ακολουθώντας το πρότυπο συμπίεσης JPEG, εφαρμόζεται μετασχηματισμός DCT σε τετραγωνίδια της εικόνας και η

υδατογράφιση γίνεται στους συντελεστές DCT βάσει ενός πίνακα αντιστοίχισης (look-up table, LUT). Ο πίνακας αυτός αντιστοιχίζει τυχαία όλες τις πιθανές τιμές των συντελεστών DCT στο 0 ή στο 1 και η ενσωμάτωση ενός δυαδικού bit σε ένα συντελεστή γίνεται με βάση την τιμή που του αντιστοιχεί στον πίνακα. Εάν το προς ενσωμάτωση bit διαφέρει από αυτήν, ο συντελεστής παίρνει την τιμή του πιο κοντινού του που έχει την επιθυμητή αντιστοίχιση στον πίνακα.

Οι Zeng και Liu εξετάζουν τις αδυναμίες προγενέστερων υδατογραφικών τεχνικών σε εφαρμογές κατοχύρωσης πνευματικής ιδιοκτησίας και τονίζουν την ανάγκη σχεδίασης «τυφλών» υδατογραφικών σχημάτων [41]. Στο προτεινόμενο από αυτούς σχήμα χρησιμοποιείται στο ρόλο της προς εξέταση υπογραφής μια ψευδοτυχαία ακολουθία, η οποία διαμορφώνεται μέσω μιας συνάρτησης και στη συνέχεια προστίθεται στην εικόνα. Η ανίχνευση της υπογραφής γίνεται μέσω της συσχέτισης της υδατογραφημένης εικόνας με κατάλληλα επιλεγμένη ψευδοτυχαία ακολουθία. Στην ίδια εργασία οι ερευνητές εφαρμόζουν το σχήμα τους στο πεδίο μετασχηματισμού DCT, επιλέγοντας τη συνάρτηση διαμόρφωσης βάσει του χαρακτηριστικού μειωμένης ευαισθησίας του ματιού σε συγκεκριμένες συχνότητες.

Η Fridrich προτείνει ένα υβριδικό «τυφλό» υδατογραφικό σχήμα, το οποίο αξιοποιεί την αυξημένη ανθεκτικότητα που προκύπτει από το συνδυασμό υδατογράφισης χαμηλών συχνοτήτων και διαμόρφωσης ευρέος φάσματος [42]. Το σχήμα εφαρμόζει Διακριτό Μετασχηματισμό Συνημιτόνου σε όλη την εικόνα, υδατογραφεί σε πρώτη φάση τους συντελεστές DCT χαμηλών συχνοτήτων και στη συνέχεια προσθέτει ένα σήμα ευρέος φάσματος στους συντελεστές μεσαίων συχνοτήτων, αποφεύγοντας έτσι την αλληλεπίδραση των δύο υδατογραφημάτων λόγω της ενσωμάτωσής τους σε διαφορετικές περιοχές συχνοτήτων. Για την υδατογράφιση των χαμηλών συχνοτήτων χρησιμοποιείται ειδική συνάρτηση κβαντοποίησης, ενώ οι παράμετροι που ρυθμίζουν την ένταση και των δύο υδατογραφημάτων καθορίζονται εφαρμόζοντας μοντέλο «χωρικής απόκρυψης» (spatial masking) του ματιού. Η ανίχνευση των υδατογραφημάτων γίνεται βάσει της συσχέτισης και το προτεινόμενο σχήμα παρουσιάζεται ως ανθεκτικό σε πληθώρα επιθέσεων, όπως για παράδειγμα σε βαθυπερατό φιλτράρισμα, συμπίεση JPEG, προσθήκη θορύβου, τροποποίηση ιστογράμματος κ.λπ.

Όπως προαναφέρθηκε, τα ποικίλα πλεονεκτήματα του μετασχηματισμού κυματιδίων έδωσαν μεγάλη ώθηση στη σχεδίαση και ανάπτυξη υδατογραφικών αλγορίθμων που βασίζονται σε αυτόν, με αποτέλεσμα τον εντυπωσιακό εμπλουτισμό της σχετικής βιβλιογραφίας κατά τα τελευταία χρόνια.

Οι Kundur και Hatzinakos [43] προτείνουν ένα «ενημερωμένο» (non-blind) υδατογραφικό σχήμα που βασίζεται σε τεχνικές πολυδιακριτής σύντηξης (multiresolution fusion) εικόνων και στη μοντελοποίηση του ανθρώπινου οπτικού συστήματος. Συγκεκριμένα εφαρμόζεται Διακριτός Μετασχηματισμός Κυματιδίων (DWT) τόσο στην εικόνα όσο και στον πίνακα που αντιπροσωπεύει το υδατογράφημα και ακολουθεί σύντηξη των DWT συντελεστών τους, ρυθμίζοντας την ένταση του υδατογραφήματος βάσει της ευαισθησίας του ματιού στις διάφορες συχνότητες. Η ανίχνευση του υδατογραφήματος απαιτεί τη γνώση της αρχικής εικόνας, γεγονός το οποίο, αν και δεν αποτρέπει τη χρήση του σχήματος για κατοχύρωση πνευματικής ιδιοκτησίας, περιορίζει την εφαρμοσιμότητά του σε άλλες εφαρμογές.

Οι ίδιοι ερευνητές προτείνουν σε επόμενο άρθρο τους ένα «τυφλό» σχήμα που επιτρέπει την εισαγωγή υδατογραφήματος στους συντελεστές κυματιδίων μιας εικόνας με χρήση κατάλληλης συνάρτησης κβαντοποίησης [44]. Το σχήμα αυτό ανήκει σε μια ευρύτερη κατηγορία τεχνικών που βασίζονται στη λεγόμενη Διαμόρφωση Δείκτη Κβαντοποίησης (Quantization Index Modulation). Πιο σύνθετα σχήματα αυτής της κατηγορίας περιγράφονται από τους Chen και Wornell [45]-[48].

Ο Xia κ.ά. [8] εφαρμόζουν Διακριτό Μετασχηματισμό Κυματιδίων στην εικόνα και υδατογραφούν τους συντελεστές DWT υψηλών και μεσαίων συχνοτήτων που έχουν σχετικά μεγάλες τιμές. Οι συντελεστές με μεγάλες τιμές στις υψηλές συχνότητες αντιστοιχούν συνήθως σε περιοχές σύνθετης υψής, όπου μικρές μεταβολές δε γίνονται εύκολα αντιληπτές από το μάτι. Από τη διαδικασία της υδατογράφησης αποκλείονται οι συντελεστές χαμηλών συχνοτήτων προκειμένου να αποφευχθούν ορατές αλλοιώσεις στην εικόνα. Το υδατογράφημα που προστίθεται στους επιλεγμένους συντελεστές αποτελείται από μια ψευδοτυχαία ακολουθία Gauss και η ανίχνευσή του γίνεται σταδιακά, χάρη στην ιεραρχική κωδικοποίηση που παρέχει ο μετασχηματισμός κυματιδίων. Σε πρώτη φάση υπολογίζεται η

διαφορά των συντελεστών της υδατογραφημένης και της αρχικής εικόνας σε μια συγκεκριμένη υποζώνη και στη συνέχεια εξετάζεται η συσχέτιση της διαφοράς αυτής με το υδατογράφημα. Εάν η συσχέτιση δεν ξεπεράσει μια συγκεκριμένη τιμή, η διαδικασία της ανίχνευσης επαναλαμβάνεται περιλαμβάνοντας διαδοχικά και τις υπόλοιπες υποζώνες, έως ότου είτε ανιχνευτεί το υδατογράφημα είτε εξεταστούν όλες οι πιθανώς υδατογραφημένες υποζώνες. Δεδομένου ότι η προτεινόμενη τεχνική προορίζεται για την ανίχνευση ενός δοθέντος υδατογραφήματος εν γνώσει της αρχικής εικόνας, είναι προφανείς οι περιορισμοί ως προς την εφαρμοσιμότητά της.

Ο Wang κ.ά. [14] προτείνουν ένα «τυφλό» υδατογραφικό σχήμα, το οποίο εφαρμόζει Διακριτό Μετασχηματισμό Κυματιδίων και τεχνική διασποράς φάσματος για την υδατογράφιση συντελεστών DWT που επηρεάζουν σημαντικά το αισθητικό αποτέλεσμα. Η ένταση του υδατογραφήματος προσαρμόζεται ανάλογα με την υποζώνη και τη σπουδαιότητα των συντελεστών, ώστε να επιτευχθεί ικανοποιητικός συνδυασμός ανθεκτικότητας και διαφάνειας. Ο καθορισμός των σημαντικών συντελεστών κυματιδίων βασίζεται σε ένα σχήμα διαδοχικής κβαντοποίησης υποζωνών (successive subband quantization) και η ανίχνευση του υδατογραφήματος γίνεται μέσω του υπολογισμού της συσχέτισης.

Είναι σαφές ότι η βιβλιογραφική ανασκόπηση που παρουσιάστηκε παραπάνω δεν είναι πλήρης. Στοχεύει στην παρουσίαση μεμονωμένων σχημάτων που δίνουν απλώς μια ένδειξη των κατευθύνσεων που έχουν ακολουθηθεί από τους ερευνητές στον τομέα της ψηφιακής υδατογραφίας. Λόγω του μεγάλου όγκου της σχετικής βιβλιογραφίας, κάθε ερευνητής καλείται να εστιάσει στις τεχνικές εκείνες που ανταποκρίνονται και προσαρμόζονται στις ανάγκες και τα χαρακτηριστικά της εφαρμογής με την οποία ασχολείται. Στο Κεφάλαιο 4 παρουσιάζεται μια βιβλιογραφική ανασκόπηση που εστιάζεται στις ερευνητικές προσπάθειες που έχουν σημειωθεί προς την κατεύθυνση της αξιοποίησης της ψηφιακής υδατογραφίας σε ιατρικές εφαρμογές.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

- [1] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, "Information Hiding – A survey," *Proc. IEEE*, vol. 87, no. 7, July 1999.
- [2] F. Hartung, M. Kutter, "Multimedia watermarking techniques," in *Proc. IEEE Special Issue on Identification and Protection of Multimedia Information*, vol. 87, no. 7, pp. 1069--1107, July 1999.
- [3] U. Rajendra Acharya, D. Anand, P. Subbanna Bhat, U.C. Niranjan, "Compact storage of medical images with patient information," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 4, pp. 320-323, Dec. 2001.
- [4] S. Tzelepi, G. Pangalos, G. Nikolacopoulou, "Security of medical multimedia," *Med. Inform.*, vol. 27, no. 3, pp. 169-184, 2002.
- [5] G. W. Braudaway, K. A. Magerlein, F. Mintzer, "Protecting publically-available images with a visible image watermark," in *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques* (R. L. van Renesse, ed.), vol. 2659, pp. 126-133, February 1996.
- [6] I.J. Cox, J. Kilian, T. Leighton, T. Shamoan, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. Image Processing*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.
- [7] X. G. Xia, C. G. Boncelet, G. R. Arce, "A multiresolution watermark for digital images," *Proc. IEEE Int. Conf. Image Processing*, v.1, pp. 548-551, Santa Barbara, CA, Oct. 26-29, 1997.
- [8] X. G. Xia, C. G. Boncelet, G. R. Arce, "Wavelet transform based watermark for digital images," *Optics Express*, vol. 3, no. 12, pp. 497-511, Dec. 1998.
- [9] C.I. Podilchuk, W. Zeng, "Image-Adaptive Watermarking Using Visual Models," *IEEE Trans. Selected Areas of Comm.*, vol.16, no.4, pp.525-539, May 1998.
- [10] C. I. Podilchuk, E. J. Delp, "Digital watermarking: algorithms and applications," *IEEE Sig. Proc. Mag.*, vol. 18, no. 4, pp. 33-46, July 2001.
- [11] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3&4, pp. 313-336, 1996.
- [12] E. Koch, J. Zhao, "Towards robust and hidden image copyright labelling," *Proc. IEEE Workshop Nonlinear Signal and Image Process.*, I. Pitas, Ed., Neos Marmaras, Greece, June 20-22, 1995, pp. 452-455.

- [13] J.-F. Delaigle, C.D. Vleeschouwer, B. Macq, "Digital Watermarking," *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques*, vol. 2659, pp. 99-110, Feb. 1996.
- [14] H. J. M. Wang, P. C. Su, C. C. J. Kuo, "Wavelet-based digital image watermarking," *Optics Express*, vol. 3, no. 12, pp. 491-496, Dec. 1998.
- [15] A. H. Paquet, R. K. Ward, "Wavelet-based digital watermarking for image authentication," in *Proc. IEEE Canadian Conf. Electrical and Computer Engineering, CCECE 2002, Winnipeg, Canada*, vol. 2, pp. 879 – 884, May 2002.
- [16] I. J. Cox, M. L. Miller, J. A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan Kaufmann, 2002.
- [17] E.T. Lin, E.J. Delp, "A Review of Data Hiding in Digital Images," *Proc. Image Processing, Image Quality, Image Capture Systems Conference (PICS '99)*, Savannah, Georgia, pp. 274-278, April 25-28, 1999.
- [18] S. Craver, N. Memon, B. Yeo, M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications," *IEEE Journal of Selected Areas in Communications*, vol. 16, no.4, May 1998.
- [19] S. Katzenbeisser, *Information Hiding Techniques for Steganography and Digital Watermarking*, Norwood: Artech House Inc., 2000.
- [20] R. Venkatesan, S.-M. Koon, M. H. Jakubowski, P. Moulin, "Robust Image Hashing," *Proc. IEEE Int. Conf. Image Processing, ICIP 2000, Vancouver, Canada*, Sept. 10 - 13, 2000.
- [21] N.V. Boulgouris, I. Kompatsiaris, V. Mezaris, M.G. Strintzis, "Content-based Watermarking for Indexing Using Robust Segmentation," *Proc. Workshop Image Analysis for Multimedia Interactive Services*, Tampere, Finland, May 2001.
- [22] J. Jiang, A. Armstrong, "A Data Hiding Approach for Efficient Image Indexing," *Electronic Letters, IEE*, vol. 38, no. 23, pp. 1424-1425, 2002.
- [23] E. Louprias, N. Sebe, S. Bres, J. M. Jolion, "Wavelet-based salient points for image retrieval," in *Proc. Intern. Conf. Image Proc., ICIP 2000, Vancouver, Canada*, September 10-13, 2000, vol. 2, pp. 518-521.
- [24] V. Mezaris, N. V. Boulgouris, I. Kompatsiaris, D. Simitopoulos, M. G. Strintzis, "Segmentation and content-based watermarking for image indexing," *Proc. 4th COST 276 Workshop Information and Knowledge Management for Integrated Media*

Communication: Transmitting, processing and watermarking multimedia contents, Bordeaux, France, March 31-April 1, 2003.

- [25] N. F. Johnson, "In search of the right image: recognition and tracking of images in image databases, collections, and the internet," Technical report, George Mason University, Center for Secure Information Systems, June 1999.
- [26] G. C. Langelaar, I. Setyawan, R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Sig. Proc. Mag.*, vol. 17, no. 5, pp. 20-46, Sept. 2000.
- [27] R. J. Anderson, F. A. P. Petitcolas, "On the limits of Steganography," *IEEE J. Sel. Areas Commun Special Issue on Copyright and Privacy Protection*, vol. 16, no. 4, pp. 474-481, May 1998.
- [28] G. L. Friedman, "The trustworthy camera: restoring credibility to the photographic image," *IEEE Trans. Consumer Electronics*, vol. 39, no. 4, pp. 905-910, 1993.
- [29] M. Charrier, D. S. Cruz, M. Larsson, "JPEG2000, the next millennium compression standard for still images," *Proc. IEEE Intern. Conf. Multimedia & Computing Systems, ICMCS '99*, vol. 1, pp. 131-132, Florence, Italy, June 1999.
- [30] M. Barni, C.I. Podilchuk, F. Bartolini, E.J. Delp, "Watermark Embedding: Hiding a Signal Within a Cover Image," *IEEE Communication Magazine, Special Issue on Digital Watermarking for Copyright Protection: A Communication Perspective*, vol. 39, no. 8, pp. 102-108, Aug. 2001.
- [31] M. D. Swanson, B. Zhu, A. H. Tewfik, "Transparent Robust Image Watermarking," *Proc. IEEE International Conference on Image Processing*, vol. 3, pp. 211-214, 1996.
- [32] J.F. Delaigle, C. De Vleeschouwer, B. Macq, "Watermarking algorithm based on a human visual model," *Signal Processing*, vol. 66, no. 3, pp. 319-335, 1998.
- [33] M. Barni, F. Bartolini, V. Cappellini, A. Piva, "A DCT-domain system for robust image watermarking," *Signal Processing*, vol. 66, no. 3, pp. 357-372, 1998.
- [34] S. Pereira, T. Pun, "Robust template matching for affine-resistant image watermarks," *IEEE Transactions on Image Processing*, vol. 9, no.6, pp. 1123-1129, 2000.

- [35] C.-T. Hsu, J.-L. Wu, "Hidden digital watermarks in images," *IEEE Transactions on Image Processing*, vol. 8, no.1, pp. 58-68, 1999.
- [36] J.-P. M. G. Linnartz, T. Kalker, G. Depovere, "Modelling the false alarm and missed detection rate for electronic watermarks," *Proc. International Information Hiding Workshop (IHW'98)*, April 1998.
- [37] M. L. Miller, J. A. Bloom, "Computing the Probability of False Watermark Detection," *Proc. Workshop on Information Hiding*, Dresden, Germany, Sept. 29 - Oct. 1, 1999.
- [38] J. Zhao, E. Koch, "Embedding robust labels into images for copyright protection," *Proc. Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, Vienna, August 1995.
- [39] M.D. Swanson, B. Zhu, A.H. Tewfik, "Robust Data Hiding for Images," *Proc. IEEE 7th Digital Signal Processing Workshop*, Loen, Norway, pp. 37-40, Sept. 1996.
- [40] M. Wu, B. Liu, "Watermarking for image authentication," *Proc. IEEE Int. Conf. Image Processing, ICIP'98*, Chicago, 1998.
- [41] W. Zeng, B. Liu, "On Resolving Rightful Ownerships of Digital Images by Invisible Watermarks," *IEEE Signal Processing Society 1997, International Conference on Image Processing, ICIP'97*, Santa Barbara, California, Oct. 1997.
- [42] J. Fridrich, "Combining low-frequency and spread spectrum watermarking," *Proc. SPIE Conference on Mathematics of Data/Image Coding, Compression and Encryption*, M.S. Schmalz, Ed., vol. 3456, pp. 2-12, 1998.
- [43] D. Kundur, D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," *Proc. 4th IEEE Int. Conf. Image Processing, ICIP '97*, vol. 1, pp. 544-547, Santa Barbara, CA, USA, Oct. 26-29, 1997.
- [44] D. Kundur, D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," in *Proc. IEEE Special Issue on Identification and Protection of Multimedia Information*, vol. 87, no. 7, pp. 1167-1180, July 1999.
- [45] B. Chen, G. Wornell, "Preprocessed and Postprocessed quantization index modulation methods for digital watermarking," *Proc. SPIE: Security and Watermarking of Multimedia Contents II*, Vol. 3971, pp. 48-59, San Jose, Ca, USA, January 2000.

- [46] B. Chen, G. Wornell, "Dither modulation: A new approach to digital watermarking and information embedding," *Proc. SPIE, Security Watermarking Multimedia Contents*, San Jose, vol. 3657, pp. 342–353, Jan. 1999.
- [47] B. Chen, G. Wornell, "Quantization Index Modulation Methods for Digital Watermarking and Information Embedding of Multimedia," *Journal of VLSI Signal Processing*, no. 27, pp. 7-33, 2001.
- [48] B. Chen, G. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," *IEEE Trans. Information Theory*, vol. 47, no. 4, pp. 1423-1443, May 2001.

ΚΕΦΑΛΑΙΟ 3

ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΙΑΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

3.1 ΕΙΣΑΓΩΓΗ

Στις μέρες μας η ιατρική περίθαλψη βασίζεται σε μεγάλο βαθμό στη διαχείριση ψηφιακής πληροφορίας. Οι πρόσφατες εξελίξεις στις τεχνολογίες πληροφορικής και επικοινωνιών παρέχουν νέους τρόπους πρόσβασης, διαχείρισης και μετάδοσης ιατρικών εικόνων και φακέλων, αυξάνοντας όμως παράλληλα τον κίνδυνο σε ό,τι αφορά την ασφάλεια της εύκολα διακινούμενης και κατανεμημένης πληροφορίας. Αποτελεί πλέον συνήθη πρακτική η μετάδοση και αποθήκευση ιατρικών δεδομένων όχι μόνο στα πλαίσια ενός τοπικού δικτύου νοσοκομείου, αλλά και μεταξύ διαφορετικών μονάδων περίθαλψης μέσω ανοικτών δικτύων μη ασφαλών συνδέσεων. Είναι φανερό επομένως η ανάγκη υιοθέτησης πρόσθετων μέτρων και πρωτοκόλλων ασφαλείας στα σύγχρονα ιατρικά πληροφοριακά συστήματα. Οι βασικές απαιτήσεις που προκύπτουν ως προς την ασφάλεια των ιατρικών δεδομένων αποτυπώνονται σε κανονισμούς που έχουν θεσπιστεί σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο. Στις επόμενες ενότητες του κεφαλαίου, παρουσιάζονται τα πρότυπα και οι οδηγίες που αφορούν τη διαχείριση και αποθήκευση των ιατρικών δεδομένων και περιγράφονται οι βασικές απαιτήσεις ασφαλείας ως προς τη διαχείριση της παραγόμενης και διακινούμενης πληροφορίας σε συστήματα υπηρεσιών υγείας. Στη συνέχεια γίνεται αναφορά στα κύρια μέτρα

αντιμετώπισης των προβλημάτων και απειλών σε πληροφοριακά συστήματα υγείας, καθώς και στους περιορισμούς που διέπουν τις παρούσες τεχνολογίες και οδηγούν στην ανάγκη εύρεσης συμπληρωματικών λύσεων ασφάλειας.

3.2 ΠΕΡΙΓΡΑΦΗ ΝΟΜΙΚΟΥ ΠΛΑΙΣΙΟΥ

Σε διεθνές επίπεδο έχουν εκδοθεί κατά καιρούς από ποικίλους φορείς διάφορες οδηγίες και πρότυπα ως προς την ασφάλεια ιατρικών εικόνων και δεδομένων. Παρακάτω παρουσιάζεται το ισχύον νομικό πλαίσιο, όπως έχει διαμορφωθεί μέχρι σήμερα.

3.2.1 Κανονισμοί σε Διεθνές Επίπεδο

Στις Η.Π.Α., η νομοθετική πράξη “Fair Health Information Practices Act” του 1994 απαιτούσε τον περιορισμό της χρήσης προσωπικών δεδομένων υγείας μόνο στα σημεία που είναι απαραίτητα [1], [2]. Την ίδια χρονιά, ο οργανισμός ACR (American College of Radiology) εξέδωσε το Πρότυπο ACR για την τηλεραδιολογία (ACR Technical Standard for Teleradiology, Res. 21), το οποίο υπέστη διαδοχικές αναθεωρήσεις, με πιο πρόσφατη αυτήν του 2005 (Res. 39). Το πρότυπο αυτό περιλαμβάνει συστάσεις για τη χρήση και τους στόχους της τηλεραδιολογίας, τις προδιαγραφές του εξοπλισμού, τις ικανότητες, την πιστοποίηση και την υπευθυνότητα του ιατρικού και παραϊατρικού προσωπικού, τον έλεγχο ποιότητας και την επικοινωνία [3]-[7]. Το 1995, το Ινστιτούτο CPRI (Computer-based Patient Record Institute) εξέδωσε οδηγία για τον καθορισμό πολιτικών ασφαλείας, όπου αναφέρεται ότι κάθε οργανισμός που δημιουργεί, χρησιμοποιεί, αποθηκεύει ή μεταδίδει προσωποποιημένα δεδομένα υγείας, έχει ηθική και νομική υποχρέωση να διατηρεί το απόρρητο και την ακεραιότητα των δεδομένων αυτών [1], [8].

Επίσης στις Η.Π.Α., η νομοθετική πράξη Health Insurance Portability and Accountability Act (HIPAA) του 1996 (Public Law 104-191) διασαφηνίζει μια σειρά διαχειριστικών θεμάτων στον τομέα της υγείας και ορίζει ένα πλαίσιο προδιαγραφών που πρέπει να τηρούνται από τους φορείς υγείας κατά τη μετάδοση

και αποθήκευση ιατρικής πληροφορίας, με στόχο την ασφάλεια των δεδομένων και την προστασία των προσωπικών στοιχείων του ασθενή [9], [10]. Σύμφωνα με το νόμο αυτό, το Υπουργείο Υγείας (Department of Health and Human Services – HHS) όφειλε να θεσπίσει πρότυπα ασφάλειας βάσει του οριζόμενου πλαισίου. Ως απάντηση, το υπουργείο δημοσίευσε το 1998 πρότυπα για την ασφάλεια των ιατρικών δεδομένων και την ηλεκτρονική υπογραφή [11] και έθεσε προθεσμία πέντε ετών στους αρμόδιους φορείς για πλήρη συμμόρφωση με τα πρότυπα αυτά.

Ο οργανισμός NEMA (National Electrical Manufacturers Association) έχει ιδρύσει μια Επιτροπή (Privacy and Security Committee) η οποία επιλαμβάνεται θεμάτων προστασίας και ασφάλειας των προσωπικών δεδομένων, αλλά και ειδικά της ιατρικής πληροφορίας που χρήζει ιδιαίτερης προσοχής [12]. Η Επιτροπή αυτή μελετά τους σχετικούς κανονισμούς που έχουν θεσπιστεί στις ΗΠΑ, την Ευρώπη και την Ιαπωνία και επιχειρεί να αναδείξει στοιχεία ασυμβατότητας μεταξύ τους, τα οποία περιπλέκουν τη σχεδίαση και εφαρμογή λύσεων ασφάλειας που να είναι καθολικά αποδεκτές. Επιδιώκει να συμβάλει στην καθιέρωση διεθνών προτύπων εναρμονισμένων με τις διαφορετικές μεταξύ χωρών νομοθετικές ρυθμίσεις ως προς τη σχεδίαση και θεμιτή χρήση του ιατροτεχνολογικού εξοπλισμού και των ιατρικών πληροφοριακών συστημάτων, προκειμένου να διευκολυνθεί η συνεργασία και ανταλλαγή προϊόντων και να διασφαλιστεί η προστασία των ασθενών σε παγκόσμια κλίμακα. Για το σκοπό αυτό, συνεργάζεται στενά με την Ευρωπαϊκή Ομοσπονδία Κατασκευαστών Ιατρικού Εξοπλισμού (European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry – COCIR) [13] – που αποτελεί τον αντίστοιχο φορέα στην Ευρώπη – και επιδιώκει συνεργασία τόσο με τον αντίστοιχο ιαπωνικό οργανισμό JIRA (Japan Industries Association of Radiological Systems) [14], όσο και με άλλους ενδιαφερόμενους οργανισμούς και εταιρείες. Από τη συνεργασία των οργανισμών NEMA και ACR προέκυψε η σύσταση της Επιτροπής Ψηφιακής Απεικόνισης και Μετάδοσης στην Ιατρική DICOM (Digital Image and Communication in Medicine), με στόχο την προτυποποίηση της μετάδοσης ιατρικών εικόνων και μεταδεδομένων [15].

Η ενότητα 15 του Προτύπου DICOM εκδόθηκε το 2001 προκειμένου να παράσχει μια προτυποποιημένη μέθοδο για ασφαλή μετάδοση και ψηφιακή

υπογραφή (PS 3.15-2001) [3], [15]. Προδιαγράφει τα τεχνικά μέσα (επιλογή προτύπων ασφάλειας, αλγορίθμους και παραμέτρους) για οντότητες εφαρμογής που εμπλέκονται στην ανταλλαγή πληροφορίας για εφαρμογή πολιτικών ασφάλειας. Σε αυτήν την ενότητα του DICOM έχουν προστεθεί τέσσερα προφίλ ασφάλειας: ασφαλούς χρήσης, ασφαλούς σύνδεσης μετάδοσης (secure transport connection profile), ψηφιακής υπογραφής και ασφαλούς αποθήκευσης δεδομένων (media storage secure profiles). Τα παραπάνω προφίλ θέτουν θέματα όπως χρήση χαρακτηριστικών, ασφάλεια στις συνδέσεις, πιστοποίηση αντικειμένων και ασφάλεια των αρχείων.

Επιπλέον, ο Οργανισμός Εφαρμογών Πληροφορικής στην Ακτινολογία (Society of Computer Applications in Radiology – SCAR) εξέδωσε την οδηγία «Θέματα ασφαλείας σε ψηφιακές ιατρικές επιχειρήσεις» («Security issues in the digital medical enterprise») το 2000, προκειμένου να δώσει έμφαση στην επιτακτική ανάγκη αντιμετώπισης του συγκεκριμένου κρίσιμου ζητήματος [3], [16].

Με βάση τα παραπάνω, διεθνείς οργανισμοί έχουν καθορίσει μια σειρά από πρότυπα σχετικά με την ασφάλεια πληροφοριακών συστημάτων και δεδομένων στο χώρο της υγείας. Οι οργανισμοί αυτοί συνεργάζονται στενά μεταξύ τους και περιλαμβάνουν:

- την Ευρωπαϊκή Επιτροπή Τυποποίησης (European Standards Committee – CEN) που συνέστησε το 1990 την Τεχνική Επιτροπή 251 (TC 251) με στόχο την προτυποποίηση στον τομέα της ιατρικής πληροφορικής [17], [18]
- το διεθνή οργανισμό τυποποίησης ISO (International Standards Organization) που συνέστησε το 1998 την Τεχνική Επιτροπή 215 (TC 215) για τον ίδιο σκοπό [19]
- τον οργανισμό HL7 (Health Level 7) που ιδρύθηκε το 1987 στις Η.Π.Α., εγκρίθηκε από τον ANSI (American National Standards Institute) το 1994 ως Οργανισμός Ανάπτυξης Προτύπων (Standards Developing Organization – SDO) και πλέον έχει παραρτήματα σε όλον τον κόσμο [20]
- την επιτροπή DICOM [15]
- το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών IEEE (Institute of Electrical and Electronics Engineers) που ίδρυσε την επιτροπή

1073, η οποία στοχεύει στη διαμόρφωση προτύπων σχετικών με την επικοινωνία μεταξύ ιατρικών συσκευών [21].

Παρακάτω παρατίθεται μια ενδεικτική λίστα από πρότυπα που έχουν εκδοθεί με στόχο την ασφάλεια πληροφοριακών συστημάτων και δεδομένων στο χώρο της υγείας [15], [17] – [21]:

- Τα κείμενα εργασίας της Ευρωπαϊκής Επιτροπής Τυποποίησης CEN/TC251 για τα ιατρικά πληροφοριακά συστήματα. Ενδεικτικά αναφέρονται τα ακόλουθα:
 - ENV 12924: 1996 Health informatics – security categorization and protection for healthcare information systems
 - ENV 12388: 1997 Health informatics - Algorithm for digital signature services in healthcare
 - ENV 13608: 2000 Health informatics - Security for health care communications
 - o Part 1 Concepts and terminology ENV 13608 – 1
 - o Part 2 Secure data objects ENV 13608 – 2
 - o Part 3 Secure data channels ENV 13608 – 3
 - ENV 13729: 2000 Health informatics – Secure user identification – strong authentication using microprocessor cards
 - ENV 12551: 2000 Health informatics – Secure user authentication for health care – Management and security of authentication by passwords
 - EN 14484: 2002 Health Informatics – International transfer of personal health data covered by the EU Data Protection Directive – High level security policy
 - CR 13694: 1999 Health Informatics – Safety and security related software quality standards for healthcare
 - CR 14301: 2002 Health Informatics – Framework for security protection of healthcare communication
 - CR 14302: 2002 Health Informatics – Framework for security requirements for intermittently connected devices.

- Από το διεθνή οργανισμό τυποποίησης (ISO):
 - ISO DTS 17090 Health Informatics – Public Key Infrastructure
 - ISO/IEC 17799: 2005 (=BS 7799) Information Technology – Security techniques – Code of practice for information security management.
 - o Part 1: Code of Practice for information security management
 - o Part 2: Specification for information security management systems
 - ISO/ CD TC 215: TR 21089, Health Informatics – Trusted end-to-end information flows
 - ISO/IEC TR 13335 Guidelines for the Management of IT Security
 - o Part 1: Concepts and Models
 - o Part 2: Managing and Planning IT Security
 - o Part 3: Techniques for the management of IT Security
- Οι κατευθυντήριες γραμμές της ASTM (American Society for Testing and Materials) σχετικά με την ασφάλεια ιατρικών πληροφοριακών συστημάτων:
 - E 2086-00 Standard Guide for Internet and Intranet Healthcare Security
 - E 2085-00a Standard Guide on Security Framework for Healthcare Information
- Τα Κοινά Κριτήρια (Common Criteria for Information Technology Security) που αναφέρονται στην αξιολόγηση της ασφάλειας πληροφοριακών συστημάτων:
 - ISO/IEC 15408-1: 1999 Information technology – Security techniques – Evaluation criteria for IT security.

3.2.2 Ευρωπαϊκή Νομοθεσία

3.2.2.1 Ιδιοκτησιακό καθεστώς

Ένα βασικό ζήτημα που διασαφηνίζεται από την ευρωπαϊκή νομοθεσία αποτελεί το ιδιοκτησιακό καθεστώς των ιατρικών δεδομένων, το οποίο καθορίζει τα δικαιώματα πρόσβασης σε ιατρικούς φακέλους. Θέματα σχετικά με το ποιος και σε

ποιο βαθμό έχει πρόσβαση σε ιατρικούς φακέλους, αλλά και το ποιος καθορίζει τα δικαιώματα πρόσβασης, έχουν απασχολήσει πληθώρα ευρωπαϊκών έργων και διεθνών πρωτοβουλιών. Η ισχύουσα νομοθεσία καθορίζει ότι τα δεδομένα που αφορούν την υγεία του ατόμου αποτελούν μέρος της προσωπικότητας του ατόμου και όχι ιδιοκτησία του φορέα που τα συλλέγει και τα επεξεργάζεται. Ωστόσο, το συμπέρασμα που προέκυψε από πολλά σχετικά έργα είναι ότι η ιδιοκτησία του ιατρικού φακέλου δεν μπορεί να ανήκει σε ένα μόνο άτομο καθώς πολλοί επαγγελματίες υγείας ενδέχεται να έχουν συνεισφέρει και να έχουν προσθέσει πληροφορία σε αυτόν.

3.2.2.2 Διατάξεις και γνωμοδοτήσεις σε ευρωπαϊκό επίπεδο

Παρακάτω παρουσιάζονται συνοπτικά οι διατάξεις, ρυθμίσεις και γνωμοδοτήσεις σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα στον ευρωπαϊκό χώρο:

- Η Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου – ΕΣΔΑ (European Human Rights Convention - EHRC) του 1950. Το άρθρο 8 προστατεύει την ιδιωτική ζωή, στην οποία συγκαταλέγονται και τα προσωπικά δεδομένα. Ως προς τα ιατρικά δεδομένα το Δικαστήριο Ανθρωπίνων Δικαιωμάτων όρισε αυστηρές προϋποθέσεις για την ανακοίνωσή τους σε τρίτους.
- Οι κατευθυντήριες γραμμές που εξέδωσε το 1980 ο ΟΟΣΑ (Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης / Organisation for Economic Co-operation and Development – OECD) για την προστασία των προσωπικών δεδομένων γενικά. Επίσης, το 1998 ο ΟΟΣΑ εξέδωσε μια οδηγία σχετικά με την υλοποίηση των παραπάνω γραμμών σε παγκόσμια δίκτυα, ενώ το 2002 υιοθέτησε κατευθυντήριες γραμμές για την Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων (OECD Guidelines for the Security of Information Systems and Networks), υποδεικνύοντας ότι η ασφάλεια εμπίπτει στην ευθύνη όλων των συμμετεχόντων, ανάλογα με το ρόλο τους [22].
- Η Σύσταση 108 του Συμβουλίου της Ευρώπης (28/1/1981) για την προστασία ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού

χαρακτήρα, η οποία ορίζει ότι τα ιατρικά δεδομένα δεν μπορούν να γίνουν αντικείμενο αυτοματοποιημένης επεξεργασίας, χωρίς εγγυήσεις για την προστασία τους βάσει νόμου. Μετά την έκδοση της οδηγίας 95/46/ΕΕ ωστόσο η Σύσταση αυτή έχει περιορισμένη σπουδαιότητα.

- Ο Χάρτης (Διακήρυξη) των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Charter of Fundamental Rights of the European Union), που αποτελεί την πιο πρόσφατη εξέλιξη στον τομέα των θεμελιωδών δικαιωμάτων των πολιτών. Η διακήρυξη αυτή ορίζει ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Επίσης, κάθε πρόσωπο έχει δικαίωμα να έχει πρόσβαση στα δεδομένα που το αφορούν και να τα διορθώνει [23].
- Η Οδηγία 95/46/ΕΕ (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) της ΕΕ προς τα κράτη-μέλη, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών [24].
- Η Οδηγία 2002/58/ΕΕ (2002/58/EC) για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών που αντικατέστησε την Οδηγία 97/66/ΕΕ (Directive 97/66/EC) για την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα [24].
- Η Σύσταση No R (97) 5 (Recommendation No R (97) 5 on the protection of medical data), η οποία έγινε δεκτή από το Συμβούλιο της Ευρώπης το 1997 και αφορά την προστασία ιατρικών δεδομένων [25].
- Η Σύσταση No R (99) 5 (Recommendation No R (99) 5), η οποία έγινε δεκτή από το Συμβούλιο της Ευρώπης το 1999 και η οποία παρέχει κατευθυντήριες γραμμές (guidelines) για την προστασία των ατόμων σε σχέση με τη συλλογή και επεξεργασία προσωπικών δεδομένων σε «λεωφόρους πληροφοριών» (information highways) [26].

- Η Γνωμοδότηση του European Group on Ethics in Science and New Technologies (Opinion No 13 – Ethical issues of healthcare in the information society) του 1999, η οποία κατοχυρώνει τον ορισμό των προσωπικών ιατρικών δεδομένων. Η γνωμοδότηση δίνει έμφαση σε βασικές αρχές που αφορούν την επεξεργασία των ιατρικών δεδομένων, ορίζοντας μεταξύ άλλων ότι απαιτούνται τεχνικά και οργανωτικά μέτρα ασφαλείας και η εφαρμογή τεχνολογιών κρυπτογραφίας. Η γνωμοδότηση καταλήγει στο ότι τα θέματα αυτά πρέπει να κατοχυρωθούν νομικά, κατά προτίμηση μέσω κάποιας οδηγίας της Ευρωπαϊκής Ένωσης σχετικά με την προστασία των ιατρικών δεδομένων [27].

3.2.3 Ελληνική Νομοθεσία

Η ελληνική νομοθεσία προβλέπει τα εξής: η προστασία των προσωπικών δεδομένων διασφαλίζεται καταρχάς από το άρθρο 9Α του Συντάγματος, όπου κατοχυρώνεται ρητά το ατομικό δικαίωμα προστασίας απέναντι στη συλλογή, αποθήκευση και επεξεργασία, με συμβατικό ή ηλεκτρονικό τρόπο, των προσωπικών πληροφοριών και δεδομένων. Αποτελεί τη συνταγματική επιβεβαίωση της σχετικής σύμβασης του 1981 του Συμβουλίου της Ευρώπης (η οποία κυρώθηκε με το νόμο 2068/1992).

Η εναρμόνιση της ελληνικής νομοθεσίας προς τη σχετική Κοινοτική Οδηγία 95/46/EE (Data Protection Directive) [24] σχετικά με την «προστασία του ατόμου όσον αφορά την επεξεργασία προσωπικών δεδομένων και την ελεύθερη διακίνησή τους» και τη σύσταση R 97 (5) περί προστασίας ιατρικών δεδομένων [25], έγινε με τη θέσπιση του Νόμου 2472/1997 περί «Προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» [28].

Ο Νόμος 2472/97 μεταφέρει την Οδηγία 95/46/EE στο εσωτερικό δίκαιο και συγχρόνως εκπληρώνει την υποχρέωση της Ελλάδας που απορρέει από τη Σύμβαση 108 του Συμβουλίου της Ευρώπης. Επιπλέον, η Οδηγία 97/66/EE, που εξειδικεύει την Οδηγία 95/46/EE ως προς ορισμένες πτυχές που συνδέονται με τη συγκεκριμένη κατηγορία εφαρμογής, μεταφέρεται στο εσωτερικό δίκαιο με τον ελληνικό νόμο

2774/99 [29]. Ειδικά για τα ιατρικά δεδομένα, η προστασία τους διέπεται, εκτός από τις διατάξεις των νόμων 2472/97 και 2774/99, από το άρθρο 371 του Ποινικού Κώδικα στο οποίο κατοχυρώνεται το ιατρικό απόρρητο. Η προστασία της ιδιωτικής ζωής του ασθενούς και ο απόρρητος χαρακτήρας του ιατρικού φακέλου κατοχυρώνονται επιπλέον στο Άρθρο 47 του Ν. 2071/92 (Νόμος Ε.Σ.Υ.).

3.3 ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Η ισχύουσα νομοθεσία ορίζει ρητά τα δικαιώματα των πολιτών και διασφαλίζει την προστασία των ευαίσθητων προσωπικών δεδομένων επιβάλλοντας μια σειρά μέτρων ασφαλείας που αφορούν τον έλεγχο πρόσβασης στην ιατρική πληροφορία, την προστασία της από τυχαία ή εσκεμμένη διαρροή σε μη εξουσιοδοτημένα άτομα και την αποφυγή μη εγκεκριμένης τροποποίησης, καταστροφής, ή απώλειας. Παρακάτω παρουσιάζονται οι βασικές απαιτήσεις ασφαλείας στα ιατρικά πληροφοριακά συστήματα [12], [30]:

- *Εμπιστευτικότητα*: η προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένα άτομα αποτελεί πρώτη προτεραιότητα και απαιτείται η εφαρμογή μέτρων που θα επιτρέπουν την πρόσβαση σε πληροφορία μόνο από αναγνωρισμένα και πιστοποιημένα άτομα. Κάθε χρήστης πρέπει να έχει δικαίωμα πρόσβασης μόνο στην απολύτως απαραίτητη πληροφορία που χρειάζεται και να εκτελεί μόνο το σύνολο των λειτουργιών που απαιτούνται προκειμένου να επιτελέσει το έργο του, χωρίς ωστόσο να διακυβεύεται η παροχή σωστής περίθαλψης.
- *Ακεραιότητα*: στα συστήματα διαχείρισης ιατρικής πληροφορίας πρέπει να διασφαλιστεί η ακρίβεια και ακεραιότητα των δεδομένων, καθώς σε αυτά βασίζεται η διάγνωση και η προτεινόμενη αγωγή. Προκειμένου να προστατευτεί η διαγνωστική αξία της ιατρικής πληροφορίας επιβάλλεται η χρήση κατάλληλων μηχανισμών ελέγχου της ακεραιότητας των δεδομένων, που να επιτρέπουν την παρακολούθηση ενδεχόμενων τροποποιήσεων. Για τον αποτελεσματικό έλεγχο και την προστασία των δεδομένων από μη εγκεκριμένη τροποποίηση χρειάζεται

ένας μηχανισμός που θα δίνει τη δυνατότητα ελέγχου κάθε πληροφορίας χωριστά και που θα είναι ανεξάρτητος από το σύστημα.

- *Μη αποποίηση ευθύνης:* Στα πλαίσια του αυστηρού ελέγχου για την αξιοπιστία των δεδομένων απαιτείται επιπλέον η αναγνώριση και πιστοποίηση των επικοινωνούντων οντοτήτων, που αποτελεί ένα βασικό μέτρο προφύλαξης από ενδεχόμενη μη εξουσιοδοτημένη διείσδυση στο σύστημα και αθέμιτη τροποποίηση στοιχείων ή πιστοποίηση μη αυθεντικών δεδομένων. Ένας ισχυρός μηχανισμός ελέγχου της αξιοπιστίας της διακινούμενης πληροφορίας είναι η λεγόμενη «μη αποποίηση ευθύνης» (non-repudiation), η αδυναμία δηλαδή των εμπλεκομένων σε μία συναλλαγή μερών να αρνηθούν τη συμμετοχή τους σε αυτή, η οποία αυξάνει την προστασία της ακεραιότητας των δεδομένων.
- *Ένδειξη χρόνου αποστολής – λήψης πληροφορίας:* η χρονική στιγμή της δημιουργίας και της αποστολής – λήψης πληροφορίας έχει ιδιαίτερη σημασία σε εφαρμογές διαχείρισης ιατρικών δεδομένων, όπως για παράδειγμα κατά την έκδοση επιδημιολογικών αποτελεσμάτων εργαστηρίων. Η απαίτηση της απόδειξης του χρόνου αποστολής – λήψης εξασφαλίζει επιπλέον τη μοναδικότητα της διακινούμενης πληροφορίας μέσω της σύνδεσής της με μία μοναδική στιγμή στο χρόνο.
- *Διαθεσιμότητα:* η ιατρική πληροφορία θα πρέπει να είναι διαθέσιμη όποτε ζητηθεί, προκειμένου να διασφαλιστεί η ομαλή διεξαγωγή των προγραμματισμένων ενεργειών πρόσβασης και διαχείρισής της και η παροχή έγκαιρης περίθαλψης στους ασθενείς. Υπό κανονικές συνθήκες λειτουργίας η ανάκτηση και διαχείριση πληροφορίας θα πρέπει να είναι εύκολη και ταχεία. Επιπλέον είναι απαραίτητο να γίνει πρόβλεψη για τη διασφάλιση της διαθεσιμότητας της πληροφορίας σε ηλεκτρονική μορφή ακόμη και σε έκτακτες περιπτώσεις, όπως για παράδειγμα στην περίπτωση βλάβης εξοπλισμού ή διακοπής ρεύματος.

3.4 ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

Οι υπηρεσίες ασφάλειας στοχεύουν στην προστασία μεταδιδόμενων ή αποθηκευμένων ιατρικών δεδομένων από συγκεκριμένες ενέργειες. Παρακάτω παρουσιάζονται οι υπηρεσίες που απαιτούνται για την ασφάλεια των συστημάτων ιατρικών βάσεων δεδομένων και της μετάδοσης ιατρικών εικόνων [30]:

3.4.1 Υπηρεσίες Ασφάλειας Ιατρικών Βάσεων Δεδομένων

Μια βασική απαίτηση αποτελεί η εξασφάλιση *ελέγχου πρόσβασης* στα συστήματα ιατρικών βάσεων πολυμεσικών δεδομένων, καθώς σε αυτά αποθηκεύονται ευαίσθητα προσωπικά δεδομένα των ασθενών, αλλά και οι εικόνες από τις ιατρικές εξετάσεις τους. Υπάρχουν άλλωστε τόσο νομικοί όσο και ηθικοί κανόνες που υπαγορεύουν την απόλυτα ελεγχόμενη πρόσβαση σε αυτά τα δεδομένα. Οι υπηρεσίες ελέγχου πρόσβασης γενικά περιλαμβάνουν το συνδυασμό μιας μορφής αναγνώρισης «ομότιμης οντότητας» (peer entity identification) – για την πιστοποίηση της οντότητας που επιθυμεί να χρησιμοποιήσει την ευαίσθητη πληροφορία – με ένα σύστημα έγκρισης βάσει κανόνων (rules-based permission system). Γενικά, μια οντότητα που επιθυμεί πρόσβαση στους πόρους του συστήματος πρέπει κατ' αρχάς να αυθεντικοποιηθεί, να πιστοποιήσει δηλαδή την ταυτότητά της. Μετά την ταυτοποίησή της, μια διεργασία καθορίζει εάν η οντότητα επιτρέπεται να αποκτήσει πρόσβαση στα αιτούμενα δεδομένα, βάσει προκαθορισμένων κανόνων. Σε περίπτωση αίτησης πρόσβασης από απόσταση, απαιτούνται πρόσθετες υπηρεσίες ασφάλειας για την εξασφάλιση εμπιστευτικότητας, ακεραιότητας των δεδομένων και μη αποποίησης. Οι υπηρεσίες εμπιστευτικότητας στοχεύουν στην προστασία της πληροφορίας από μη εξουσιοδοτημένη πρόσβαση. Τα συστήματα βάσεων ιατρικών εικόνων απαιτούν την εφαρμογή μιας υπηρεσίας πιστοποίησης προέλευσης δεδομένων (data origin authentication service) ώστε να εξασφαλιστεί ότι μόνο δεδομένα από επιτρεπτές πηγές θα εισαχθούν στο σύστημα βάσης ιατρικών δεδομένων. Διαφορετικά, θα ήταν πιθανό για κάποιον κακόβουλο εξωτερικό χρήστη (outsider) να εισαγάγει φαινομενικά έγκυρη πληροφορία στο σύστημα.

Σε τέτοια συστήματα απαιτούνται επίσης μηχανισμοί για «μη αποποίηση» και προστασία πνευματικών δικαιωμάτων (copyright protection), ειδικά για δεδομένα που σχετίζονται με ιατρικές εικόνες ασθενών. Δεδομένου ότι στις βάσεις αποθηκεύονται ιατρικές εικόνες για μακροχρόνιο διάστημα, είναι αναγκαίο να διασφαλίζεται η αποδοχή της ευθύνης για τις εικόνες που αποθηκεύονται σε αυτές και οι οποίες λαμβάνονται από εξουσιοδοτημένες πηγές. Δε θα πρέπει δηλαδή να υπάρχει αργότερα η δυνατότητα ούτε για τη βάση ιατρικών εικόνων αλλά ούτε και για την οντότητα αποστολής (πηγή προέλευσης) να αρνηθούν ότι έχουν παραλάβει και αποστείλει αντίστοιχα τα ιατρικά δεδομένα. Επιπλέον, η βάση ιατρικών εικόνων δε θα πρέπει στη συνέχεια να έχει τη δυνατότητα να παραποιήσει ή να διανείμει εικόνες χωρίς να έχει προηγηθεί η κατάλληλη εξουσιοδότηση. Οι ίδιοι περιορισμοί ισχύουν και στις πληροφορίες που αποθηκεύονται σε βάσεις δεδομένων που συνδέονται με μια βάση ιατρικών εικόνων, χωρίς απαραίτητα να αποτελούν τμήμα αυτής.

Δύο βασικές απαιτήσεις που πρέπει να πληρούνται κατά την αποθήκευση δεδομένων σε βάσεις ιατρικών εικόνων αποτελούν η *ακεραιότητα των δεδομένων* αυτών, καθώς επίσης και η *άρρηκτη σύνδεση* μεταξύ των ιατρικών εικόνων και του ασθενή στον οποίον αυτές αντιστοιχούν. Επιβάλλεται επομένως η ύπαρξη μηχανισμών οι οποίοι επιτρέπουν την ανίχνευση μεταβολών (εσκεμμένων ή μη) που ενδέχεται να έχουν σημειωθεί σε αποθηκευμένα δεδομένα. Το πρόβλημα της ακεραιότητας των δεδομένων είναι ιδιαίτερα κρίσιμο στην περίπτωση των βάσεων ιατρικών εικόνων, τόσο γιατί αποθηκεύονται σε αυτές δεδομένα για μακροχρόνιο διάστημα, κατά το οποίο θα πρέπει να διαφυλαχθεί η ακεραιότητά τους, όσο και γιατί θα πρέπει να διασφαλιστεί η προστασία των δεδομένων κατά τη μετάδοσή τους. Επιπλέον πρέπει να διαφυλαχθεί η *άρρηκτη σύνδεση* των εικόνων από τις εξετάσεις του ασθενούς με τα προσωπικά του στοιχεία, καθώς και με άλλη πληροφορία που τον αφορά (ιατρικό ιστορικό κ.λπ.), τόσο κατά τη μετάδοση, όσο και κατά την αποθήκευσή τους.

Η *διαθεσιμότητα* της πληροφορίας αποτελεί μια άλλη κρίσιμη απαίτηση. Τα δεδομένα που αποθηκεύονται σε βάσεις ιατρικών εικόνων και άλλες σχετικές βάσεις απαιτούν προστασία έναντι καταστροφής εξοπλισμού (equipment failure) και

χρειάζεται να ληφθούν μέτρα προκειμένου να διασφαλιστεί η απρόσκοπτη λειτουργία του συστήματος σε περίπτωση έκτακτων περιστατικών.

Κατά τον καθορισμό των προδιαγραφών ασφάλειας βάσεων ιατρικών εικόνων πρέπει επίσης να ληφθούν υπόψη πολιτικές διαχείρισης (administrative and management policies). Στη συγκεκριμένη περίπτωση οι πολιτικές αυτές πρέπει να βασίζονται στην «αρχή των ελάχιστων προνομίων και εξουσιοδοτημένων ενεργειών» (least privilege and authorized actions). Κάτι τέτοιο είναι απαραίτητο προκειμένου να ελαχιστοποιηθεί η πιθανότητα ζημιάς τόσο σε περίπτωση μη εξουσιοδοτημένης πρόσβασης σε βάση ιατρικών εικόνων, όσο και σε περίπτωση πρόσβασης από κακόβουλο άτομο. Πρέπει επιπλέον να τεθούν επί τάπητος θέματα διαχείρισης προσωπικού· η διαδικασία επιλογής των εξουσιοδοτημένων χρηστών που θα αποκτήσουν πρόσβαση στα ιατρικά δεδομένα πρέπει να είναι αποδοτική, προκειμένου να εξαιρεθούν οι πιθανώς αναξιόπιστοι ή χωρίς τα απαιτούμενα προσόντα υποψήφιοι. Επιβάλλεται επίσης η εκπαίδευση των χρηστών των βάσεων ιατρικών εικόνων στη χρήση τέτοιων συστημάτων και στις ευθύνες τους ως προς την παρεχόμενη ασφάλεια.

Τέλος, πρέπει να ληφθούν υπόψη θέματα αξιοπιστίας δεδομένων. Μια βάση ιατρικών δεδομένων προορίζεται για αποθήκευση μεγάλου όγκου πληροφορίας για μακροχρόνιο διάστημα και το μεγαλύτερο μέρος της πληροφορίας που περιέχεται σε αυτήν πρακτικά δεν αντικαθίσταται. Είναι επιβεβλημένο επομένως να δοθεί η απαιτούμενη προσοχή στα πιθανά προβλήματα που συνδέονται με τη μακροπρόθεσμη αποθήκευση και να προβλεφθεί περιοδική δημιουργία αντιγράφων ασφαλείας (back-up) των δεδομένων.

3.4.2 Υπηρεσίες Ασφάλειας κατά τη Μετάδοση Ιατρικών Εικόνων

Στην ενότητα αυτή παρουσιάζονται οι υπηρεσίες ασφάλειας που απαιτείται να εφαρμοστούν προκειμένου να διασφαλιστεί η προστασία των ιατρικών εικόνων κατά τη μετάδοσή τους.

Μια βασική απαίτηση για την ασφάλεια κατά τη μετάδοση πολυμεσικών ιατρικών δεδομένων αποτελεί η εφαρμογή υπηρεσίας αυθεντικοποίησης «ομότιμης

οντότητας» (peer entity authentication). Πριν από τη μετάδοση των ιατρικών δεδομένων, οι χρήστες του συστήματος πρέπει να διασφαλίσουν ότι η άλλη οντότητα που εμπλέκεται στη μετάδοση των δεδομένων είναι πραγματικά αυτή που ισχυρίζεται ότι είναι. Η αυθεντικοποίηση αυτή πρέπει να είναι αμοιβαία· είναι εξίσου σημαντικό για ένα γιατρό από απόσταση να γνωρίζει με βεβαιότητα ότι το σύστημα από το οποίο έχει ζητήσει να λάβει αρχεία σχετικά με περιστατικά ενός συγκεκριμένου ασθενή είναι πράγματι το σύστημα από το οποίο τα ζήτησε, όσο είναι και για το σύστημα να γνωρίζει ότι ο απομακρυσμένος γιατρός είναι πράγματι εξουσιοδοτημένος χρήστης του συστήματος.

Μια άλλη βασική απαίτηση είναι η *εμπιστευτικότητα*. Γίνεται η παραδοχή ότι τουλάχιστον κάποιο τμήμα του καναλιού μετάδοσης που εμπλέκεται στη μετάδοση της πολυμεσικής ιατρικής πληροφορίας από και προς απομακρυσμένους σταθμούς είναι προσπελάσιμο από άτομα που δεν έχουν εξουσιοδότηση να αποκτήσουν πρόσβαση στο σύστημα της βάσης ιατρικών δεδομένων. Αυτό ισχύει γενικά κάθε φορά που χρησιμοποιούνται δημόσια δίκτυα επικοινωνίας για τη μετάδοση ιατρικής πληροφορίας – περιλαμβανομένων και των περιπτώσεων όπου χρησιμοποιούνται εκμισθωμένα ιδιωτικά κυκλώματα. Η φυσική ή ηλεκτρονική πρόσβαση στο κανάλι μετάδοσης ενέχει τον κίνδυνο υποκλοπής της μεταδιδόμενης πληροφορίας και αποκάλυψής της σε μη εξουσιοδοτημένα άτομα.

Υπηρεσίες ακεραιότητας δεδομένων απαιτούνται και για την ασφάλεια κατά τη μετάδοση ιατρικών εικόνων. Αυτές οι υπηρεσίες απαιτούνται τόσο για την ανίχνευση τυχαίων λαθών που συμβαίνουν κατά τη μετάδοση των δεδομένων, όσο και για τον εντοπισμό αλλοιώσεων που οφείλονται σε κακόβουλες προσπάθειες παραποίησης των δεδομένων κατά τη διάρκεια μετάδοσής τους. Είναι επίσης απαραίτητη η διατήρηση της σύνδεσης των πληροφοριών κατά τη μετάδοσή τους από ένα σύστημα βάσης ιατρικών δεδομένων. Η εξασφάλιση της ακεραιότητας της πληροφορίας, σε συνδυασμό με μια αποδοτική μέθοδο που εγγυάται την ισχυρή σύνδεση μεταξύ σχετιζόμενων δεδομένων, μπορεί να εξασφαλίσει την κάλυψη των παραπάνω απαιτήσεων.

3.5 ΑΝΑΣΚΟΠΗΣΗ ΤΕΧΝΙΚΩΝ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ

Τα σύγχρονα συστήματα διαχείρισης ιατρικής πληροφορίας υιοθετούν μια σειρά τεχνικών μέτρων προκειμένου να εναρμονιστούν με την εθνική, ευρωπαϊκή και διεθνή νομοθεσία περί ασφάλειας και προστασίας των ιατρικών και ευαίσθητων προσωπικών δεδομένων. Στην παρούσα ενότητα γίνεται μια ανασκόπηση των πρακτικών ασφαλείας που ακολουθούνται στις μέρες μας με στόχο την κάλυψη των προαναφερθέντων βασικών απαιτήσεων που διέπουν τη διαχείριση ιατρικών δεδομένων.

Οι βασικοί κίνδυνοι σε σχέση με την εμπιστευτικότητα είναι η αναδρομολόγηση (re-routing) και η αποκάλυψη της πληροφορίας σε μη εξουσιοδοτημένους χρήστες [31]. Κάτι τέτοιο ενδέχεται να συμβεί κατά τη μετάδοση, οπότε υπάρχει ο κίνδυνος υποκλοπής (interception) αρχείων και φακέλων, ή στη βάση δεδομένων, όπου πιθανόν να αντιμετωπιστούν περιστατικά διείσδυσης (intrusion), αντιποίησης ταυτότητας (identity usurpation) ή «δούρειοι ίπποι» (Trojan horses) που θα αφήσουν ένα ανοικτό «παράθυρο» πρόσβασης μέσω του δικτύου. Η απαίτηση για εμπιστευτικότητα στο κανάλι επικοινωνίας διασφαλίζεται με την υιοθέτηση πρωτοκόλλων ασφαλούς επικοινωνίας, όπως το SSL (Secure Sockets Layer), ενώ, προκειμένου για συστήματα σε ανοικτά δίκτυα, ο έλεγχος πρόσβασης μπορεί να γίνει με χρήση firewalls. Από την άλλη πλευρά, η απαίτηση για εμπιστευτικότητα των δεδομένων καλύπτεται με τεχνικές κρυπτογράφησης [30]-[32].

Η κρυπτογραφία αποτελεί την πιο διαδεδομένη τεχνολογία στον τομέα της ασφάλειας δεδομένων κατά τη μετάδοσή τους μέσω δημοσίων επικοινωνιακών δικτύων [33]. Τα κρυπτογραφικά συστήματα δημοσίου κλειδιού (public-key cryptography) παρέχουν την τεχνική υποδομή που χρησιμοποιείται συνήθως για να προστατευθεί η ασφάλεια των δεδομένων ως προς την εμπιστευτικότητα, την πιστοποίηση και την ακεραιότητά τους. Σε συστήματα δημοσίου κλειδιού («ασύμμετρα συστήματα») χρησιμοποιείται ένα ζεύγος κλειδιών, το δημόσιο και το ιδιωτικό κλειδί, τα οποία κρυπτογραφούν και αποκρυπτογραφούν αντίστοιχα το μήνυμα. Τα δύο κλειδιά έχουν μια μαθηματική σχέση μεταξύ τους, αλλά είναι

υπολογιστικά αδύνατο να εξαγάγει κάποιος το ιδιωτικό κλειδί έχοντας γνώση του δημοσίου. Ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί της οντότητας με την οποία επιθυμεί να επικοινωνήσει προκειμένου να κρυπτογραφήσει το μήνυμα. Το κρυπτογραφημένο μήνυμα μπορεί στη συνέχεια να αποκρυπτογραφηθεί μόνο από τον παραλήπτη που έχει στην κατοχή του το αντίστοιχο ιδιωτικό κλειδί. Με αυτόν τον τρόπο διασφαλίζεται η προστασία των δεδομένων από μη εξουσιοδοτημένη χρήση και κατά συνέπεια ικανοποιείται η απαίτηση για εμπιστευτικότητα.

Ο κίνδυνος τροποποίησης ή καταστροφής των ιατρικών δεδομένων αντιμετωπίζεται προληπτικά με μηχανισμούς ασφάλειας που προορίζονται και για την τήρηση της εμπιστευτικότητας, καθώς αποτελεί σημαντικό μέτρο προστασίας ο περιορισμός των δικαιωμάτων προσπέλασης και διαχείρισης της κρίσιμης πληροφορίας μόνο σε εξουσιοδοτημένα άτομα. Η ακρίβεια και αξιοπιστία των ιατρικών δεδομένων μπορεί επομένως να προστατευτεί μέσω αναγνώρισης και πιστοποίησης του χρήστη (αποφυγή πλαστοπροσωπίας), με χρήση απλών κωδικών πρόσβασης στο σύστημα (passwords) ή/και μέσω ισχυρών μηχανισμών πιστοποίησης βάσει ψηφιακής υπογραφής (προαιρετικά με χρήση έξυπνης κάρτας). Στην προστασία της αξιοπιστίας των δεδομένων συμβάλλει επίσης ο διαχωρισμός δικαιωμάτων πρόσβασης για απλή ανάγνωση ή τροποποίηση των δεδομένων και η ύπαρξη συστήματος καταγραφής κίνησης (audit trail). Το τελευταίο είναι αναγκαίο επειδή εκτός από την απειλή που υπάρχει από τους χωρίς άδεια πρόσβασης χρήστες, πρέπει να ληφθούν μέτρα αποφυγής προβλημάτων και από τους νόμιμους χρήστες. Τα firewalls χρησιμεύουν στον έλεγχο της πρόσβασης και την παρακολούθηση της επικοινωνίας του εσωτερικού με το εξωτερικό δίκτυο, ενισχύοντας την προστασία της ευαίσθητης πληροφορίας από επίδοξους παράνομους διαχειριστές της. Ο βασικός όμως τρόπος κάλυψης των απαιτήσεων για ακεραιότητα και μη αποποίηση ευθύνης είναι η χρήση ψηφιακής υπογραφής, που παίζει τον ίδιο ρόλο με την πραγματική υπογραφή, λειτουργώντας ως «σφραγίδα» εγκυρότητας των δεδομένων και του αποστολέα τους [31]-[34]. Η δημιουργία των ψηφιακών υπογραφών που στοχεύουν στην πιστοποίηση της γνησιότητας και ακεραιότητας των δεδομένων βασίζεται σε τεχνολογίες κρυπτογράφησης. Ο αποστολέας των δεδομένων μπορεί κωδικοποιώντας τα δεδομένα με χρήση του ιδιωτικού του κλειδιού να δημιουργήσει

την ψηφιακή υπογραφή του, την οποία και θα προσαρτήσκει στα δεδομένα αυτά. Με αυτόν τον τρόπο δίνεται η δυνατότητα στον παραλήπτη να πιστοποιήσει την πηγή προέλευσης των δεδομένων και την ακεραιότητά τους, χρησιμοποιώντας το αντίστοιχο δημόσιο κλειδί και ελέγχοντας εάν η προκύπτουσα ψηφιακή υπογραφή είναι ίδια με αυτήν που συνοδεύει τα δεδομένα. Εάν ο παραλήπτης διαπιστώσει ότι η προκύπτουσα ψηφιακή υπογραφή διαφέρει από την αρχική, συνεπάγεται ότι τα δεδομένα έχουν υποστεί κάποια μεταβολή κατά τη μετάδοσή τους ή υπάρχει αναντιστοιχία δημόσιου και ιδιωτικού κλειδιού, οπότε σε αυτήν την περίπτωση δεν υπάρχουν εγγυήσεις ούτε για την ακεραιότητα των δεδομένων ούτε για την πηγή προέλευσής τους.

Η απαίτηση για απόδειξη του χρόνου αποστολής – λήψης πληροφορίας καλύπτεται με χρήση χρονικής σφραγίδας (time-stamp), η οποία επικολλείται στα δεδομένα και δηλώνει τη χρονική στιγμή της δημιουργίας ή/και αποστολής τους. Και αυτός ο μηχανισμός βασίζεται σε λειτουργίες κρυπτογράφησης και ψηφιακής υπογραφής.

Όσον αφορά τη διαθεσιμότητα, οι κύριες απειλές περιλαμβάνουν την εξουδετέρωση του συστήματος διαχείρισης αρχείων, την καταστροφή κάποιου σκληρού δίσκου και την εσκεμμένη ή μη αλλοίωση της δομής ή του περιεχομένου της πληροφορίας, συνυπολογίζοντας και τον παράγοντα ανθρώπινου λάθους [31]. Στις απειλές που αφορούν τη διαθεσιμότητα περιλαμβάνεται και η μη εξουσιοδοτημένη πρόσβαση σε πόρους εσωτερικού δικτύου [32]. Απαιτείται επομένως η αυστηρή εφαρμογή των κανόνων διαχείρισης δεδομένων (έλεγχος πρόσβασης, παρακολούθηση ενεργειών κ.λπ.), η χρήση αρχιτεκτονικών firewall και η τεχνική προστασία κρίσιμων μηχανημάτων και συσκευών (π.χ. δημιουργία αντιγράφων ασφαλείας).

Αξίζει να σημειωθεί ότι η επιλογή και εφαρμογή των κατάλληλων τεχνικών μέτρων επιβάλλεται να γίνει στα πλαίσια σαφώς καθορισμένων Πολιτικών Ασφαλείας για κάθε επίπεδο ασφάλειας (φυσικό, τεχνικό, δικτύου, δεδομένων).

Ο Πίνακας 1 συνοψίζει τους μηχανισμούς ασφάλειας που χρησιμοποιούνται κατά βάση στα σύγχρονα συστήματα διαχείρισης ιατρικής πληροφορίας [34]:

Υπηρεσία Ασφάλειας	Μηχανισμός Ασφάλειας
Αναγνώριση / πιστοποίηση οντοτήτων και πηγής προέλευσης	Ψηφιακή Υπογραφή
Εξουσιοδότηση και έλεγχος πρόσβασης	Ψηφιακή Υπογραφή, κρυπτογραφία, λίστες ελέγχου πρόσβασης
Ακεραιότητα	Ψηφιακή Υπογραφή, τιμές επαλήθευσης (check values)
Εμπιστευτικότητα	Κρυπτογραφία
Υπευθυνότητα (Accountability)	Σύστημα καταγραφής κίνησης (Audit trail)
Διαθεσιμότητα	Λίστες ελέγχου πρόσβασης, ψηφιακή υπογραφή, διαφύλαξη κλειδιών (key escrow)
Μη αποποίηση (non-repudiation)	Ψηφιακή Υπογραφή

Πίνακας 1: Μηχανισμοί παροχής υπηρεσιών ασφάλειας

3.6 ΠΕΡΙΟΡΙΣΜΟΙ ΥΦΙΣΤΑΜΕΝΩΝ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ

Είναι γεγονός ότι τα μέτρα ασφαλείας που προαναφέρθηκαν έχουν κάποιους περιορισμούς και δεν εξασφαλίζουν απόλυτη προστασία. Όσον αφορά την πρόσβαση στο σύστημα, τα firewalls απομονώνουν το εσωτερικό δίκτυο (intranet) από το διαδίκτυο ως ένα βαθμό, μπορούν όμως σχετικά εύκολα να παρακαμφθούν από εισβολείς (hackers). Επιπλέον, οι επικεφαλίδες (headers) των αρχείων είναι σε μορφή απλού κειμένου (plain-text format) και κατά συνέπεια μπορούν να προσπελαστούν από μη εξουσιοδοτημένους χρήστες. Από την άλλη μεριά, η κρυπτογραφία αποτελεί ένα αποτελεσματικό εργαλείο για την προστασία των δεδομένων κατά τη μετάδοση και αποθήκευσή τους, αδυνατεί όμως να τα προστατεύσει μετά την αποκρυπτογράφησή τους. Από τη στιγμή που τα δεδομένα αποκρυπτογραφούνται, εκτίθενται στον κίνδυνο της πρόσβασης και αλλοίωσής τους από κακόβουλους χρήστες. Η παραβίαση των δικαιωμάτων πρόσβασης και των αρχείων καταγραφής κίνησης (log files) οδηγεί σε ρήξη της εμπιστευτικότητας και σε αδυναμία εγγύησης ως προς την ακεραιότητα και την πιστοποίηση των δεδομένων. Έναν πρόσθετο περιορισμό αποτελεί το γεγονός ότι τα κρυπτογραφημένα κείμενα

είναι ιδιαίτερα ευαίσθητα σε σφάλματα στα bits που συμβαίνουν κατά την αποθήκευση ή μετάδοση των δεδομένων, πρόβλημα όμως που μπορεί να αντιμετωπιστεί με τη χρήση κάποιου κώδικα διόρθωσης σφαλμάτων (error correction code).

Όπως διαπιστώνεται τα τελευταία χρόνια και στη βιβλιογραφία, η υδατογραφία αποτελεί μια νέα τεχνολογία που έχει τη δυνατότητα να δώσει συμπληρωματικές ή/και εναλλακτικές λύσεις σε ζητήματα ασφάλειας δεδομένων. Στο επόμενο κεφάλαιο περιγράφονται οι προοπτικές της υδατογραφίας στον ιατρικό τομέα, οι οποίες δεν περιορίζονται μόνο στο ζήτημα της ασφάλειας, αλλά επεκτείνονται και σε μια σειρά άλλων καίριων ιατρικών εφαρμογών.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

- [1] T. Huston, "Security issues for implementation of e-medical records," Communications of the ACM, vol. 44, no. 9, pp. 89-94, September 2001.
- [2] R. L. Simpson "Ensuring patient data, privacy, confidentiality, and security", Nursing Management, vol. 25, no. 7, pp. 18-20, July 1994.
- [3] F. Cao, H. K. Huang, X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," Computerized Medical Imaging and Graphics, vol. 27, no. 2-3, pp. 185-196, March-June 2003.
- [4] A. E. James, E. James, B. Johnson, J. James, "Legal considerations of medical imaging", The Journal of Legal Medicine, pp. 87-113, 1993.
- [5] S. B. Berger, B. B. Cepelewicz, "Medical-legal issues in teleradiology", AJR American journal of roentgenology, no. 166, pp. 505-510, 1996.
- [6] L. Berlin, "Malpractice issue in radiology-teleradiology", AJR American journal of roentgenology, no. 170, pp. 1417-22, 1998.
- [7] G. H. Kamp, "Medical-legal issues in teleradiology: a commentary". AJR American journal of roentgenology, no. 166, pp.511-512, 1996.
- [8] D. Kohl, "Crossing the privacy minefield", Health Management Technology, vol. 16, no. 9, p. 50, Aug. 1995.
- [9] HIPAA, <http://aspe.os.dhhs.gov/admnsimp>, US Department of Health and Human Services.
- [10] HIPAA, <http://www.rx2000.org/KnowledgeCenter/hipaa/hipfaq.htm>.
- [11] Department of Health and Human Services. Security and electronic signature standards. Federal Register 63, 55 (Aug. 12, 1998).
- [12] Security and Privacy: An Introduction to HIPAA, Privacy and Security Committee, Medical Imaging Informatics Section, NEMA. Available at: <http://medical.nema.org/privacy/privacy.html>
- [13] European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry. <http://www.cocir.org>
- [14] Japan Industries Association of Radiological Systems. <http://www.jira-net.or.jp/e/index.htm>

- [15] Digital Imaging and Communications in Medicine (DICOM). National Electrical Manufacturers Association (NEMA). Rosslyn, VA, <http://medical.nema.org/dicom/2001.html>, Part 15: Security Profiles, PS 3.15-2001; 2001.
- [16] H. K. Huang, F. Cao, J. G. Zhang, B. J. Liu, M. L. Tsai, "Fault tolerant picture archiving and communication system and teleradiology design", Chapter 8, in "Security Issues in the Digital Medical Enterprise", Editors: Bruce I. Reiner et al., Society for Computer Applications in Radiology (SCAR) University Primer, vol. I, pp. 57-64, Nov. 2000.
- [17] G.O. Klein, "Standardization of health informatics - results and challenges", Yearbook of Medical Informatics 2002, pp. 103-114.
- [18] CEN/TC 251: <http://www.centc251.org>
- [19] ISO/TC 215: <http://isotc.iso.org>
- [20] Health Level 7 (HL7): <http://www.hl7.org>
- [21] IEEE 1073 General Committee: <http://www.ieee1073.org>
- [22] OECD Guidelines for the Security of Information Systems and Networks (2002). Available: <http://www.oecd.org/dataoecd/16/22/15582260.pdf>
- [23] Charter of Fundamental Rights of the European Union, 2000. Available: http://ec.europa.eu/justice_home/unit/charte/index_en.html
- [24] European Commission Legislative Documents. Available: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm
- [25] Recommendation no. R (97) 5 on the protection of medical data. Available: <http://www.legislationline.org/legislation.php?tid=219&lid=6140>
- [26] Recommendation No R (99) 5 on the protection of privacy on the internet – Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways. Available: http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/1_standard_settings/Rec_1999_5.pdf
- [27] European Group on Ethics in Science and New Technologies, Opinion No 13 – Ethical issues of healthcare in the information society, 1999. Available: http://ec.europa.eu/european_group_ethics/docs/avis13_en.pdf

- [28] Νόμος 2472/1997 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Available: <http://www.dpa.gr/law2472.htm>
- [29] Νόμος 2774//1999 περί προστασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα. Available: www.dpa.gr/Documents/Gre/Nomoi/2774.doc
- [30] S. Tzelepi, G. Pangalos, G. Nikolacopoulou, "Security of medical multimedia," *Med. Inform.*, vol. 27, no. 3, pp. 169-184, 2002.
- [31] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, "Relevance of watermarking in medical imaging," in *Proc. 3rd Conf. Information Technology Applications in Biomedicine, ITAB'00*, Arlington, USA, pp. 250-255.
- [32] J. Dittmann, K. Nahrstedt, P. Wohlmacher, "A survey of Multimedia Security," *Multimedia and Security Workshop at ACM Multimedia '99*, Orlando, Florida, Oct.99.
- [33] B. Schneier, "Applied cryptography: protocols, algorithms, and source code in C", John Wiley & Sons, 1996.
- [34] B. Blobel, F. Roger-France, "A systematic approach for analysis and design of secure health information systems", *International Journal of Medical Informatics*, no. 62, pp. 51-78, 2001.

ΚΕΦΑΛΑΙΟ 4

ΠΡΟΟΠΤΙΚΕΣ ΨΗΦΙΑΚΗΣ ΥΔΑΤΟΓΡΑΦΙΑΣ ΣΤΗ ΔΙΑΧΕΙΡΙΣΗ ΙΑΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

4.1 ΙΑΤΡΙΚΕΣ ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΨΗΦΙΑΚΗΣ ΥΔΑΤΟΓΡΑΦΙΑΣ

Οι τεχνολογικές εξελίξεις που έχουν σημειωθεί τα τελευταία χρόνια στους τομείς της πληροφορικής και των επικοινωνιών δημιούργησαν ένα νέο πλαίσιο εύκολης πρόσβασης, διαχείρισης και διανομής των ψηφιακών δεδομένων. Η εφαρμογή των νέων τεχνολογιών στα συστήματα παροχής ιατρικής περίθαλψης προσφέρει νέες πρακτικές και δυνατότητες στους γιατρούς και τους ασθενείς, αλλά φέρνει παράλληλα νέες προκλήσεις στο προσκήνιο. Τα Νοσοκομειακά Πληροφοριακά Συστήματα (Hospital Information Systems, HIS) και τα Συστήματα Αρχειοθέτησης και Μετάδοσης Εικόνων (Picture Archiving and Communication Systems, PACS) αποτελούν βασικά δομικά στοιχεία των σύγχρονων ολοκληρωμένων συστημάτων παροχής ιατρικής περίθαλψης, τα οποία παρέχουν εύκολη πρόσβαση, διαχείριση και διανομή ιατρικών δεδομένων. Η μετάδοση ιατρικών εικόνων και στοιχείων μέσω ενδονοσοκομειακών, δια-νοσοκομειακών και τηλεϊατρικών δικτύων, καθιστά την ασφάλεια δεδομένων ένα ζήτημα πρώτης προτεραιότητας. Ιδιαίτερα

λόγω της ευαίσθητης φύσης των προσωπικών δεδομένων των ασθενών, είναι επιτακτική η ανάγκη προστασίας από μη εξουσιοδοτημένη πρόσβαση και τήρησης του ιατρικού απορρήτου [1]-[3]. Εξαιρετικά σημαντική είναι επίσης η προστασία των δεδομένων από ενδεχόμενη τροποποίησή τους – εσκεμμένη ή μη – η οποία θα μπορούσε να οδηγήσει σε λανθασμένη διάγνωση. Στα ιατρικά πληροφοριακά συστήματα παίζει επομένως σημαντικό ρόλο ο έλεγχος της ακεραιότητας και η πιστοποίηση των ιατρικών εικόνων. Απαιτείται επιπλέον εξακρίβωση της πηγής προέλευσης, δηλαδή πιστοποίηση της ταυτότητας του γιατρού που κάνει την εξέταση και ελέγχει τα αποτελέσματα. Από την άλλη πλευρά, οι εξελίξεις στην τεχνολογία της πληροφορίας έδωσαν σημαντική ώθηση στην ανάπτυξη και επέκταση των ιατρικών ψηφιακών βιβλιοθηκών (Digital Libraries in Medicine), οι οποίες στοχεύουν στην παροχή γρήγορης και αποδοτικής ανάκτησης δεδομένων από βάσεις που διαθέτουν τεράστιο και εκθετικά αυξανόμενο όγκο ιατρικής πληροφορίας. Με αυτόν τον τρόπο ενισχύεται η δημιουργία νέας γνώσης και προωθείται η υιοθέτηση της «βέλτιστης πρακτικής» (best-practice) στον προγραμματισμό της ιατρικής περιθαλψής. Στα πλαίσια επιδίωξης αποδοτικής διαχείρισης γνώσης (knowledge management) καθίσταται εξαιρετικά σημαντική η εύρεση καινοτόμων μηχανισμών για αποδοτική αναπαράσταση και εύκολη ανάκτηση ιατρικής πληροφορίας [4], [5]. Στο πλαίσιο που διαμορφώνεται από τις σύγχρονες τεχνολογίες πρόσβασης και μετάδοσης πληροφορίας, εγείρονται πρόσθετα κρίσιμα ζητήματα για τα οποία πρέπει να ληφθούν άμεσα μέτρα, ιδιαίτερα για αυτά που σχετίζονται με τους αυξημένους κινδύνους για την ασφάλεια. Είναι επομένως φανερό η ανάγκη υιοθέτησης πρόσθετων μέτρων και πρωτοκόλλων ασφαλείας στα ιατρικά πληροφοριακά συστήματα. Η ερευνητική κοινότητα καταβάλλει μεγάλη προσπάθεια στις μέρες μας να βρει νέους τρόπους αποδοτικής και, ει δυνατόν, ενιαίας αντιμετώπισης των παραπάνω θεμάτων.

Η ψηφιακή υδατογραφία αποτελεί ένα σχετικά καινούριο ερευνητικό πεδίο που αρχικά επικεντρώθηκε στην κατοχύρωση των πνευματικών δικαιωμάτων των δημιουργών, σύντομα όμως διαπιστώθηκε η δυνατότητα αξιοποίησής της σε μια ευρεία κλίμακα εφαρμογών [6]-[8]. Προς το παρόν υπάρχουν στη βιβλιογραφία λίγες μελέτες σχετικά με τη χρήση υδατογραφίας σε ιατρικές εφαρμογές, ωστόσο

διαφαίνεται ήδη η προοπτική της σε πληθώρα ιατρικών εφαρμογών, όπως στην προστασία του ιατρικού απορρήτου, την παροχή πρόσθετης βοηθητικής πληροφορίας σχετικής με τον ασθενή και την εξέταση, την πιστοποίηση της πηγής προέλευσης και τον έλεγχο ακεραιότητας των δεδομένων. Η ψηφιακή υδατογραφία παρέχει τη δυνατότητα ενσωμάτωσης πληροφορίας απευθείας στις ιατρικές εικόνες μέσω ανεπαίσθητης τροποποίησης είτε των αρχικών δεδομένων είτε κάποιας μετασχηματισμένης εκδοχής τους [9]. Καθώς οι διάφοροι τύποι υδατογραφημάτων ικανοποιούν τις βασικές απαιτήσεις (ανθεκτικότητα, διαφάνεια, χωρητικότητα) σε διαφορετικό βαθμό, η επιλογή του κατάλληλου υδατογραφήματος εξαρτάται από την εκάστοτε εφαρμογή. Επομένως κατά τη σχεδίαση ενός υδατογραφικού σχήματος προορισμένου για χρήση σε ιατρικές εφαρμογές θα πρέπει να ληφθούν υπόψη οι ιδιαίτερες απαιτήσεις κάθε εφαρμογής, σε συνδυασμό με τους ειδικούς περιορισμούς στους οποίους υπόκεινται τα ιατρικά δεδομένα, προκειμένου να καθοριστούν οι κατάλληλοι τύποι υδατογραφημάτων. Είναι φανερό ότι και στις ιατρικές εφαρμογές καλείται το υδατογραφικό σχήμα να ανταποκριθεί σε ένα σύνολο ζητούμενων χαρακτηριστικών που είναι αντιφατικά μεταξύ τους, λόγω της ιδιαιτερότητας κάθε εφαρμογής. Επιδιωκόμενο αποτέλεσμα είναι στην ιδανική περίπτωση η σχεδίαση ενός ενιαίου σχήματος που θα ανταποκρίνεται στο σύνολο των εφαρμογών, ή τουλάχιστον η ταυτόχρονη εφαρμογή περισσότερων τεχνικών που θα επιτρέπουν την ανεξάρτητη διαχείριση πολλαπλών υδατογραφημάτων που προορίζονται για διαφορετικούς σκοπούς.

Οι ιατρικές εικόνες έχουν ιδιαίτερα χαρακτηριστικά και απαιτήσεις σε σύγκριση με άλλα είδη εικόνων. Επίσης υπόκεινται σε πρόσθετους νομικούς και ηθικούς περιορισμούς ως προς τη δυνατότητα επεξεργασίας τους, καθώς ο οποιοσδήποτε συμβιβασμός όσον αφορά την ποιότητά τους ενέχει τον κίνδυνο να οδηγήσει σε λανθασμένη διάγνωση [10]-[12]. Είναι σαφές ότι η σχεδίαση ενός υδατογραφικού σχήματος που προορίζεται για επίλυση θεμάτων που άπτονται της διαχείρισης ιατρικής πληροφορίας, θα πρέπει να συμμορφώνεται με τις νομικές και ηθικές αρχές που διέπουν τον τομέα της υγείας. Η τήρηση των αυστηρών προδιαγραφών που αφορούν την ποιότητα των ιατρικών εικόνων μπορεί να εξασφαλιστεί με χρήση αντιστρεπτής υδατογραφίας (invertible watermarking), που

επιτρέπει την ανάκτηση της αρχικής εικόνας χωρίς απώλεια πληροφορίας [13], [14]. Οι τεχνικές αντιστρεπτής υδατογραφίας όμως χαρακτηρίζονται από περιορισμένη χωρητικότητα, γεγονός που τις καθιστά μάλλον ακατάλληλες για εφαρμογές απόκρυψης πρόσθετης πληροφορίας, στις οποίες απαιτείται η εισαγωγή μεγάλου αριθμού bits στην εικόνα. Μια εναλλακτική λύση αποτελεί η διάκριση των περιοχών όπου επιτρέπεται η εισαγωγή υδατογραφήματος από τις περιοχές ενδιαφέροντος (Regions Of Interest – ROI), οι οποίες δε χρησιμοποιούνται για ενσωμάτωση υδατογραφήματος προκειμένου να διασφαλιστεί η διαγνωστική τους αξία [15]. Το υπόλοιπο τμήμα της εικόνας μπορεί να χρησιμοποιηθεί για προσθήκη υδατογραφήματος με αυξημένη σχετικά ανθεκτικότητα ή/και χωρητικότητα, καθώς δεν υπόκειται στις ιδιαίτερα αυστηρές απαιτήσεις διαφάνειας που ισχύουν για τις διαγνωστικά σημαντικές περιοχές. Υπάρχει πάντως η άποψη ότι σταδιακά θα αρθούν οι επιφυλάξεις και θα υιοθετηθούν και από ιατρικές εφαρμογές υδατογραφικά σχήματα που χρησιμοποιούν ολόκληρη την εικόνα χωρίς να προκαλούν ορατή αλλοίωση [10].

Παρακάτω γίνεται παρουσίαση των θεμάτων που άπτονται της διαχείρισης ιατρικών δεδομένων και στα οποία η συμβολή της ψηφιακής υδατογραφίας αναμένεται να αποδειχθεί ιδιαίτερα σημαντική [16], [17]:

- *Έλεγχος πρόσβασης*: η προστασία του ιατρικού απορρήτου αποτελεί ένα ζήτημα μείζονος σημασίας, απαιτούνται επομένως συμπληρωματικές λύσεις προκειμένου να περιοριστεί η πρόσβαση στα ευαίσθητα ιατρικά δεδομένα μόνο σε εξουσιοδοτημένα άτομα. Κάθε μέλος του προσωπικού θα πρέπει να μπορεί να προσπελάσει και να τροποποιήσει προσωπικά / ιατρικά δεδομένα ανάλογα με τα δικαιώματα πρόσβασής του. Είναι προφανές ότι ένας νοσοκόμος έχει περιορισμένα δικαιώματα σε σχέση με ένα γιατρό. Η χρήση διαφορετικών υδατογραφικών κλειδιών επιτρέπει την αποκωδικοποίηση διαφορετικής πληροφορίας, γεγονός που καθιστά την ψηφιακή υδατογραφία έναν αποδοτικό μηχανισμό ελέγχου πρόσβασης [18], συμβάλλοντας στην προστασία του ιατρικού απορρήτου. Δεδομένα όπως το όνομα του ασθενή, ο κωδικός αναγνώρισής του, η ημερομηνία και η ώρα της εξέτασης (time-stamp), η κλινική

όπου διενεργήθηκε η εξέταση, ή ακόμη και διαγνωστικές αναφορές και το ιατρικό ιστορικό του ασθενή, μπορούν να ενσωματωθούν ως υδατογραφήματα σε ιατρικές εικόνες. Με αυτόν τον τρόπο αποφεύγεται η ξεχωριστή μετάδοση και αποθήκευση μεταδεδομένων, η οποία θα οδηγούσε σε αυξημένες απαιτήσεις μνήμης και εύρους μετάδοσης [19]-[22]. Ένα πρόσθετο πλεονέκτημα είναι ότι τα ευαίσθητα προσωπικά δεδομένα είναι σαφώς πιο προστατευμένα σε σύγκριση με τα μεταδεδομένα, καθώς η πρόσβαση σε αυτά είναι εφικτή μόνο εν γνώσει του μυστικού κλειδιού που χρησιμοποιείται για την εισαγωγή των υδατογραφημάτων [10], [23]. Επιπλέον, η μόνιμη σύνδεση των δεδομένων αυτών με την αντίστοιχη εικόνα αποτρέπει το ενδεχόμενο της εσφαλμένης αντιστοίχισης εικόνων – ασθενούς, η οποία θα μπορούσε να οδηγήσει σε λανθασμένη διάγνωση και θεραπευτική αγωγή [24].

- *Αναγνώριση προέλευσης:* η πιστοποίηση της πηγής από την οποία προήλθαν τα δεδομένα είναι βασικό στοιχείο στη διαχείριση ιατρικής πληροφορίας, δηλαδή ο γιατρός που διενεργεί την εξέταση και εξάγει τα αποτελέσματα είναι υποχρεωμένος να πιστοποιεί την ταυτότητά του. Η εισαγωγή στα ιατρικά δεδομένα ενός υδατογραφήματος που περιέχει τον κωδικό αναγνώρισης ή την ψηφιακή υπογραφή του γιατρού παρέχει έναν τρόπο ταυτοποίησής του [19]-[21]. Η ψηφιακή υδατογραφία μπορεί να συνδυαστεί αποτελεσματικά με την κρυπτογραφία για πρόσθετη ασφάλεια σε εφαρμογές πιστοποίησης [18], [21], [24]. Η ενσωμάτωση στα δεδομένα ενός υδατογραφήματος που αποτελείται από μια κρυπτογραφημένη εκδοχή της ψηφιακής υπογραφής του γιατρού προσφέρει ένα υψηλότερο επίπεδο ασφάλειας στην πιστοποίηση της πηγής προέλευσης, καθώς ο κωδικός αναγνώρισης δεν είναι απλώς κρυμμένος στα δεδομένα, αλλά και κρυπτογραφημένος. Για την πρόσβαση σε αυτόν επομένως απαιτείται η γνώση των δύο κλειδιών που χρησιμοποιήθηκαν για την ενσωμάτωση και την κρυπτογράφησή του, γεγονός που εγγυάται αυξημένη ασφάλεια.
- *Έλεγχος ακεραιότητας:* η προστασία της ιατρικής πληροφορίας από οποιασδήποτε μορφής αλλοίωση κατά τη μετάδοση ή αποθήκευσή της αποτελεί βασική προϋπόθεση προκειμένου να διασφαλιστεί η διαγνωστική της αξία.

Απαιτούνται επομένως αποδοτικοί μηχανισμοί ελέγχου ακεραιότητας των δεδομένων στα ιατρικά πληροφοριακά συστήματα [10], [11]. Για το σκοπό αυτόν ενδείκνυται η χρήση εύθραυστων υδατογραφημάτων, τα οποία παρέχουν τη δυνατότητα ελέγχου της ακεραιότητας των μεταδοθέντων ή αποθηκευμένων δεδομένων και επιπλέον προσδιορίζουν τα τμήματα εκείνα που υπέστησαν μεταβολές [25]. Η σύγκριση του εξαχθέντος υδατογραφήματος με το αρχικό υδατογράφημα αναφοράς φανερώνει την έκταση της αλλοίωσης, από την οποία τελικά κρίνεται και η αξιοπιστία των δεδομένων όσον αφορά τη δυνατότητα εξαγωγής έγκυρης διάγνωσης.

- *Προσθήκη επικεφαλίδων / σχολίων (captioning)*: η εισαγωγή υδατογραφημάτων που λειτουργούν ως τίτλοι ή σχόλια για τα απεικονιζόμενα στοιχεία δίνει τη δυνατότητα πρόσθετης βοηθητικής πληροφορίας σχετικής με τα προσωπικά δεδομένα του ασθενή, το ιατρικό του ιστορικό, αποτελέσματα εξετάσεων και άλλη πληροφορία που θα μπορούσε να συνεισφέρει στη διεξοδική αποτίμηση της κατάστασής του. Επίσης θα μπορούσαν να τονιστούν σημεία ιδιαίτερης διαγνωστικής αξίας μέσω περιγραφικών υδατογραφημάτων, για μελλοντική αναφορά ή καθοδήγηση άλλων γιατρών [26].
- *Αποπροσωποποίηση (de-identification)*: παρόλο που τα ευαίσθητα προσωπικά δεδομένα πρέπει να παραμένουν προστατευμένα και απροσπέλαστα από μη εξουσιοδοτημένους χρήστες, η απομάκρυνση των αναγνωριστικών στοιχείων από την ιατρική πληροφορία επιτρέπει τη χρήση της σε μη κλινικές εφαρμογές, προωθώντας την έρευνα για τη «βέλτιστη πρακτική». Οι υδατογραφημένες εικόνες μπορούν να χρησιμοποιηθούν για αυτόν το σκοπό, καθώς η υδατογραφία επιτρέπει κάποιας μορφής αποπροσωποποίηση: οι εικόνες μπορούν να περιέχουν ευαίσθητα προσωπικά δεδομένα που όμως παραμένουν προστατευμένα και απροσπέλαστα από μη εξουσιοδοτημένα άτομα που δε γνωρίζουν το κατάλληλο υδατογραφικό κλειδί.
- *Τοποθέτηση δεικτών (indexing)*: τα σύγχρονα πληροφοριακά συστήματα νοσοκομείων διαχειρίζονται και κατανέμουν τεράστιους όγκους ιατρικής

πληροφορίας, κάνοντας επιτακτική την ανάγκη εύρεσης εναλλακτικών λύσεων για αποδοτική διαχείριση των δεδομένων. Η υδατογραφία παρέχει έναν τρόπο εύκολης δεικτοδότησης, αρχειοθέτησης και διαχείρισης ιατρικών δεδομένων, καθώς τα υδατογραφήματα μπορούν να παίξουν το ρόλο δεικτών (indices) και ιχνηθετών (markers), στους οποίους θα βασιστεί η αποδοτική αρχειοθέτηση και εύκολη ανάκτηση δεδομένων από μηχανισμούς αναζήτησης (querying mechanisms). Η προσθήκη δεικτών ως υδατογραφήματα στις εικόνες έχει ως αποτέλεσμα μειωμένες απαιτήσεις μνήμης αποθήκευσης και εύρους μετάδοσης [27]. Οι δείκτες αυτοί θα μπορούσαν να περιλαμβάνουν δημογραφικά στοιχεία του ασθενή, διαγνωστικούς κωδικούς (π.χ. ICD-10, CPT), χαρακτηριστικά της εξέτασης (π.χ. εγκάρσια / στεφανιαία τομή) κ.λπ. Τα Συστήματα Αρχειοθέτησης και Μετάδοσης Εικόνων (PACS) στις μέρες μας επιτρέπουν ανάκτηση εικόνων βάσει της παραπάνω διαδικασίας. Τα τελευταία χρόνια έχουν καταγραφεί στη βιβλιογραφία ερευνητικές προσπάθειες αναζήτησης στοιχείων από βάσεις δεδομένων βάσει περιεχομένου (content-based querying) [28]-[31]: τα υδατογραφήματα μπορούν να παίξουν το ρόλο των δεικτών και σε αυτήν την περίπτωση. Υπάρχουν ήδη στην αρθρογραφία κάποιες καινοτόμες τεχνικές που χρησιμοποιούν ανάλυση κυματιδίων (wavelets) στις εικόνες για εξαγωγή χαρακτηριστικών κατάλληλων για ανάκτηση εικόνων [32]. Αξίζει να σημειωθεί ότι η τεχνική που σχεδιάστηκε και αναπτύχθηκε στα πλαίσια της παρούσας διδακτορικής διατριβής, βασίζεται στο μετασχηματισμό κυματιδίων για την ενσωμάτωση πολλαπλών υδατογραφημάτων σε ιατρικές εικόνες, γεγονός που επιτρέπει την εύκολη προσαρμογή της ώστε να υποστηρίζει αναζήτηση εικόνων βάσει περιεχομένου [16].

- *Καταγραφή ενεργειών*: η τήρηση αρχείων με το σύνολο των μεταβολών που σημειώνονται στα ιατρικά δεδομένα είναι εφικτή με τη χρήση κατάλληλων υδατογραφημάτων.

Τα παραπάνω φανερώνουν την προοπτική της ψηφιακής υδατογραφίας σε πληθώρα ιατρικών εφαρμογών, καθώς έχει τη δυνατότητα να αποτελέσει ένα

εργαλείο που διευκολύνει και αναβαθμίζει τη διαχείριση δεδομένων σε ιατρικά πληροφοριακά συστήματα.

4.2 ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΡΕΥΝΑ

Παρά το γεγονός ότι τα τελευταία χρόνια η βιβλιογραφία εμπλουτίστηκε σημαντικά με μελέτες που αφορούν ποικίλες υδατογραφικές εφαρμογές και τεχνικές, μόλις πρόσφατα άρχισαν να διερευνώνται οι προοπτικές της τεχνολογίας αυτής σε ιατρικές εφαρμογές.

Ο Coatrieux και οι συνεργάτες του πρότειναν τη χρήση υδατογραφίας ως συμπληρωματικού μέτρου προστασίας των ιατρικών εικόνων και παρουσίασαν τις προϋποθέσεις που πρέπει να πληρούνται προκειμένου να γίνει αποδεκτό σε ιατρικό περιβάλλον ένα υδατογραφικό σύστημα [10]. Διασαφήνισαν το συμπληρωματικό ρόλο ενός τέτοιου συστήματος στα πλαίσια των υφιστάμενων μέτρων ασφαλείας και εξέτασαν ένα σενάριο εφαρμογής του στην πιστοποίηση και ανίχνευση (tracing) εικόνων και ένα δεύτερο για έλεγχο ακεραιότητας του ιατρικού φακέλου. Σε επόμενο άρθρο τους επανεξέτασαν το ρόλο της υδατογραφίας στον τομέα της ασφάλειας ιατρικών πληροφοριακών συστημάτων και εστίασαν στον έλεγχο ακεραιότητας των ιατρικών εικόνων, προτείνοντας τον καθορισμό μιας Περιοχής Ενδιαφέροντος που φέρει διαγνωστική πληροφορία και την εισαγωγή του υδατογραφήματος στην υπόλοιπη εικόνα (Region of non-Interest) [15]. Παρουσίασαν επίσης τα αποτελέσματα της σύγκρισης τριών εναλλακτικών σχημάτων εξαγωγής υπογραφών επικύρωσης ως προς την απόδοσή τους στην ανίχνευση παραποίησης των εικόνων.

Ο Wakatani πρότεινε την ενσωμάτωση μιας εικόνας ως ψηφιακή υπογραφή σε τμήματα της ιατρικής εικόνας που δεν ανήκουν στην περιοχή ενδιαφέροντος, ώστε να διατηρηθεί η διαγνωστική της αξία [11]. Πιο συγκεκριμένα, εφάρμοσε τον αλγόριθμο προοδευτικής συμπίεσης EZW (Embedded Zerotree Wavelet progressive coding) στην ψηφιακή υπογραφή και ενσωμάτωσε στην ιατρική εικόνα την προκύπτουσα ακολουθία bits, αντικαθιστώντας με αυτήν τα bits τυχαία επιλεγμένου επιπέδου (bit plane) των pixels που βρίσκονται εκτός περιοχής ενδιαφέροντος.

Ο Acharya και οι συνεργάτες του εφάρμοσαν την υδατογραφική τεχνική αντικατάστασης του ελάχιστου σημαντικού ψηφίου (Least Significant Bit - LSB) για να ενσωματώσουν κρυπτογραφημένα δεδομένα ηλεκτρονικού φακέλου ασθενή σε ιατρικές εικόνες, με σκοπό τη μείωση των απαιτήσεων αποθηκευτικής μνήμης και εύρους μετάδοσης [21]. Σύμφωνα με τη μέθοδό τους, το αρχείο κειμένου που περιέχει τα στοιχεία του ασθενή κρυπτογραφείται μέσω λογαριθμικής κωδικοποίησης, ενώ για το σήμα καρδιακής συχνότητας (Heart Rate) εφαρμόζονται τεχνικές διαφορικής παλμοκωδικής διαμόρφωσης (Differential Pulse Code Modulation – DPCM) και προσαρμοστικής δέλτα διαμόρφωσης (Adaptive Delta Modulation – ADM). Στη συνέχεια επανέλαβαν τις δοκιμές τους κάνοντας χρήση κώδικα διόρθωσης σφαλμάτων (error control coding), προκειμένου να βελτιώσουν την αξιοπιστία του συστήματος στη μετάδοση και αποθήκευση εικόνων παρουσία θορύβου ή άλλων παρεμβολών [33]. Σε επόμενη εργασία τους, ο Acharya και οι συνεργάτες του δοκίμασαν τη μέθοδο αντικατάστασης του ελάχιστου σημαντικού ψηφίου (LSB) στο πεδίο της συχνότητας [34]. Πιο συγκεκριμένα χώρισαν την εικόνα σε τετραγωνίδια (blocks) διαστάσεων 8x8 pixels, σε καθένα από τα οποία εφάρμοσαν Διακριτό Μετασχηματισμό Συνημιτόνου (DCT). Στη συνέχεια αντικατέστησαν το ελάχιστο σημαντικό ψηφίο των DCT συντελεστών που ανήκαν στην κλίμακα μεσαίων συχνοτήτων με τα bits της ακολουθίας που προέκυψε από την κρυπτογράφηση των στοιχείων του ιατρικού φακέλου. Σε πιο πρόσφατο άρθρο τους, παρέθεσαν μια συγκριτική παρουσίαση των αποτελεσμάτων εφαρμογής της μεθόδου αντικατάστασης LSB στα πεδία του χώρου και της συχνότητας, εξετάζοντας στη δεύτερη περίπτωση όχι μόνο το Διακριτό Μετασχηματισμό Συνημιτόνου (DCT), αλλά και τους Διακριτούς Μετασχηματισμούς Fourier (DFT) και κυματιδίων (DWT) [35]. Αξίζει πάντως να σημειωθεί ότι παρά την αμελητέα επίδραση της συγκεκριμένης μεθόδου στη διαγνωστική αξία των εικόνων και τη χαμηλή υπολογιστική της πολυπλοκότητα, στην πράξη είναι μη εφαρμόσιμη λόγω των γνωστών αδυναμιών και περιορισμών της που απορρέουν από την υπερβολική ευθραυστότητά της [36].

Ωστόσο, το γεγονός ότι η μέθοδος αντικατάστασης του ελάχιστου σημαντικού ψηφίου είναι εξαιρετικά ευάλωτη τόσο σε κακόβουλες επιθέσεις όσο και

σε συνηθισμένες ενέργειες επεξεργασίας της εικόνας, δεν απέτρεψε ούτε κάποιους άλλους ερευνητές να την εφαρμόσουν σε ιατρικά δεδομένα. Συγκεκριμένα, ο Zhou και οι συνεργάτες του εφάρμοσαν LSB υδατογράφιση για την επικύρωση της αυθεντικότητας και της ακεραιότητας ψηφιακών εικόνων μαστογραφίας [37]. Για το σκοπό αυτό, ενσωμάτωσαν στην εικόνα τον ψηφιακό ιατρικό φάκελο μέσω αντικατάστασης του ελάχιστου σημαντικού ψηφίου τυχαία επιλεγμένων pixels της εικόνας από τα bits της ακολουθίας που απάρτιζε το φάκελο. Η ακολουθία αυτή περιλάμβανε στοιχεία του ασθενή και την ψηφιακή υπογραφή που προέκυψε από την κρυπτογραφημένη «σύννοψη» (digest) της εικόνας, επιτρέποντας έτσι τον έλεγχο της αυθεντικότητας και της ακεραιότητας των δεδομένων. Προκειμένου να αποφευχθεί η αλλοίωση της «σύννοψης» της εικόνας λόγω της υδατογράφισης, εξαιρέθηκαν από τη διαδικασία υπολογισμού της τα ελάχιστα σημαντικά ψηφία των pixels της εικόνας. Σε επόμενο άρθρο τους, ο Zhou και οι συνεργάτες του παρουσίασαν το υφιστάμενο πλαίσιο προστασίας ιατρικών δεδομένων στα Συστήματα Αρχειοθέτησης και Μετάδοσης Εικόνων (Picture Archiving and Communication Systems – PACS) βάσει του προτύπου DICOM και ανέλυσαν τα πλεονεκτήματα και τα μειονεκτήματα της υδατογραφικής τεχνικής LSB σε σχέση με τα ισχύοντα μέτρα ασφάλειας [22].

Ο Chao και οι συνεργάτες του πρότειναν μια υδατογραφική τεχνική αντικατάστασης ελάχιστων σημαντικών ψηφίων (LSBs) που στοχεύει στην πιστοποίηση της γνησιότητας και ακεραιότητας των ιατρικών εικόνων και την προστασία του ιατρικού φακέλου του ασθενή [19], [20]. Το υδατογράφημα αποτελείται από ένα ηλεκτροκαρδιογράφημα, τη διαγνωστική αναφορά και την ψηφιακή υπογραφή του γιατρού και η ενσωμάτωσή του στην εικόνα γίνεται μέσω αλγορίθμου που χρησιμοποιεί αριθμητικό σύστημα «διπολικών πολλαπλών βάσεων» (bipolar multiple-number base). Πρέπει όμως να σημειωθεί ότι για την εξαγωγή του υδατογραφήματος, το σύστημα απαιτεί γνώση της αρχικής, μη υδατογραφημένης εικόνας, γεγονός που αναιρεί τη χρησιμότητά του στην πράξη.

Οι Macq και Dewey επικεντρώθηκαν στο θέμα της «αξιόπιστης επικεφαλίδας» (trusted header), προτείνοντας μια αντιστρέψιμη υδατογραφική τεχνική για την επικύρωση της επικεφαλίδας DICOM μέσω της ενσωμάτωσης της

«σύνοψης» της (hash) στην ιατρική εικόνα [38]. Η τεχνική αυτή χρησιμοποιεί «ψευδο-αθροίσματα» και «ψευδο-διαφορές» (pseudo-sum/differences) γειτονικών pixels της εικόνας για την ενσωμάτωση της «σύνοψης», η οποία στη συνέχεια συγκρινόμενη με τη «σύνοψη» που αντιστοιχεί στη ληφθείσα εικόνα επιτρέπει τον έλεγχο της ορθότητας αντιστοίχισης εικόνας – επικεφαλίδας.

Ο Trichili και οι συνεργάτες του πρότειναν την εφαρμογή «mirror effect» στην εικόνα για τη δημιουργία ενός εικονικού ορίου (virtual border), το οποίο χρησιμοποιείται για εισαγωγή στοιχείων του ασθενή [39]. Η υδατογράφιση γίνεται και σε αυτήν την περίπτωση με αντικατάσταση του ελάχιστου σημαντικού ψηφίου (LSB), ώστε να μη γίνει αντιληπτή.

Οι Kong και Feng συνέκριναν τρεις γνωστές υδατογραφικές τεχνικές ως προς τη δυνατότητα ελέγχου της ακεραιότητας σήματος από ηλεκτροεγκεφαλογράφημα (EEG) σε μια εφαρμογή ανίχνευσης εγκεφαλικής βλάβης [40]. Συγκεκριμένα δοκίμασαν τη μέθοδο patchwork, την αντικατάσταση ελάχιστου σημαντικού ψηφίου (LSB) και την κβαντοποίηση δεδομένων ως προς την ευαισθησία στην παρουσία θορύβου, την ανθεκτικότητα στις αλλαγές των χαρακτηριστικών του σήματος EEG λόγω εγκεφαλικής βλάβης και την απόδοση σε διαφορετικά κανάλια επικοινωνίας. Εφάρμοσαν «αυτοπαλινδρομική μοντελοποίηση» (autoregressive – AR) στο σήμα EEG και ενσωμάτωσαν το υδατογράφημα πιστοποίησης στην ακολουθία υπολοίπου (residual sequence). Το συμπέρασμα της μελέτης τους είναι ότι η τεχνική patchwork πλεονεκτεί σε συνθήκες μέτριου ρυθμού μετάδοσης σφαλμάτων (bit error rate) στο κανάλι επικοινωνίας, συνδυάζοντας μικρότερη πιθανότητα διέλευσης εσφαλμένων bits και μεγαλύτερο σηματοθορυβικό λόγο (SNR).

Οι Yang και Bao συνόψισαν σε άρθρο τους κάποιες μεθόδους αντιστρεπτής υδατογράφισης που έχουν προταθεί στη βιβλιογραφία και πρότειναν στη συνέχεια μια μέθοδο αποκλειστικά για πιστοποίηση ηλεκτρονικού κλινικού άτλαντα εγκεφάλου [41]. Η μέθοδος τους χρησιμοποιεί για υδατογράφιση το σύνολο μεταξύ διαφορετικών δομών στον άτλαντα και μεταβάλλει με αντιστρέψιμο τρόπο το χρώμα συγκεκριμένων σημείων του προκειμένου να ενσωματώσει την επιθυμητή δυαδική ακολουθία.

Πρόσφατα οι Puech και Rodrigues πρότειναν το συνδυασμό τεχνικών κρυπτογράφησης και υδατογράφησης για την ασφαλή μετάδοση ιατρικών εικόνων [42]. Η προτεινόμενη μεθοδολογία περιλαμβάνει κρυπτογράφηση της εικόνας με χρήση μυστικού κλειδιού, το οποίο κρυπτογραφείται με εφαρμογή σχήματος ιδιωτικού – δημοσίου κλειδιού και ενσωματώνεται στη συνέχεια στην κρυπτογραφημένη εικόνα. Η ενσωμάτωση του κρυπτογραφημένου κλειδιού γίνεται με εφαρμογή υδατογραφικής τεχνικής βασισμένης στο Διακριτό Μετασχηματισμό Συνημιτόνου (DCT). Σύμφωνα με τους Puech και Rodrigues, η μέθοδός τους είναι ανθεκτική σε συνθήκες μέτριου θορύβου, όπως για παράδειγμα στη συμπίεση JPEG με υψηλό συντελεστή ποιότητας.

Τέλος, ο Osborne και οι συνεργάτες του ανέπτυξαν μια ημι-εύθραυστη (semi-fragile) υδατογραφική τεχνική στοχεύοντας στην επικύρωση της ακεραιότητας της Περιοχής Ενδιαφέροντος (ROI) των ιατρικών εικόνων μετά τη μετάδοσή τους [43]. Η μέθοδος που χρησιμοποίησαν βασίζεται σε κβαντοποίηση και επιτρέπει την πολλαπλή ενσωμάτωση μιας υπογραφής σε τμήματα της εικόνας που δεν ανήκουν στην περιοχή ενδιαφέροντος. Η υπογραφή προκύπτει συγκρίνοντας τις τιμές των συντελεστών ψευδο-τυχαίων ζευγαριών που ανήκουν σε τετραγωνίδια (blocks) DCT της περιοχής ενδιαφέροντος. Οι συγγραφείς έδωσαν έμφαση στην ανθεκτικότητα της μεθόδου στη συμπίεση JPEG και τη μετάδοση των εικόνων στα - επιρρεπή σε σφάλματα - κανάλια ασύρματης μετάδοσης (error-prone mobile channels).

Όπως προκύπτει από την παραπάνω βιβλιογραφική ανασκόπηση, η εφαρμογή πολλαπλής υδατογράφησης στην ιατρική απεικόνιση με σκοπό την ενιαία προσέγγιση διαφορετικών θεμάτων διαχείρισης ιατρικών δεδομένων αποτελεί καινοτομική ιδέα και δεν έχουν καταγραφεί παρόμοιες ερευνητικές προσπάθειες στη βιβλιογραφία.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

- [1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, L 281, pp.31-50. Available at:
http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
- [2] Security and Privacy: An Introduction to HIPAA, Privacy and Security Committee, Medical Imaging Informatics Section, NEMA. Available at:
<http://medical.nema.org/privacy/privacy.html>
- [3] *ACR Standard for Digital Image Data Management*, American College of Radiology Standards, 2000. Available at:
http://www.acr.org/dyna/?doc=departments/stand_accred/standards/dl_list.html
- [4] Y. C. Li, "Toward a medical information collective: trends in the development of digital libraries in medicine", in *Yearbook of Medical Informatics 2001*, R. Haux, C. Kulikowski, Ed. Stuttgart: Schattauer Publ. Company, 2001, pp. 77-82.
- [5] S. Chu, "Information Retrieval and Health/Clinical Management", in *Yearbook of Medical Informatics 2002*, R. Haux, C. Kulikowski, Ed. Stuttgart: Schattauer Publ. Company, 2002, pp. 271-275.
- [6] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3&4, pp. 313-336, 1996.
- [7] M. Swanson, M. Kobayashi, A. Tewfik, "Multimedia data-embedding and watermarking technologies" in *Proc. IEEE*, vol. 86, no. 6, pp. 1064-1087, June 1998.
- [8] I. J. Cox, M. L. Miller, "The first 50 years of electronic watermarking," *EURASIP J. Applied Signal Processing*, vol. 2002, no. 2, pp. 126-132, Feb. 2002.
- [9] C. I. Podilchuk, E. J. Delp, "Digital watermarking: algorithms and applications," *IEEE Sig. Proc. Mag.*, vol. 18, no. 4, pp. 33-46, July 2001.
- [10] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, "Relevance of watermarking in medical imaging," in *Proc. 3rd Conf. Information Technology Applications in Biomedicine, ITAB'00*, Arlington, USA, pp. 250-255.

- [11] A. Wakatani, "Digital watermarking for ROI medical images by using compressed signature image," presented at the 35th Annu. Hawaii Intern. Conf. System Sciences, HICSS'02, Big Island, HI, USA.
- [12] A. Bruckmann, A. Uhl, "Selective medical image compression using wavelet techniques," J. Computing and Information Technology Special Issue on Biomedical Image Processing and Analysis, vol. 6, no. 2, pp. 203-213, 1998.
- [13] J. Fridrich, M. Goljan, R. Du, "Lossless data embedding for all image formats," in Proc. SPIE Photonics West, Security and Watermarking of Multimedia Contents, San Jose, CA, vol. 4675, pp. 572-583, Jan. 2002.
- [14] J. Fridrich, M. Goljan, R. Du, "Invertible authentication," in Proc. SPIE Photonics West, Security and Watermarking of Multimedia Contents, San Jose, CA, vol. 3971, pp. 197-208, 2001.
- [15] G. Coatrieux, H. Maitre, B. Sankur, "Strict integrity control of biomedical images," in Proc. SPIE Security and Watermarking of Multimedia Contents III, SPIE2001, San Jose, USA, vol. 4314, pp. 229-240, Jan. 2001.
- [16] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple image watermarking applied to health information management", *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. 722-732, Oct. 2006.
- [17] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "A multiple watermarking scheme applied to medical image management", Proc. 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS), pp. 3241-3244, San Francisco, CA, USA, September 1-5, 2004.
- [18] F. Hartung, M. Kutter, "Multimedia watermarking techniques," in Proc. IEEE Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1069-1107, July 1999.
- [19] H. M. Chao, C. M. Hsu, S. G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Trans. Inf. Technol. Biomed.*, vol. 6, no. 1, pp. 46-53, March 2002.
- [20] S. G. Miaou, C. M. Hsu, Y. S. Tsai, H. M. Chao, "A secure data hiding technique with heterogeneous data combining capability for electronic patient records," in Proc.

- 22nd Annu. Intern. Conf. IEEE Engineering in Medicine and Biology Society, EMBS'00, Chicago, USA, vol. 1, pp. 280-283.
- [21] U. Rajendra Acharya, D. Anand, P. Subbanna Bhat, U.C. Niranjan, "Compact storage of medical images with patient information," IEEE Trans. Inf. Technol. Biomed., vol. 5, no. 4, pp. 320-323, Dec. 2001.
- [22] F. Cao, H. K. Huang, X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," Computerized Medical Imaging and Graphics, vol. 27, no. 2-3, pp. 185-196, March-June 2003.
- [23] R. J. Anderson, F. A. P. Petitcolas, "On the limits of Steganography," IEEE J. Sel. Areas Commun Special Issue on Copyright and Privacy Protection, vol. 16, no. 4, pp. 474-481, May 1998.
- [24] S. Tzelepi, G. Pangalos, G. Nikolacopoulou, "Security of medical multimedia," Med. Inform., vol. 27, no. 3, pp. 169-184, 2002.
- [25] E. T. Lin, E. J. Delp, "A review of fragile image watermarks," in Proc. ACM Multimedia and Security Workshop, Orlando, Florida, pp. 47-51, Oct. 1999.
- [26] S. Shaw, "Overview of watermarks, fingerprints, and digital signatures," JISC Technology Applications Programme (JTAP), August 1999. Available: http://www.jisc.ac.uk/uploaded_documents/jtap-034.doc
- [27] N. F. Johnson, "In search of the right image: recognition and tracking of images in image databases, collections, and the internet," Technical report, George Mason University, Center for Secure Information Systems, June 1999.
- [28] H. D. Tagare, C. C. Jaffe, J. Duncan, "Medical image databases: a content-based retrieval approach," J. Am. Med. Inform. Assoc., vol. 4, no. 3, pp. 184-198, May 1997.
- [29] T. M. Lehmann, B. B. Wein, H. Greenspan, "Integration of Content-based Image Retrieval to Picture Archiving and Communication Systems," in Proc. Medical Informatics Europe, MIE 2003, St. Malo, France, May 4-7, 2003.
- [30] C. Traina, A. J. M. Traina, R. R. Santos, E.Y. Senzako, "A support system for content-based medical image retrieval in object oriented databases," J. Med. Syst., vol. 21, no. 6, pp. 339-352, 1997.

- [31] W. D. Bidgood, et al., "Image acquisition context: procedure description attributes for clinically relevant indexing and selective retrieval of biomedical images," J. Am. Med. Inform. Assoc., vol. 6, no. 1, pp. 61-75, Jan. 1999.
- [32] E. Louprias, N. Sebe, S. Bres, J. M. Jolion, "Wavelet-based salient points for image retrieval," in Proc. Intern. Conf. Image Proc., ICIP 2000, Vancouver, Canada, September 10-13, 2000, vol. 2, pp. 518-521.
- [33] R. U. Acharya, P. S. Bhat, S. Kumar, L. Choo Min, "Transmission and storage of medical images with patient information," Computers in Biology and Medicine, no. 33, pp. 303-310, 2003.
- [34] R. U. Acharya, U.C. Niranjana, S.S. Iyengar, N. Kannathal, L. C. Min, "Simultaneous storage of patient information with medical images in the frequency domain," Computer Methods and Programs in Biomedicine, no. 76, pp.13-19, 2004.
- [35] Jagadish Nayak, Subbanna P. Bhat, Rajendra U. Acharya, Niranjana U. Chola, "Simultaneous storage of medical images in the spatial and frequency domain: A comparative study," BioMedical Engineering OnLine, Jun 05, 2004, 3(1):17.
- [36] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images", Medical & Biological Engineering & Computing, vol. 44, no. 8, pp. 619-631, Springer Berlin / Heidelberg, August 2006. Available at: <http://dx.doi.org/10.1007/s11517-006-0081-x>
- [37] X. Q. Zhou, H. K. Huang, S. L. Lou, "Authenticity and integrity of digital mammography images," IEEE Trans. Medical Imaging, vol. 20, no. 8, pp. 784-791, Aug. 2001.
- [38] B. Macq, F. Dewey, "Trusted Headers for Medical Images," Proc. DFG VIII-DII Watermarking Workshop, Erlangen, Germany, Oct. 1999.
- [39] H. Trichili, M. Boubel, N. Derbel, L. Kamoun, "A new medical image watermarking scheme for a better telediagnosis," Proc. IEEE International Conference on Systems, Man and Cybernetics, vol. 1, pp. 556-559, Oct. 6-9, 2002.
- [40] X. Kong, R. Feng, "Watermarking medical signals for telemedicine," IEEE Trans. Inf. Technol. Biomed., vol. 5, no. 3, pp. 195-201, Sept. 2001.

- [41] Y. Yang, F. Bao, "An invertible watermarking scheme for authentication of Electronic Clinical Brain Atlas," Proc. IEEE Intern. Conf. on Acoustics, Speech, and Signal Processing (ICASSP '03), vol. 3, pp. 533-536, April 6-10, 2003.
- [42] W. Puech, J. M. Rodrigues, "A new crypto-watermarking method for medical images safe transfer", Proc. 12th Europ. Signal Processing Conf., Vienna, Austria, pp. 1481-1484.
- [43] D. Osborne, D. Abbott, M. Sorell, D. Rogers, "Multiple embedding using robust watermarks for wireless medical images," Proc. 3rd Intern. Conf. Mobile and Ubiquitous Multimedia, College Park, Maryland, USA, pp. 245-250, 2004.

ΚΕΦΑΛΑΙΟ 5

ΑΝΑΛΥΣΗ ΑΠΑΙΤΗΣΕΩΝ ΧΡΗΣΤΩΝ

5.1 ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό αναλύονται οι απαιτήσεις των χρηστών ως προς τις προδιαγραφές στις οποίες καλείται να ανταποκριθεί ένα λειτουργικό υδατογραφικό σύστημα που προορίζεται για ιατρικές εφαρμογές. Η καταγραφή των απαιτήσεων σε σχέση με την αξιοποίηση της ψηφιακής υδατογραφίας στη διαχείριση ιατρικής πληροφορίας έγινε με χρήση ερωτηματολογίου, το οποίο διανεμήθηκε σε χρήστες ιατρικών πληροφοριακών συστημάτων. Το σύνολο των ερωτηθέντων περιλάμβανε γιατρούς, νοσηλευτές και IT προσωπικό, οι οποίοι ήταν εξοικειωμένοι με τις νέες τεχνολογίες στο χώρο της υγείας, όπως με συστήματα διαχείρισης ιατρικής πληροφορίας (PACS, RIS, HIS) και τηλεϊατρικά συστήματα. Η αντίληψη της λειτουργίας των συστημάτων αυτών και των αναγκών τους, βάσει της εμπειρίας που διαθέτουν, είχε ως αποτέλεσμα την απόρροια χρήσιμων συμπερασμάτων σε ό,τι αφορά τα χαρακτηριστικά και τις υπηρεσίες που πρέπει να προσφέρει το υδατογραφικό σύστημα. Οι ερωτηθέντες χρήστες ιατρικών πληροφοριακών συστημάτων ενημερώθηκαν για ένα σύνολο προτεινόμενων υπηρεσιών του υδατογραφικού συστήματος και κλήθηκαν να αξιολογήσουν τη χρησιμότητά τους, να καθορίσουν τα απαιτούμενα χαρακτηριστικά τους, καθώς επίσης να προτείνουν άλλες πιθανές υπηρεσίες. Μέσω των ερωτηματολογίων διερευνήθηκε η

ανταπόκριση των ερωτηθέντων ως προς τις πιθανές ωφέλειες από την προσθήκη πληροφορίας μέσα στις εικόνες (πρόσθετη ασφάλεια, μόνιμη αντιστοίχιση ασθενούς – εικόνας, μείωση απαιτήσεων μνήμης, αποδοτική δεικτοδότηση και ανάκτηση δεδομένων, έλεγχος αξιοπιστίας εικόνας, κ.λπ.) και καθορίστηκαν τα είδη πληροφορίας που θα ήταν χρήσιμο να ενσωματωθούν.

Στη συνέχεια του κεφαλαίου παρουσιάζονται οι απαιτήσεις των χρηστών και βάσει της ανάλυσής τους, τα λειτουργικά χαρακτηριστικά που πρέπει να διαθέτει το υδατογραφικό σύστημα προκειμένου να καλύψει τους επιδιωκόμενους στόχους, και στη συνέχεια παρουσιάζονται τα προβλεπόμενα σενάρια χρήσης του. Τέλος, περιγράφονται κάποιες περιπτώσεις εφαρμογής του και δίνονται πληροφορίες ως προς την ολοκλήρωση ενός τέτοιου συστήματος στα πλαίσια των προτεινόμενων εφαρμογών.

5.2 ΑΠΑΙΤΗΣΕΙΣ ΧΡΗΣΤΩΝ

Με βάση τις απαντήσεις των ερωτηθέντων χρηστών πληροφοριακών συστημάτων στο χώρο της υγείας και πιθανών μελλοντικών χρηστών του υδατογραφικού συστήματος, προέκυψαν τα ακόλουθα συμπεράσματα ως προς τα χαρακτηριστικά που πρέπει αυτό να διαθέτει:

1. Η γραφική διαπροσωπεία πρέπει να είναι απλή, φιλική στο χρήστη και εργονομική.
2. Ο χρόνος εισαγωγής και εξαγωγής υδατογραφημάτων πρέπει να είναι περιορισμένος και να μην προκαλεί καθυστέρηση στη διαχείριση του περιστατικού.
3. Απαιτείται η χρήση κλειδιού για την ενσωμάτωση και την εξαγωγή των υδατογραφημάτων, προκειμένου να εξασφαλιστεί ο έλεγχος πρόσβασης των ευαίσθητων ιατρικών δεδομένων και η προσπέλασή τους μόνο από εξουσιοδοτημένους χρήστες.
4. Το σύστημα πρέπει να παρέχει τη δυνατότητα καθορισμού από το χρήστη μιας Περιοχής Ενδιαφέροντος που περικλείει την κρίσιμη από άποψη

διαγνωστικής αξίας πληροφορία και για την οποία θα υπάρχει η επιλογή ελάχιστης ή ακόμη και μη υδατογράφησης της.

Σε γενικές γραμμές, οι χρήστες ιατρικών πληροφοριακών συστημάτων που συμμετείχαν στην έρευνα ήταν θετικοί στις προοπτικές της ψηφιακής υδατογράφησης ιατρικών εικόνων και συμφώνησαν στη χρησιμότητα των συμπληρωματικών ή/και εναλλακτικών λύσεων που επιχειρούνται μέσω του υδατογραφικού συστήματος. Οι ερωτηθέντες έδωσαν έμφαση στην αναγκαιότητα εφαρμογής πρόσθετων μέτρων για την ασφάλεια των ιατρικών δεδομένων και την προστασία του ιατρικού απορρήτου. Αποτυπώθηκε επίσης στα ερωτηματολόγια η καθολική επιθυμία των συμμετεχόντων να υπάρχει περιορισμός στην πρόσβαση των δεδομένων που εμπίπτουν στο ιατρικό απόρρητο ανάλογα με την κατηγορία του εργαζομένου (π.χ. γιατρός, νοσηλευτικό προσωπικό κ.λπ.).

Βάσει των απαντήσεων των ερωτηθέντων σε ό,τι αφορά την πληροφορία που θα μπορούσε να ενσωματωθεί μέσω υδατογραφημάτων στις ιατρικές εικόνες, προέκυψε ότι το εν λόγω σύστημα πρέπει να επιτρέπει την εισαγωγή των ακόλουθων υδατογραφημάτων:

1. Ένα υδατογράφημα υπογραφής που περιέχει στοιχεία αναγνώρισης της πηγής προέλευσης της εικόνας, όπως την ψηφιακή υπογραφή του γιατρού που διενεργεί την εξέταση, τον αναγνωριστικό κωδικό του ιατρικού απεικονιστικού μηχανήματος ή του κινητού τηλεϊατρικού σταθμού από όπου αποστέλλεται η εικόνα, το όνομα του διαγνωστικού κέντρου κ.λπ.
2. Ένα υδατογράφημα δείκτη που περιλαμβάνει λέξεις-κλειδιά για την εύκολη αρχειοθέτηση και ανάκτηση (retrieval) ιατρικών εικόνων. Οι δείκτες μπορούν να περιλαμβάνουν κωδικό ασθένειας, κωδικό εξέτασης, κωδικό ασθενή κ.λπ.
3. Ένα υδατογράφημα επικεφαλίδας που περιέχει ευαίσθητα δεδομένα που αφορούν τον ασθενή και την εξέταση και τα οποία χρήζουν αυξημένης προστασίας από μη εξουσιοδοτημένη πρόσβαση. Τα δεδομένα αυτά μπορούν να περιλαμβάνουν τα προσωπικά στοιχεία του ασθενή, την

ημερομηνία εξέτασης, την αρχική διάγνωση, το όνομα του διαγνωστικού κέντρου, τον τύπο του ιατρικού απεικονιστικού μηχανήματος κ.ά. Θεωρείται επίσης χρήσιμη η επισήμανση χαρακτηριστικών και η καταγραφή σχολίων και βοηθητικής πληροφορίας για την καθοδήγηση άλλων γιατρών.

4. Ένα υδατογράφημα αναφοράς που επιτρέπει τον έλεγχο της ακεραιότητας των ιατρικών δεδομένων και τον εντοπισμό τυχόν παραποιημένων τμημάτων τους, καθώς η παραμικρή αλλοίωσή τους θα μπορούσε να οδηγήσει στη διαμόρφωση λανθασμένης διάγνωσης και κατά συνέπεια ακατάλληλης θεραπευτικής αγωγής.

5.3 ΤΕΧΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΤΩΝ ΕΦΑΡΜΟΓΩΝ

5.3.1 Λειτουργικές Απαιτήσεις

Οι λειτουργικές απαιτήσεις των εφαρμογών παρουσιάζονται με τη μορφή περιπτώσεων χρήσης (use cases), οι οποίες περιγράφουν την αλληλεπίδραση χρήστη – συστήματος μέσω των ακολουθιών ενεργειών. Ο παρακάτω πίνακας παρουσιάζει συνοπτικά τις περιπτώσεις χρήσης για το υδατογραφικό σύστημα:

Περίπτωση Χρήσης	Περιγραφή
Π.Χ.1	Εισαγωγή στοιχείων πηγής προέλευσης
Π.Χ.2	Προβολή στοιχείων πηγής προέλευσης
Π.Χ.3	Εισαγωγή στοιχείων σχετικά με τον ασθενή και την εξέταση
Π.Χ.4	Προβολή στοιχείων σχετικά με τον ασθενή και την εξέταση
Π.Χ.5	Εισαγωγή υδατογραφήματος ελέγχου ακεραιότητας
Π.Χ.6	Έλεγχος ακεραιότητας

Περίπτωση Χρήσης	Περιγραφή
Π.Χ.7	Εισαγωγή δεικτών
Π.Χ.8	Εξαγωγή δεικτών για ανάκτηση εικόνων / δεδομένων

Στους πίνακες που ακολουθούν παρουσιάζονται οι περιπτώσεις χρήσης που προσδιορίστηκαν στον παραπάνω πίνακα με τις ακολουθίες ενεργειών που τους αντιστοιχούν.

Π.Χ.1: Εισαγωγή στοιχείων πηγής προέλευσης	
Σχετιζόμενοι ρόλοι	Ιατρικός Υπεύθυνος (Γιατρός, νοσηλευτικό προσωπικό)
Βασική ακολουθία ενεργειών	1. Ο ιατρικός υπεύθυνος επιλέγει την εισαγωγή δεδομένων σχετικά με την πηγή προέλευσης της εικόνας. 2. Το σύστημα παρουσιάζει τη φόρμα εισαγωγής στοιχείων (υπογραφή γιατρού, όνομα διαγνωστικού κέντρου, κ.λπ.) 3. Ο ιατρικός υπεύθυνος εισάγει τα στοιχεία που επιθυμεί. 4. Το σύστημα παρουσιάζει τη φόρμα επιλογής ιατρικής εικόνας. 5. Ο ιατρικός υπεύθυνος επιλέγει την προς υδατογράφιση ιατρική εικόνα. 6. Το σύστημα παρουσιάζει την επιλεγμένη εικόνα. 7. Ο ιατρικός υπεύθυνος ορίζει προαιρετικά στην εικόνα μια Περιοχή Ενδιαφέροντος. 8. Ο ιατρικός υπεύθυνος εισάγει το υδατογραφικό κλειδί. 9. Το σύστημα υδατογραφεί την εικόνα με την πηγή προέλευσής της. 10. Το σύστημα παρουσιάζει την υδατογραφημένη εικόνα.
Διαχείριση Εξαιρέσεων (Exception Handling), Χειρισμός Λαθών (Error situations)	1. Εάν τα δεδομένα υπερβαίνουν τη χωρητικότητα της εικόνας ενημερώνεται ο χρήστης

Π.Χ.2: Προβολή στοιχείων πηγής προέλευσης	
Σχετιζόμενοι ρόλοι	Ιατρικός Υπεύθυνος (Γιατρός, νοσηλευτικό προσωπικό)
Βασική ακολουθία ενεργειών	1. Ο ιατρικός υπεύθυνος επιλέγει την προβολή της πηγής προέλευσης. 2. Το σύστημα παρουσιάζει τη φόρμα επιλογής ιατρικής εικόνας. 3. Ο ιατρικός υπεύθυνος επιλέγει την ιατρική εικόνα. 4. Ο ιατρικός υπεύθυνος εισάγει το υδατογραφικό κλειδί. 5. Το σύστημα παρουσιάζει την πηγή προέλευσης της ιατρικής εικόνας.
Διαχείριση Εξαιρέσεων (Exception Handling), Χειρισμός Λαθών (Error situations)	

Π.Χ.3: Εισαγωγή στοιχείων σχετικά με τον ασθενή και την εξέταση	
Σχετιζόμενοι ρόλοι	Ιατρικός Υπεύθυνος (Γιατρός, νοσηλευτικό προσωπικό)
Βασική ακολουθία ενεργειών	1. Ο ιατρικός υπεύθυνος επιλέγει την εισαγωγή δεδομένων σχετικών με τον ασθενή και την εξέταση. 2. Το σύστημα παρουσιάζει τη φόρμα εισαγωγής στοιχείων (προσωπικά δεδομένα ασθενή, στοιχεία εξέτασης, σχόλια, κ.λπ.). 3. Ο ιατρικός υπεύθυνος εισάγει τα στοιχεία που επιθυμεί. 4. Το σύστημα παρουσιάζει τη φόρμα επιλογής ιατρικής εικόνας. 5. Ο ιατρικός υπεύθυνος επιλέγει την προς υδατογράφιση ιατρική εικόνα. 6. Το σύστημα παρουσιάζει την επιλεγμένη εικόνα. 7. Ο ιατρικός υπεύθυνος ορίζει προαιρετικά στην εικόνα μια Περιοχή Ενδιαφέροντος. 8. Ο ιατρικός υπεύθυνος εισάγει το υδατογραφικό κλειδί. 9. Το σύστημα υδατογραφεί την εικόνα με τα μεταδεδομένα.

	10. Το σύστημα παρουσιάζει την υδατογραφημένη εικόνα.
Διαχείριση Εξαιρέσεων (Exception Handling), Χειρισμός Λαθών (Error situations)	1. Εάν τα δεδομένα υπερβαίνουν τη χωρητικότητα της εικόνας ενημερώνεται ο χρήστης

Π.Χ.4: Προβολή στοιχείων σχετικά με τον ασθενή και την εξέταση	
Σχετιζόμενοι ρόλοι	Ιατρικός Υπεύθυνος (Γιατρός, νοσηλευτικό προσωπικό)
Βασική ακολουθία ενεργειών	1. Ο ιατρικός υπεύθυνος επιλέγει την προβολή δεδομένων σχετικών με τον ασθενή και την εξέταση. 2. Το σύστημα παρουσιάζει τη φόρμα επιλογής ιατρικής εικόνας. 3. Ο ιατρικός υπεύθυνος επιλέγει την ιατρική εικόνα. 4. Ο ιατρικός υπεύθυνος εισάγει το υδατογραφικό κλειδί. 5. Το σύστημα παρουσιάζει τα μεταδεδομένα.
Διαχείριση Εξαιρέσεων (Exception Handling), Χειρισμός Λαθών (Error situations)	

Π.Χ.5: Εισαγωγή υδατογραφήματος ελέγχου ακεραιότητας	
Σχετιζόμενοι ρόλοι	Ιατρικός Υπεύθυνος (Γιατρός, νοσηλευτικό προσωπικό)
Βασική ακολουθία ενεργειών	1. Ο ιατρικός υπεύθυνος επιλέγει την εισαγωγή υδατογραφήματος ελέγχου ακεραιότητας. 2. Το σύστημα παρουσιάζει τη φόρμα επιλογής ιατρικής εικόνας. 3. Ο ιατρικός υπεύθυνος επιλέγει την προς υδατογράφιση ιατρική εικόνα. 4. Το σύστημα παρουσιάζει την επιλεγμένη εικόνα. 5. Ο ιατρικός υπεύθυνος ορίζει προαιρετικά στην εικόνα μια Περιοχή Ενδιαφέροντος. 6. Ο ιατρικός υπεύθυνος εισάγει το

	υδατογραφικό κλειδί. 7. Το σύστημα ενσωματώνει στην ιατρική εικόνα το υδατογράφημα ελέγχου ακεραιότητας. 8. Το σύστημα παρουσιάζει την υδατογραφημένη εικόνα.
Διαχείριση Εξαιρέσεων (Exception Handling), Χειρισμός Λαθών (Error situations)	

Π.Χ.6: Έλεγχος ακεραιότητας	
Σχετιζόμενοι ρόλοι	Ιατρικός Υπεύθυνος (Γιατρός, νοσηλευτικό προσωπικό)
Βασική ακολουθία ενεργειών	1. Ο ιατρικός υπεύθυνος επιλέγει τον έλεγχο της ακεραιότητας μιας εικόνας. 2. Το σύστημα παρουσιάζει τη φόρμα επιλογής ιατρικής εικόνας. 3. Ο ιατρικός υπεύθυνος επιλέγει την ιατρική εικόνα. 4. Ο ιατρικός υπεύθυνος εισάγει το υδατογραφικό κλειδί. 5. Το σύστημα ελέγχει την ακεραιότητα της εικόνας και πληροφορεί το χρήστη για τις ενδεχόμενες αλλοιώσεις.
Διαχείριση Εξαιρέσεων (Exception Handling), Χειρισμός Λαθών (Error situations)	

Π.Χ.7: Εισαγωγή δεικτών	
Σχετιζόμενοι ρόλοι	Ιατρικός Υπεύθυνος (Γιατρός, νοσηλευτικό προσωπικό)
Βασική ακολουθία ενεργειών	1. Ο ιατρικός υπεύθυνος επιλέγει την εισαγωγή δεικτών. 2. Το σύστημα παρουσιάζει τη φόρμα εισαγωγής δεικτών. 3. Ο ιατρικός υπεύθυνος επιλέγει τους δείκτες που επιθυμεί να εισαγάγει. 4. Το σύστημα παρουσιάζει τη φόρμα επιλογής ιατρικής εικόνας.

Π.Χ.7: Εισαγωγή δεικτών	
	5. Ο ιατρικός υπεύθυνος επιλέγει την προς υδατογράφιση ιατρική εικόνα. 6. Το σύστημα παρουσιάζει την επιλεγμένη εικόνα. 7. Ο ιατρικός υπεύθυνος ορίζει προαιρετικά στην εικόνα μια Περιοχή Ενδιαφέροντος. 8. Ο ιατρικός υπεύθυνος εισάγει το υδατογραφικό κλειδί. 9. Το σύστημα ενσωματώνει τους δείκτες στην εικόνα. 10. Το σύστημα παρουσιάζει την υδατογραφημένη εικόνα.
Διαχείριση Εξαιρέσεων (Exception Handling), Χειρισμός Λαθών (Error situations)	1. Εάν τα δεδομένα υπερβαίνουν τη χωρητικότητα της εικόνας ενημερώνεται ο χρήστης

Π.Χ.8: Εξαγωγή δεικτών για ανάκτηση εικόνων / δεδομένων	
Σχετιζόμενοι ρόλοι	Ιατρικός Υπεύθυνος (Γιατρός, νοσηλευτικό προσωπικό)
Βασική ακολουθία ενεργειών	1. Ο ιατρικός υπεύθυνος επιλέγει την εξαγωγή δεικτών για εύρεση εικόνων / δεδομένων. 2. Το σύστημα παρουσιάζει τη φόρμα επιλογής ιατρικής εικόνας. 3. Ο ιατρικός υπεύθυνος επιλέγει την ιατρική εικόνα. 4. Ο ιατρικός υπεύθυνος εισάγει το υδατογραφικό κλειδί. 5. Το σύστημα παρουσιάζει τους δείκτες της εικόνας.
Διαχείριση Εξαιρέσεων (Exception Handling), Χειρισμός Λαθών (Error situations)	

5.3.2 Μη Λειτουργικές Απαιτήσεις

5.3.2.1 Απαιτούμενη ανθεκτικότητα των πολλαπλών υδατογραφημάτων

Μια από τις βασικές παραμέτρους που χαρακτηρίζουν τα διάφορα είδη υδατογραφημάτων αποτελεί η ανθεκτικότητά τους απέναντι σε συνηθισμένες ενέργειες επεξεργασίας σήματος / εικόνας αλλά και σε κακόβουλες επιθέσεις. Ο απαιτούμενος βαθμός ανθεκτικότητας κάθε υδατογραφήματος εξαρτάται από την εφαρμογή για την οποία προορίζεται. Η ανθεκτικότητα είναι επίσης σε άμεση συνάρτηση με τον όγκο πληροφορίας που καλείται το υδατογράφημα να ενσωματώσει, το λεγόμενο «φορτίο» ή «χωρητικότητα». Όσο αυξάνεται η απαιτούμενη χωρητικότητα απόκρυψης, τόσο μειώνεται η ανθεκτικότητα που μπορεί να παρουσιάσει το υδατογράφημα.

Σε σχέση με τις περιπτώσεις χρήσης του υδατογραφικού συστήματος που έχουν καθοριστεί, απαιτούνται οι ακόλουθοι τύποι υδατογραφημάτων:

- Προστασία ιατρικού απορρήτου / Επισήμανση χαρακτηριστικών: *ανθεκτικά υδατογραφήματα*
- Προσδιορισμός πηγής προέλευσης: *ανθεκτικά υδατογραφήματα*
- Ακεραιότητα δεδομένων: *εύθραυστα υδατογραφήματα*
- Ανάκτηση δεδομένων: *ανθεκτικά υδατογραφήματα*

5.3.2.2 Απαιτούμενη χωρητικότητα των πολλαπλών υδατογραφημάτων

Η χωρητικότητα των υδατογραφημάτων αφορά τον όγκο της πληροφορίας που χρειάζεται αυτά να περιέχουν και καθορίζεται από τις απαιτήσεις της εκάστοτε εφαρμογής. Ο αλγόριθμος που επιλέγεται για την ενσωμάτωση του υδατογραφήματος θα πρέπει – σε συνδυασμό με τις διαστάσεις των εικόνων – να έχει τη δυνατότητα να παράσχει την απαιτούμενη χωρητικότητα.

Σε σχέση με τις περιπτώσεις χρήσης του υδατογραφικού συστήματος που έχουν καθοριστεί, προκύπτουν οι απαιτήσεις που παρουσιάζονται στον ακόλουθο πίνακα.

Πεδίο Εφαρμογής	Δεδομένα προς Αποθήκευση	Τυπικό Μέγεθος Δεδομένων	Συνολική Απαιτούμενη Χωρητικότητα (bits)
Προσδιορισμός πηγής προέλευσης	Όνομα διαγνωστικού κέντρου	128 bits	256 bits
	Υπογραφή γιατρού	128 bits	
Ανάκτηση δεδομένων	Κωδικοί ασθενειών	10 chars	480 bits
	Κωδικός εξέτασης	10 chars	
	Κωδικός ασθενή	10 chars	
Προστασία ιατρικού απορρήτου / Επισήμανση χαρακτηριστικών	Ονοματεπώνυμο ασθενή	40 chars	4000 bits
	Ημερομηνία εξέτασης	10 chars	
	Νοσηλευτικό κέντρο	20 chars	
	Τύπος μηχανήματος	30 chars	
	Διάγνωση	50 chars	
	Σχόλια	50 chars	
	Άλλο	50 chars	

5.3.2.3 Αλληλεπίδραση με το χρήστη

Οι βασικές αλληλεπιδράσεις μεταξύ χρήστη και εφαρμογών όπως προκύπτουν από τις περιπτώσεις χρήσης (use cases) συνοψίζονται στα εξής:

□ **Λειτουργίες 1ου επιπέδου (1st Level Menu)**

1. Υδατογράφιση δεδομένων ιατρικού απορρήτου και μετα-πληροφορίας
2. Προβολή δεδομένων ιατρικού απορρήτου και μετα-πληροφορίας
3. Υδατογράφιση δεδομένων πηγής προέλευσης
4. Προβολή δεδομένων πηγής προέλευσης
5. Εισαγωγή υδατογραφήματος ακεραιότητας
6. Έλεγχος ακεραιότητας εικόνας
7. Εισαγωγή δεικτών
8. Εξαγωγή δεικτών για εύρεση εικόνων / δεδομένων

□ **Λειτουργίες 2ου επιπέδου (2nd Level Menu)**

1. Φόρμα επιλογής υδατογραφημάτων που θα χρησιμοποιηθούν από την εφαρμογή
2. Φόρμα επιλογής ιατρικής εικόνας
3. Φόρμα επιλογής της περιοχής διαγνωστικής αξίας στην εικόνα
4. Φόρμα εισαγωγής του κλειδιού υδατογράφησης
5. Φόρμα εισαγωγής στοιχείων πηγής προέλευσης
6. Φόρμα εισαγωγής δεικτών
7. Φόρμα εισαγωγής στοιχείων ιατρικού απορρήτου και μετα-πληροφορίας

Οι λειτουργίες 1^{ου} επιπέδου αφορούν τις βασικές λειτουργίες που έχει διαθέσιμες ένας χρήστης. Η απαίτηση ως προς τις λειτουργίες αυτές είναι ότι θα πρέπει να παρέχονται με κάποιο είδος μενού προς το χρήστη.

Οι λειτουργίες 2^{ου} επιπέδου αφορούν τις επιλογές των χρηστών σχετικά με φόρμες εισαγωγής στοιχείων. Γενικές απαιτήσεις σχετικά με αυτές τις λειτουργίες είναι οι εξής:

- Χρήση λιστών για επιλογή εφόσον είναι εφικτό (π.χ. λίστα ICD-10 για επιλογή δεικτών)

- Γραφικός τρόπος επιλογής παραμέτρων (π.χ. αρχεία)
- Γραφικός τρόπος χειρισμού εικόνων όπου απαιτείται (π.χ. προσδιορισμός περιοχής ενδιαφέροντος)
- Ενημέρωση χρήστη για ενδιάμεσα αποτελέσματα (π.χ. λάθη στην εισαγωγή)

5.3.3 Εργαλεία Ανάπτυξης των Εφαρμογών

Βάσει της ανάλυσης των απαιτήσεων των χρηστών και των επιδιωκόμενων στόχων, το υδατογραφικό σύστημα πρέπει να παρέχει μεταξύ άλλων τις ακόλουθες δυνατότητες:

- δυνατότητα διαχείρισης και επεξεργασίας ιατρικών εικόνων
- δυνατότητα προσδιορισμού περιοχής ενδιαφέροντος
- υποστήριξη υδατογραφημάτων με διαφορετικές απαιτήσεις ως προς την ανθεκτικότητα και τη χωρητικότητα
- δυνατότητα ενσωμάτωσης ποικίλων δεδομένων στα επιλεγμένα υδατογραφήματα
- δυνατότητα παραμετροποίησης / προγραμματισμού της εφαρμογής

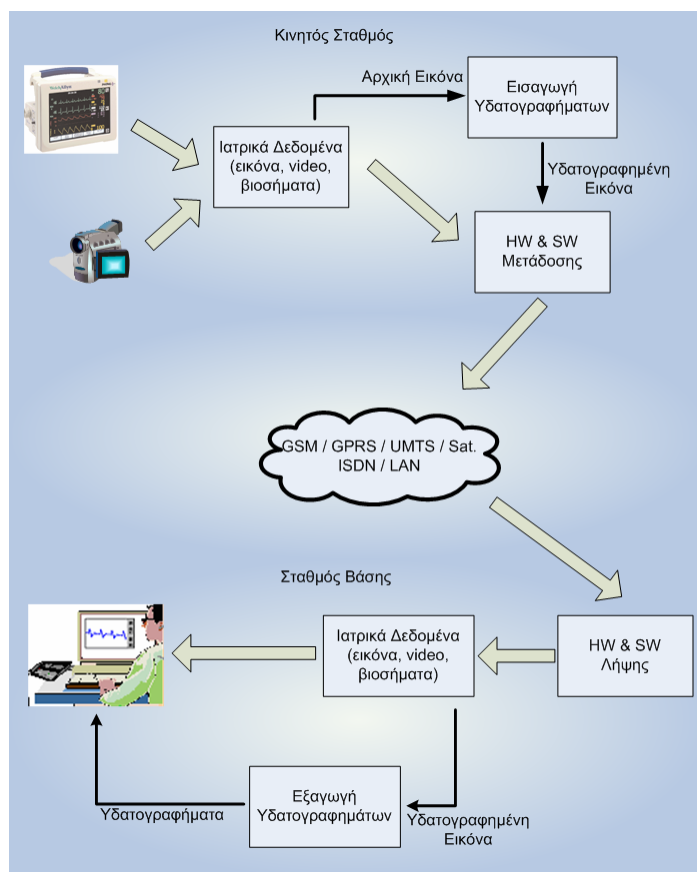
Για την επίτευξη των παραπάνω απαιτείται η χρήση κατάλληλων εργαλείων ανάπτυξης των διεπαφών με τους χρήστες και προγραμματισμού των διαφόρων λειτουργιών. Για τις ανάγκες της σχεδίασης, ανάπτυξης και δοκιμής του συστήματος στα πλαίσια της διατριβής, κρίθηκε σκόπιμο να χρησιμοποιηθεί το Matlab, που προσφέρει ένα φιλικό προγραμματιστικό περιβάλλον και διαθέτει βιβλιοθήκες με συναρτήσεις επεξεργασίας εικόνας που απαιτούνται για την ανάπτυξη του συστήματος.

5.4 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΠΕΡΙΟΧΩΝ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΥΔΑΤΟΓΡΑΦΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Το υδατογραφικό σύστημα καλείται να ανταποκριθεί με επιτυχία σε διάφορα σενάρια χρήσης. Η ενσωμάτωσή του σε διάφορα ιατρικά απεικονιστικά μηχανήματα

(π.χ. CT, MRI, υπερήχων) μπορεί να δώσει εναλλακτικές ή / και συμπληρωματικές λύσεις σε ποικίλες εφαρμογές που καλύπτουν ένα ευρύ φάσμα, από αποδοτική διαχείριση, αρχειοθέτηση και ανάκτηση ιατρικών δεδομένων μέσα σε ένα δίκτυο νοσοκομείου, έως διάγνωση και καθοδήγηση από απόσταση [1], [2]. Για παράδειγμα, μια περίπτωση εφαρμογής σε νοσοκομειακό περιβάλλον περιλαμβάνει τα εξής στάδια: μετά τη λήψη της εικόνας, ο γιατρός ενσωματώνει σε αυτήν πληροφορίες όπως τον αναγνωριστικό κωδικό του, προσωπικά δεδομένα του ασθενή και στοιχεία σχετικά με την εξέταση, λέξεις-κλειδιά για ανάκτηση της εικόνας, ή ακόμη και πρόσθετα στοιχεία χρήσιμα για την καθοδήγηση άλλων γιατρών. Η εικόνα υδατογραφείται με αυτά τα δεδομένα και στη συνέχεια αποθηκεύεται στη βάση δεδομένων του νοσοκομείου. Έπειτα, η εικόνα μπορεί να ανακληθεί από τη βάση δεδομένων μέσω κατάλληλων μηχανισμών αναζήτησης (querying mechanisms). Κάθε εξουσιοδοτημένο άτομο του ιατρικού και παραϊατρικού προσωπικού, έχοντας στη διάθεσή του το κατάλληλο κλειδί, μπορεί να εξαγάγει τα ενσωματωμένα υδατογραφήματα και να αποκτήσει πρόσβαση σε πληροφορίες που περιλαμβάνουν: τα στοιχεία του ασθενή, την ταυτότητα του γιατρού που παρήγαγε την εικόνα και επιβεβαίωσε τα αποτελέσματα, τη διάγνωση κ.λπ. Μπορεί επίσης να εξαγάγει το εύθραυστο υδατογράφημα και να εξετάσει την ακεραιότητα της εικόνας.

Μια περίπτωση τηλεϊατρικής εφαρμογής περιλαμβάνει την υδατογράφιση της αποκτηθείσας εικόνας σε μια κινητή μονάδα και τη μετάδοσή της στο σταθμό βάσης (π.χ. νοσοκομείο) όπου βρίσκεται ο εξειδικευμένος γιατρός, παρέχοντας ένα πρόσθετο επίπεδο ασφάλειας στα μεταδιδόμενα δεδομένα [3], [4], [5]. Η αρχιτεκτονική ενσωμάτωσης του εργαλείου ψηφιακής υδατογραφίας σε σύστημα τηλεϊατρικής παρουσιάζεται στο Σχήμα 3. Σύμφωνα με το σενάριο αυτό, ο κινητός σταθμός συλλέγει εικόνες και βιοσήματα (ηλεκτροκαρδιογράφημα, πίεση κ.λπ.) από τον ασθενή· στη συνέχεια οι εικόνες υδατογραφούνται και στέλνονται με τα βιοσήματα στο σταθμό βάσης (νοσοκομείο). Εκεί ο γιατρός εξάγει τα υδατογραφήματα από τις εικόνες και ανακτά τα δεδομένα που περιέχονται σε αυτές. Βάσει της συνολικής διαθέσιμης πληροφορίας ο γιατρός είναι σε θέση να κάνει μια πρώτη διάγνωση και να δώσει οδηγίες στους παροχείς ιατρικής περίθαλψης ως προς το πώς να χειριστούν το περιστατικό.



Σχήμα 3: Ενσωμάτωση υπηρεσίας ψηφιακής υδατογραφίας σε σύστημα τηλεϊατρικής

Οι παραπάνω περιπτώσεις εφαρμογής είναι απλώς ενδεικτικές, καθώς το υδατογραφικό σύστημα αναμένεται να καλύψει πληθώρα σεναρίων εφαρμογής στον ιατρικό τομέα, παρέχοντας ένα πρόσθετο επίπεδο ασφάλειας και αποδοτική διαχείριση ιατρικών δεδομένων. Στη συνέχεια αποτυπώνονται πιο αναλυτικά δύο προβλεπόμενα σενάρια χρήσης.

5.4.1 Εφαρμογές e-Health

Ένα σενάριο χρήσης του υδατογραφικού συστήματος αναφέρεται σε εφαρμογές e-Health και απεικονίζεται στο Σχήμα 4. Στις εφαρμογές e-Health η χρήση συστήματος ψηφιακής υδατογραφίας αποσκοπεί κατά κύριο λόγο στη βελτίωση της ασφάλειας των μεταδιδόμενων ιατρικών δεδομένων, που συνίσταται στην εμπιστευτικότητα, τη γνησιότητα και την ακεραιότητά τους.



Σχήμα 4: Χρήση υπηρεσίας ψηφιακής υδατογραφίας σε εφαρμογή e-Health

Σε γενικές γραμμές το σενάριο μιας εφαρμογής e-Health περιλαμβάνει δύο ή περισσότερες οντότητες που ανταλλάσσουν ιατρικά δεδομένα με σκοπό την παροχή υπηρεσιών υγείας. Ένα τέτοιο σενάριο υποστηρίζει ετερογένεια χρηστών (πολίτης-ασθενής, επαγγελματίας υπηρεσιών υγείας, ασφαλιστική εταιρεία, κ.λπ.), εφαρμογών (web server, web browser) και εξοπλισμού (τερματικές μονάδες, δίκτυο), ενώ χαρακτηρίζεται από υψηλό κίνδυνο ασφάλειας δεδομένων. Ο ρόλος της ψηφιακής υδατογραφίας είναι ουσιαστικά συμπληρωματικός στις ήδη υπάρχουσες υποδομές ασφάλειας δεδομένων (π.χ. Υποδομές Δημοσίου Κλειδιού – Public Key Infrastructure, PKI), ενώ προσφέρει και επιπλέον δυνατότητες σε ό,τι αφορά την εύκολη διαχείριση και αρχειοθέτηση των δεδομένων. Σύμφωνα με το προβλεπόμενο σενάριο, οι υπηρεσίες ψηφιακής υδατογραφίας ενσωματώνονται στις εφαρμογές e-Health παρέχοντας:

- *Προστασία απορρήτου:* το ονοματεπώνυμο του ασθενή καθώς και ορισμένα σημαντικά στοιχεία του ιατρικού φακέλου του ενσωματώνονται με χρήση ψηφιακής υδατογραφίας σε διαγνωστικές εικόνες που ανταλλάσσονται μεταξύ των δύο εφαρμογών e-Health. Η ανάκτηση των στοιχείων αυτών μπορεί να γίνει μόνο από εξουσιοδοτημένους χρήστες, η ταυτότητα των οποίων καθώς και τα κλειδιά αποκρυπτογράφησης εξασφαλίζονται από το σύστημα προστασίας δεδομένων. Με αυτό τον τρόπο δεν υπάρχει ανάγκη ξεχωριστής κρυπτογράφησης και αποστολής της επικεφαλίδας των αρχείων ιατρικών εικόνων (DICOM). Σε περιπτώσεις άλλωστε όπου δεν είναι δυνατόν με οποιονδήποτε τρόπο να συσχετιστεί η ταυτότητα του ασθενή με τις

διακινούμενες εικόνες, η ανταλλαγή αυτή μπορεί να γίνει χωρίς καμία επιπλέον κρυπτογράφηση των εικόνων αυτών.

- *Προστασία ακεραιότητας*: εύθραυστα υδατογραφήματα μπορούν να χρησιμοποιηθούν εναλλακτικά των συναρτήσεων hash, για τον έλεγχο της ακεραιότητας της μεταδιδόμενης ιατρικής πληροφορίας. Τα πλεονεκτήματα της υδατογραφίας συνοψίζονται στη δυνατότητα εντοπισμού του σημείου αλλοίωσης των αυθεντικών δεδομένων και στην ανθεκτικότητα σε τυχαία σφάλματα bit που οφείλονται στη μετάδοση.
- *Προστασία γνησιότητας*: ο τελικός χρήστης της ιατρικής πληροφορίας μπορεί να πιστοποιήσει την αυθεντικότητά της. Αν και η χρήση ψηφιακών υπογραφών εξασφαλίζει σε ένα βαθμό τη γνησιότητα κατά τη μετάδοση των δεδομένων, δεν προστατεύει από τις περιπτώσεις εκείνες όπου ένας εξουσιοδοτημένος χρήστης (ιατρός, ασθενής, ασφαλιστική εταιρεία) παραποιήσει εσκεμμένα ή μη το περιεχόμενο του ιατρικού φακέλου. Η χρήση ψηφιακής υδατογραφίας στο σημείο παραγωγής των ιατρικών δεδομένων (διαγνωστικό σύστημα, γνωμάτευση ιατρού, κ.λπ.) προστατεύει τα συμφέροντα όλων των ενδιαφερόμενων μερών και θα μπορούσε ακόμη και να αποτελέσει αποδεικτικό στοιχείο σε ενδεχόμενες νομικές διενέξεις.
- *Επισήμανση χαρακτηριστικών (feature tagging)*: η ενσωμάτωση συμπληρωματικής, βοηθητικής πληροφορίας στις εικόνες συντελεί στην έγκαιρη και έγκυρη διάγνωση και κατάλληλη αντιμετώπιση του περιστατικού. Σε αυτό βοηθά η δυνατότητα προσθήκης σχολίων για τα απεικονιζόμενα αντικείμενα, που επιτρέπει τον τονισμό περιοχών κρίσιμων για τη διάγνωση, καθώς και την επεξήγηση ασαφών σημείων.
- *Δεικτοδότηση*: η εισαγωγή δεικτών στις εικόνες επιτρέπει τη δεικτοδότησή τους και διευκολύνει την αρχειοθέτησή τους, αλλά και την ανάκτηση σχετικών πληροφοριών και εικόνων από βάσεις δεδομένων μέσω μηχανισμών αναζήτησης.

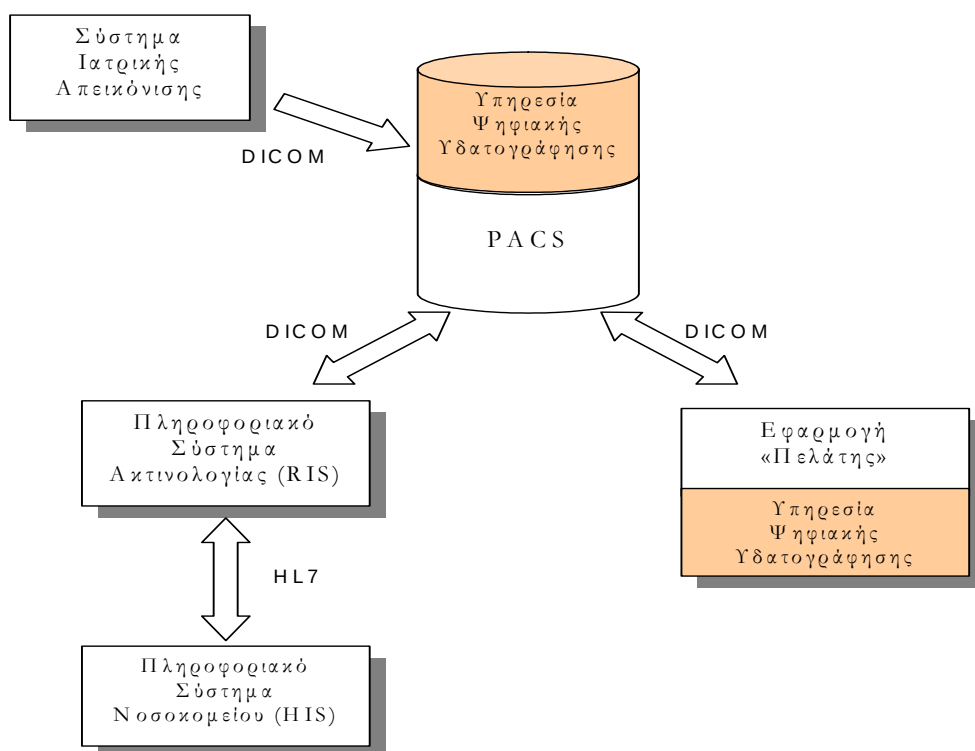
5.4.2 Διαχείριση Ιατρικών Δεδομένων σε Πληροφοριακά Συστήματα Νοσοκομείων

Ένα δεύτερο σενάριο χρήσης του υδατογραφικού συστήματος αναφέρεται στην αποδοτική διαχείριση ιατρικών δεδομένων σε νοσοκομειακά πληροφοριακά συστήματα και απεικονίζεται στο Σχήμα 5. Σε αυτήν την κατηγορία εφαρμογών η χρήση συστήματος ψηφιακής υδατογραφίας αποσκοπεί κατά κύριο λόγο στη διευκόλυνση της διαχείρισης της ιατρικής πληροφορίας, μέσω αποδοτικής δεικτοδότησης, αρχειοθέτησης και ανάκτησης δεδομένων.

Το Σχήμα 5 παρουσιάζει το συνήθη τρόπο λειτουργίας ακτινοδιαγνωστικών εργαστηρίων και την επικοινωνία και διαχείριση των ψηφιακών δεδομένων μέσα στο δίκτυο ενός νοσοκομείου, απεικονίζοντας επίσης τα σημεία όπου μπορεί να εφαρμοστεί το υδατογραφικό σύστημα σε ένα τέτοιο σενάριο.

Συνήθως στο τοπικό δίκτυο του νοσοκομείου βρίσκεται εγκατεστημένο ένα σύστημα αρχειοθέτησης και μετάδοσης εικόνων (Picture Archiving and Communication System – PACS), το οποίο καλύπτει τις ανάγκες ενός συγκεκριμένου τμήματος του νοσοκομείου (π.χ. ακτινολογικό). Το σύστημα PACS δέχεται (συνήθως μέσω του πρωτοκόλλου DICOM) το σύνολο των διαγνωστικών δεδομένων σε ψηφιακή μορφή που παράγονται από τα αντίστοιχα απεικονιστικά συστήματα (CT, MRI, ακτινολογικό, αγγειογράφος, υπερηχοτομογράφος, κ.λπ.) και τα αποθηκεύει στη βάση δεδομένων που διαχειρίζεται. Ταυτόχρονα, το σύστημα PACS επικοινωνεί με ανεξάρτητους σταθμούς εργασίας στους οποίους εκτελούνται εφαρμογές «πελάτες» (client applications) που έχουν ως σκοπό την υποστήριξη του κλινικού έργου. Οι εφαρμογές «πελάτες» περιλαμβάνουν:

- Απλή εφαρμογή απεικόνισης των διαγνωστικών εικόνων όπου ο γιατρός έχει τη δυνατότητα οριοθέτησης περιοχών ενδιαφέροντος και καταγραφής παρατηρήσεων
- Εφαρμογή υποστήριξης διάγνωσης (Computer Assisted Diagnosis),
- Εφαρμογή σχεδιασμού αγωγής (ακτινοθεραπευτική αγωγή, χειρουργικός σχεδιασμός, κ.λπ.)



Σχήμα 5: Χρήση υπηρεσίας ψηφιακής υδατογραφίας στο τοπικό δίκτυο νοσοκομείου

Επιπλέον, το PACS επικοινωνεί με το πληροφοριακό σύστημα ακτινολογίας (Radiology Information System – RIS) του συγκεκριμένου τμήματος, του οποίου ο ρόλος είναι να διαχειρίζεται όλη την ιατρική πληροφορία που δεν έχει τη μορφή διαγνωστικής εικόνας (διαχείριση ασθενών, ροή εργασιών στο τμήμα, κ.λπ.). Με τη σειρά του το σύστημα RIS επικοινωνεί με το κεντρικό πληροφοριακό σύστημα του νοσοκομείου (Hospital Information System – HIS), συνήθως μέσω του πρωτοκόλλου HL7.

Σε ένα τέτοιο σενάριο το υδατογραφικό σύστημα μπορεί να ενσωματωθεί τόσο στο σύστημα PACS όσο και στις εφαρμογές «πελάτες», προσφέροντας τις παρακάτω δυνατότητες:

- Προστασία της γνησιότητας των ιατρικών δεδομένων: καθώς τα ιατρικά δεδομένα παραλαμβάνονται στο PACS από τα διαγνωστικά συστήματα, υδατογραφούνται με τον κωδικό του ασθενή, την ημερομηνία εξέτασης και το όνομα του νοσοκομείου.

- *Επισήμανση χαρακτηριστικών*: οι χρήστες μιας εφαρμογής «πελάτη» έχουν τη δυνατότητα καταγραφής σχολίων, επισήμανσης χαρακτηριστικών και ορισμού περιοχών ενδιαφέροντος επί των διαγνωστικών εικόνων. Αυτά τα δεδομένα, μαζί με τη διάγνωση του γιατρού, είναι αποτέλεσμα επεξεργασίας της πρωτογενούς πληροφορίας των διαγνωστικών εικόνων και μπορούν να αποτελέσουν τα μεταδεδομένα (metadata) που θα ενσωματωθούν στην αρχική εικόνα με χρήση ψηφιακής υδατογραφίας. Με τον τρόπο αυτόν μειώνεται ο κίνδυνος λανθασμένης αντιστοίχισης αρχικής πληροφορίας και μεταδεδομένων και διευκολύνεται η εξαγωγή έγκυρης διάγνωσης, καθώς και η καθοδήγηση άλλων γιατρών που θα ασχοληθούν στη συνέχεια με το περιστατικό.
- *Αποδοτική αρχειοθέτηση και ανάκτηση δεδομένων*: η δεικτοδότηση των εικόνων μέσω υδατογραφήματος που περιέχει κατάλληλους δείκτες, παρέχει ένα βοηθητικό μηχανισμό αρχειοθέτησης εικόνων και επιτρέπει την εύκολη ανάκτηση σχετικής πληροφορίας και εικόνων από τη βάση δεδομένων του PACS μέσω μηχανισμών αναζήτησης.
- *Μείωση της πιθανότητας δημιουργίας σφαλμάτων*: κάθε φορά που τα ιατρικά δεδομένα χρησιμοποιούνται από την εφαρμογή «πελάτη», υπάρχει η δυνατότητα ελέγχου της ορθής αντιστοίχισης των δεδομένων (όνομα ασθενή, ημερομηνία εξέτασης, κ.λπ.) που περιέχονται στην επικεφαλίδα DICOM με αυτά που περιέχονται στο υδατογράφημα.
- *Έλεγχος της ακεραιότητας της εικόνας*: βάσει του εξαγχθέντος εύθραυστου υδατογραφήματος και της σύγκρισής του με το αρχικό υδατογράφημα ελέγχου ακεραιότητας, προκύπτουν οι περιοχές της εικόνας που ενδεχομένως υπέστησαν αλλοίωση κατά τη μετάδοση.

Στα παραπάνω αποτυπώθηκαν κάποιες πιθανές περιπτώσεις εφαρμογής του υδατογραφικού συστήματος, όπως αυτές προέκυψαν με βάση την ανάλυση των απαιτήσεων των χρηστών. Η αποδοχή ενός τέτοιου υδατογραφικού σχήματος σε συστήματα μετάδοσης και διαχείρισης ιατρικής πληροφορίας αναμένεται να εμπλουτίσει και να διευρύνει την κλίμακα εφαρμογών του.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

- [1] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple image watermarking applied to health information management", *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. 722-732, Oct. 2006.
- [2] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images", *Medical & Biological Engineering & Computing*, vol. 44, no. 8, pp. 619-631, Springer Berlin / Heidelberg, August 2006. Available: <http://dx.doi.org/10.1007/s11517-006-0081-x>
- [3] A. Giakoumaki, K. Perakis, A. Tagaris, D. Koutsouris, "Digital watermarking in telemedicine applications – Towards enhanced data security and accessibility", *Proc. 28th IEEE Annual Intern. Conf. of the Engineering in Medicine and Biology Society (EMBC'06)*, pp. 6328-6331, New York, USA, Aug. 30 – Sept. 3, 2006.
- [4] A. Tagaris, A. Giakoumaki, L. Karle, D. Koutsouris, "Watermarking SDK implementation to facilitate integration in a secure healthcare environment", *Proc. 28th IEEE Annual Intern. Conf. of the Engineering in Medicine and Biology Society (EMBC'06)*, pp. 3262-3265, New York, USA, Aug. 30 – Sept. 3, 2006.
- [5] Kostas Perakis, Aggeliki Giakoumaki, Tassos Tagaris, Dimitris Koutsouris, "Enhancement of security and accessibility in telemedical applications using digital watermarking", *Proceedings of the 4th International Conference on Information Communication Technologies in Health, ICICTH'06*, Samos Island, Greece, July 13-15, 2006.

ΚΕΦΑΛΑΙΟ 6

ΠΕΡΙΓΡΑΦΗ ΥΔΑΤΟΓΡΑΦΙΚΟΥ ΣΧΗΜΑΤΟΣ

6.1 ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό περιγράφεται το υδατογραφικό σύστημα που σχεδιάστηκε και υλοποιήθηκε στα πλαίσια της παρούσας διδακτορικής διατριβής, με βάση τις προδιαγραφές που προέκυψαν από την ανάλυση απαιτήσεων των χρηστών. Το σύστημα αυτό στοχεύει στην αξιοποίηση της ψηφιακής υδατογραφίας στην προσπάθεια ανάπτυξης ασφαλών και αποδοτικών συστημάτων διαχείρισης ιατρικών δεδομένων, με βάση το αυστηρό πλαίσιο που ορίζεται από τους νομικούς και ηθικούς κανόνες στον τομέα της υγείας. Η συμβολή του συστήματος ψηφιακής υδατογράφησης ιατρικών εικόνων στην προσπάθεια αυτή συνίσταται στην παροχή εναλλακτικών ή/και συμπληρωματικών λύσεων σε ένα σύνολο θεμάτων που άπτονται της διαχείρισης ιατρικών δεδομένων, ενισχύοντας την ασφάλεια και την αποδοτικότητα των συστημάτων μετάδοσης και διαχείρισης της ευαίσθητης ιατρικής πληροφορίας.

Στα πλαίσια εκπόνησης της παρούσας διατριβής πραγματοποιήθηκε διεξοδική μελέτη σχετικά με τις ιατρικές εφαρμογές της ψηφιακής υδατογραφίας, οι οποίες – παρά την περιορισμένη προς το παρόν βιβλιογραφία σε αυτήν την κατεύθυνση – φανερώνουν τη δυνατότητα συμβολής της στην ουσιαστική

αναβάθμιση της ποιότητας της παρεχόμενης ιατρικής περίθαλψης. Όπως παρουσιάστηκε αναλυτικά στο Κεφάλαιο 4, οι εφαρμογές αυτές περιλαμβάνουν μεταξύ άλλων την προστασία του ιατρικού απορρήτου, τον έλεγχο της ακεραιότητας των κρίσιμων ιατρικών δεδομένων, την πιστοποίηση της πηγής προέλευσής τους και την αποδοτικότερη διαχείριση της ιατρικής πληροφορίας. Λόγω των διαφορετικών και σε κάποιες περιπτώσεις αντιφατικών προδιαγραφών των ιατρικών εφαρμογών της υδατογραφίας, η υλοποίηση ενός ενιαίου υδατογραφικού σχήματος που πληροί το σύνολο των προϋποθέσεων και στόχων διαφέρει από τις συνήθεις εφαρμογές της υδατογραφίας και καθιστά αναγκαία την ταυτόχρονη εισαγωγή πολλαπλών υδατογραφημάτων. Τα υδατογραφήματα αυτά πρέπει να είναι ανεξάρτητα μεταξύ τους, να ανταποκρίνονται σε διαφορετικές απαιτήσεις και κατά συνέπεια να χαρακτηρίζονται από διαφορετικές παραμέτρους.

Βάσει των συμπερασμάτων που προέκυψαν τόσο από τη βιβλιογραφική έρευνα, όσο και από την εξέταση του νομικού και λειτουργικού πλαισίου των ιατρικών εφαρμογών, σχεδιάστηκε και αναπτύχθηκε το σχήμα πολλαπλής υδατογράφησης ιατρικών εικόνων που παρουσιάζεται στην παρούσα διατριβή, το οποίο ανταποκρίνεται στις ιδιαίτερες απαιτήσεις που διέπουν τις εφαρμογές αυτές. Στις επόμενες ενότητες του παρόντος κεφαλαίου παρατίθενται κάποια στοιχεία σχετικά με το πεδίο μετασχηματισμού που επιλέχθηκε για την ανάπτυξη του αλγορίθμου και στη συνέχεια δίνεται αναλυτική περιγραφή του υδατογραφικού σχήματος που αναπτύχθηκε για την εισαγωγή και εξαγωγή των πολλαπλών υδατογραφημάτων. Τέλος, εξηγείται διεξοδικά η διαδικασία επιλογής των συντελεστών μετασχηματισμού που κρίθηκαν κατάλληλοι για υδατογράφιση.

6.2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΠΕΔΙΟΥ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΥ ΚΥΜΑΤΙΔΙΩΝ

Ο Διακριτός Μετασχηματισμός Κυματιδίων (Discrete Wavelet Transform – DWT) αποτελεί τα τελευταία χρόνια έναν ιδιαίτερα δημοφιλή μετασχηματισμό σε πληθώρα εφαρμογών, λόγω μιας σειράς αξιόλογων χαρακτηριστικών που διαθέτει. Στη βιβλιογραφία έχει ήδη καταγραφεί εκτενής χρήση του στην επεξεργασία σήματος και εικόνας και ειδικά στη συμπίεση [1], [2]. Σχετικά πρόσφατα

διαπιστώθηκε η συμβολή της χρήσης κυματιδίων και στη σχεδίαση υδατογραφικών αλγορίθμων [3]. Ακολουθεί μια σύντομη εισαγωγή στο διακριτό μετασχηματισμό κυματιδίων προκειμένου να γίνει πιο εύκολα κατανοητός ο υδατογραφικός αλγόριθμος που αναπτύχθηκε στα πλαίσια της διδακτορικής διατριβής και ο οποίος βασίζεται στον εν λόγω μετασχηματισμό.

Στην περίπτωση μονοδιάστατου σήματος, ο διακριτός μετασχηματισμός κυματιδίων το αναλύει σε υψίσυχνες και χαμηλόσυχνες συνιστώσες. Στις υψίσυχνες συνιστώσες συγκεντρώνονται οι λεπτομέρειες (ακμές) του σήματος. Στη συνέχεια το χαμηλόσυχνο σήμα αναλύεται περαιτέρω σε υψηλές και χαμηλές συχνότητες. Η διαδικασία επαναλαμβάνεται όσες φορές χρειάζεται η εκάστοτε εφαρμογή και συνήθως τα επίπεδα ανάλυσης δεν υπερβαίνουν τα πέντε σε εφαρμογές συμπίεσης ή υδατογραφίας. Το αρχικό σήμα μπορεί να ανακατασκευαστεί με χρήση των συντελεστών μετασχηματισμού και η διαδικασία αυτή λέγεται Αντίστροφος Διακριτός Μετασχηματισμός Κυματιδίων (Inverse Discrete Wavelet Transform – IDWT). Η ανάλυση σε επίπεδο κυματιδίων αναπαρίσταται μαθηματικά ως εξής: έστω $H(\omega)$ και $G(\omega)$ ένα βαθυπερατό και ένα υψιπερατό φίλτρο αντίστοιχα, τα οποία ικανοποιούν κάποιες συγκεκριμένες συνθήκες ανακατασκευής που θα παρουσιαστούν στη συνέχεια και τα οποία εκφράζονται από τις σχέσεις:

$$H(\omega) = \sum_k h_k \cdot e^{-j \cdot k \cdot \omega} \quad (6.1)$$

$$G(\omega) = \sum_k g_k \cdot e^{-j \cdot k \cdot \omega} \quad (6.2)$$

Ένα μονοδιάστατο σήμα $F(n)$ αναλύεται διαδοχικά ως εξής:

$$f_{j-1}^{low}(k) = \sum_n h_{n-2k} f_j(n) \quad (6.3)$$

$$f_{j-1}^{high}(k) = \sum_n g_{n-2k} f_j(n) \quad (6.4)$$

όπου $j = J + 1, J, \dots, J_0$ και $f_{J+1}(k) = F(f)$, $k \in \mathbb{Z}$. Το $J + 1$ αποτελεί το δείκτη που αντιστοιχεί στο υψηλότερο επίπεδο ανάλυσης (resolution) και J_0 είναι ο δείκτης

χαμηλού επιπέδου ανάλυσης. Οι συντελεστές $f_{j_0}^{low}(k), f_{j_0}^{high}(k), f_{j_0+1}^{high}(k), \dots, f_j^{high}(k)$ αποτελούν τους συντελεστές Διακριτού Μετασχηματισμού Κυματιδίων του σήματος $F(n)$, όπου $f_{j_0}^{low}(k)$ είναι το τμήμα του σήματος $F(n)$ με τη χαμηλότερη ανάλυση – η λεγόμενη «προσέγγιση» – και $f_j^{high}(k)$ είναι οι λεπτομέρειες του σήματος $F(n)$ σε διάφορα επίπεδα ανάλυσης. Επιπλέον, το σήμα $F(n)$ μπορεί να ανακατασκευαστεί από τους παραπάνω συντελεστές μέσω της ακόλουθης σχέσης:

$$f_j^{low}(n) = \sum_k h_{n-2k} \cdot f_{j-1}^{low}(k) + \sum_k g_{n-2k} \cdot f_{j-1}^{high}(k) \quad (6.5)$$

Απαραίτητη συνθήκη για να ισχύει η παραπάνω σχέση μεταξύ Διακριτού Μετασχηματισμού Κυματιδίων (ΔΜΚ) και Αντίστροφου Διακριτού Μετασχηματισμού Κυματιδίων (ΑΔΜΚ) αποτελεί η ορθογωνιότητα μεταξύ των φίλτρων $H(\omega)$ και $G(\omega)$:

$$|H(\omega)|^2 + |G(\omega)|^2 = 1 \quad (6.6)$$

Ενδεικτικά παρατίθενται τα φίλτρα $H(\omega)$ και $G(\omega)$ του δημοφιλούς κυματιδίου Haar και τα οποία ικανοποιούν την παραπάνω απαίτηση:

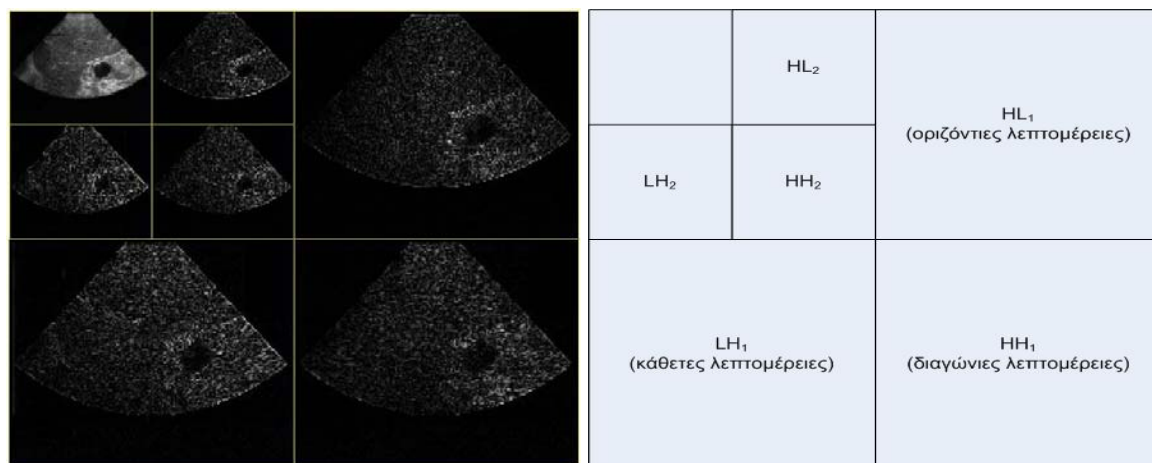
$$H(\omega) = \frac{1}{2} + \frac{1}{2}e^{-j\omega} \quad (6.7)$$

$$G(\omega) = \frac{1}{2} - \frac{1}{2}e^{-j\omega} \quad (6.8)$$

Άλλα γνωστά κυματίδια που χρησιμοποιούνται ευρέως στην επεξεργασία εικόνας είναι τα «ορθογώνια» (D-4, D-6, D-8, D-10, D-12) και «διορθογώνια» (B-5/3, B-7/9) κυματίδια της οικογένειας Daubechies.

Ο διακριτός μετασχηματισμός κυματιδίων μιας εικόνας προκύπτει από τη διαδοχική εφαρμογή του μετασχηματισμού μονοδιάστατου σήματος στις γραμμές και τις στήλες της εικόνας. Το αποτέλεσμα της ανάλυσης μιας εικόνας υπερήχων σε

δύο επίπεδα φαίνεται στο Σχήμα 6. Αξίζει να αναφερθεί ότι υπάρχει και μια παραλλαγή του μετασχηματισμού κυματιδίων, ο λεγόμενος Μετασχηματισμός Κυματιδίων σε Πακέτα (wavelet packet decomposition), κατά τον οποίο αναλύεται όχι μόνο το χαμηλόσυχνο, αλλά και το υψίσυχνο σήμα σε κάθε επίπεδο ανάλυσης.



Σχήμα 6: Ανάλυση εικόνας υπερήχων με εφαρμογή ΔΜΚ σε 2 επίπεδα

Ο διακριτός μετασχηματισμός κυματιδίων παρουσιάζει κάποια πλεονεκτήματα σε σχέση με άλλους μετασχηματισμούς, τα οποία παρατίθενται στη συνέχεια:

- Παρέχει μια πολυδιακριτή ανάλυση (multi-resolution) της εικόνας, δηλαδή μια αναπαράσταση της εικόνας σε διαδοχικά επίπεδα αυξανόμενης ανάλυσης.
- Προσεγγίζει κάποιες λειτουργίες του ανθρώπινου οπτικού συστήματος πολύ περισσότερο από άλλους μετασχηματισμούς (π.χ. DCT), προκαλώντας συγκριτικά μικρότερη οπτική αλλοίωση κατά την υδατογράφηση.
- Παρέχει αναπαράσταση της εικόνας στα πεδία κλίμακας και χώρου (scale-space representation). Στη συγκεκριμένη αναπαράσταση, τα υψίσυχνα σήματα έχουν καθορισμένη θέση με σχετική ακρίβεια σε επίπεδο pixels, ενώ τα χαμηλόσυχνα σήματα έχουν καθορισμένη θέση στο πεδίο της συχνότητας. Καθώς η ανάλυση του μετασχηματισμού κυματιδίων στο πεδίο του χώρου αυξάνει με τη συχνότητα, οι ακμές (sharp edges) που έχουν χωρικά

καθορισμένη θέση και διαθέτουν σημαντική ενέργεια στις υψηλές συχνότητες αναπαρίστανται στις υποζώνες λεπτομερειών και σχηματίζουν το περίγραμμα των αντικειμένων της εικόνας.

Τα υδατογραφικά σχήματα που εφαρμόζονται στο πεδίο του μετασχηματισμού κυματιδίων διαθέτουν αρκετά πλεονεκτήματα, για τα οποία υπάρχουν διάφορες αναφορές στη βιβλιογραφία [4]-[6]:

- Το πεδίο μετασχηματισμού κυματιδίων επιτρέπει πολύ καλή μοντελοποίηση του ανθρώπινου οπτικού συστήματος, καθώς χωρίζει το σήμα σε διακριτές ζώνες που μπορούν να υποστούν επεξεργασία ανεξάρτητα η μία από την άλλη [7]. Έχουν γίνει ήδη αρκετές μελέτες σχετικά με την αξιοποίηση της ιδιότητας επικάλυψης του οπτικού συστήματος (visual masking) στο πεδίο του μετασχηματισμού κυματιδίων, όπως επίσης και σχετικά με το θόρυβο που εισάγεται από την κβαντοποίηση των συντελεστών κυματιδίων (wavelet quantization noise) [8].
- Οι υποζώνες υψηλής ανάλυσης επιτρέπουν το χωρικό προσδιορισμό χαρακτηριστικών της εικόνας, όπως ακμών ή περιοχών έντονης υφής. Συνήθως τα υδατογραφικά σχήματα εισάγουν τα υδατογραφήματα με μεγαλύτερη ένταση στους συντελεστές μετασχηματισμού που έχουν μεγάλες τιμές, με αποτέλεσμα να επηρεάζουν κυρίως τις περιοχές στις οποίες οι όποιες αλλαγές δε γίνονται εύκολα αντιληπτές από το ανθρώπινο μάτι (ακμές, έντονης υφής / δραστηριότητας). Αυτή η τακτική επιτρέπει ουσιαστικά την έμμεση αξιοποίηση της ιδιότητας οπτικής επικάλυψης (implicit masking) στο πεδίο των κυματιδίων. Είναι άλλωστε δεδομένη η ανάγκη κατανόησης και αξιοποίησης των χαρακτηριστικών του ανθρώπινου οπτικού συστήματος προκειμένου να επιτευχθεί μη αντιληπτή υδατογράφιση με μεγάλη χωρητικότητα. Πρέπει να σημειωθεί επίσης ότι η ιδιότητα χωρικού προσδιορισμού των συντελεστών κυματιδίων επιτρέπει την υδατογράφιση εικόνων με καθορισμένη Περιοχή Ενδιαφέροντος [9].

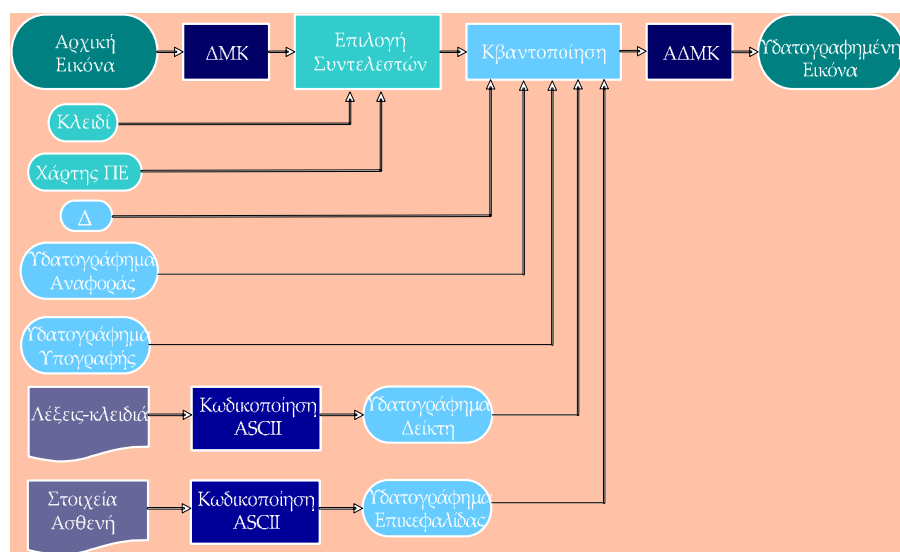
- Η ιεραρχική αναπαράσταση της εικόνας που προκύπτει από την πολυδιακριτή ανάλυση του μετασχηματισμού είναι κατάλληλη για εφαρμογές στις οποίες η εικόνα μεταδίδεται προοδευτικά, σε συστήματα πραγματικού χρόνου (real-time) ή όταν υπάρχει μεγάλος όγκος δεδομένων προς επεξεργασία (π.χ. βίντεο). Οι υδατογραφικοί αλγόριθμοι που ενσωματώνουν ένα «ιεραρχικό» υδατογράφημα παρουσιάζουν αισθητά μειωμένο υπολογιστικό κόστος, όταν το υδατογράφημα ανιχνεύεται / εξάγεται στις πρώτες φάσεις της σταδιακής μετάδοσης. Σε αυτήν την περίπτωση γίνεται σταδιακή επεξεργασία των υποζωνών ξεκινώντας από αυτές της χαμηλότερης ανάλυσης (resolution) και περιλαμβάνοντας διαδοχικά όσες χρειάζονται για την εξαγωγή του υδατογραφήματος.
- Το νέο πρότυπο κωδικοποίησης εικόνας JPEG2000 βασίζεται στο διακριτό μετασχηματισμό κυματιδίων, γεγονός που διευκολύνει τη σχεδίαση ανθεκτικών υδατογραφικών αλγορίθμων, συμβατών με το συγκεκριμένο πρότυπο.

6.3 ΣΥΝΟΨΗ ΠΡΟΤΕΙΝΟΜΕΝΗΣ ΜΕΘΟΔΟΥ

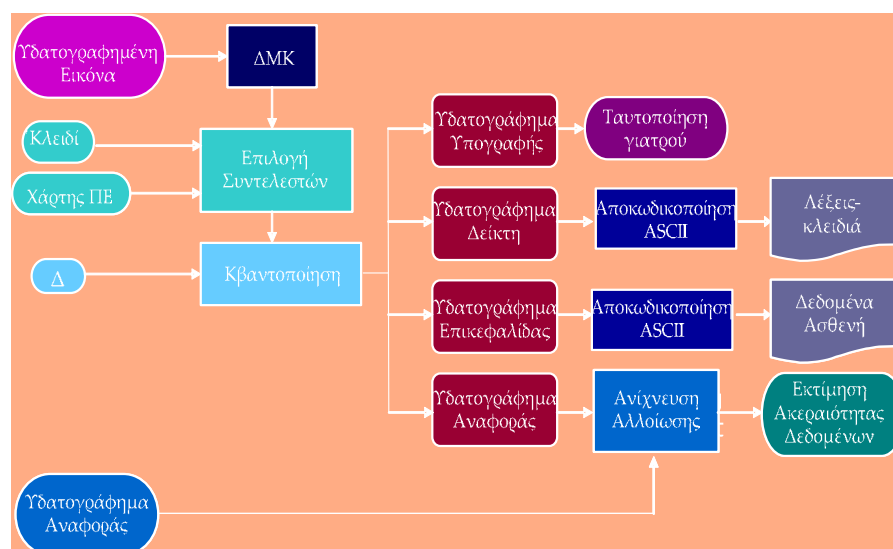
Η μέθοδος που σχεδιάστηκε και αναπτύχθηκε στα πλαίσια της διδακτορικής διατριβής εφαρμόζει Διακριτό Μετασχηματισμό Κυματιδίων Haar (Haar Discrete Wavelet Transform) για την ανάλυση της εικόνας. Οι τεχνικές ενσωμάτωσης υδατογραφημάτων σε πεδίο μετασχηματισμού υπερτερούν σε σχέση με τις τεχνικές στο πεδίο του χώρου ως προς τη διαφάνεια (transparency) και την προστασία των υδατογραφημάτων, καθώς αξιοποιούν τις ιδιότητες της ανθρώπινης αντιληπτικότητας (perceptual properties) επιτυγχάνοντας αύξηση της ανθεκτικότητάς τους σε διάφορες ενέργειες επεξεργασίας εικόνας, χωρίς αλλοίωση του οπτικού αποτελέσματος [10]-[13]. Η ερευνητική κοινότητα έχει εκδηλώσει τα τελευταία χρόνια ιδιαίτερο ενδιαφέρον για την ανάλυση κυματιδίων, κυρίως λόγω της ικανότητάς της να παρέχει ανάλυση τόσο στο πεδίο του χώρου όσο και στο πεδίο της συχνότητας [2], [4], [12]. Επιπλέον, η αξιοσημείωτη ομοιότητα μεταξύ της

δυναδικής ανάλυσης κλίμακας (dyadic scale decomposition) του μετασχηματισμού κυματιδίων και της επεξεργασίας σήματος του ανθρώπινου οπτικού συστήματος, επιτρέπει την προσαρμογή της αλλοίωσης που προκαλείται από κβαντοποίηση ή ενσωμάτωση υδατογραφήματος, λαμβάνοντας υπόψη τις ιδιότητες «επικάλυψης» (masking) του ανθρώπινου ματιού [3]. Πιο συγκεκριμένα, το ανθρώπινο οπτικό σύστημα χωρίζει μια εικόνα σε διάφορα κανάλια συχνότητας, τα οποία επεξεργάζονται τα αντίστοιχα σήματα ανεξάρτητα. Η δυναδική ανάλυση κυματιδίων κάνει μια παρόμοια ανάλυση της εικόνας σε ζώνες, που επιτρέπει ανεξάρτητη επεξεργασία των συνιστωσών που προκύπτουν, χωρίς σημαντική αλληλεπίδρασή τους ως προς το οπτικό αποτέλεσμα [14].

Το υδατογραφικό σχήμα που υλοποιήθηκε στοχεύει στην επίλυση ποικίλων θεμάτων που αφορούν τα συστήματα διαχείρισης ιατρικής πληροφορίας, όπως είναι η προστασία του ιατρικού απορρήτου, ο έλεγχος πρόσβασης και ακεραιότητας των δεδομένων, η αποδοτική διαχείριση και ανάκτηση ιατρικής πληροφορίας, ικανοποιώντας την αυστηρή απαίτηση για διατήρηση της διαγνωστικής αξίας των ιατρικών εικόνων. Προκειμένου να συμβάλει στην αντιμετώπιση των παραπάνω θεμάτων, το σχήμα παρέχει τη δυνατότητα ταυτόχρονης ενσωμάτωσης τεσσάρων τύπων υδατογραφημάτων σε εικόνες, κάθε ένα από τα οποία εξυπηρετεί διαφορετικό σκοπό. Οι διαδικασίες εισαγωγής και εξαγωγής των πολλαπλών υδατογραφημάτων παρουσιάζονται στα Σχήματα 7 και 8 αντιστοίχως.



Σχήμα 7: Διαδικασία εισαγωγής πολλαπλών υδατογραφημάτων



Σχήμα 8: Διαδικασία εξαγωγής πολλαπλών υδατογραφημάτων

Τα τέσσερα υδατογραφήματα που επιτρέπει το σχήμα να ενσωματωθούν ταυτόχρονα σε μια εικόνα περιλαμβάνουν:

1. Ένα υδατογράφημα υπογραφής (signature watermark) που περιέχει την ψηφιακή υπογραφή ή τον αναγνωριστικό κωδικό του γιατρού χρησιμοποιείται για πιστοποίηση της πηγής από τον παραλήπτη.
2. Ένα υδατογράφημα δείκτη (index watermark), το οποίο αποτελείται από λέξεις-κλειδιά (π.χ. διαγνωστικοί κωδικοί ICD-10 ή CPT), που μπορούν να χρησιμοποιηθούν για ανάκτηση εικόνων και άλλης σχετικής πληροφορίας από μηχανισμούς αναζήτησης βάσεων δεδομένων, ενσωματώνεται ως χωριστό υδατογράφημα.
3. Ένα υδατογράφημα επικεφαλίδας (caption watermark), που περιλαμβάνει προσωπικά δεδομένα του ασθενή και πρόσθετη πληροφορία που βοηθάει στη διάγνωση, εισάγεται επίσης στην εικόνα. Το υδατογράφημα επικεφαλίδας μπορεί στην πράξη να περιλαμβάνει δημογραφικά στοιχεία του ασθενή, ιατρικό ιστορικό, διαγνωστικές αναφορές κ.λπ.
4. Ένα υδατογράφημα αναφοράς (reference watermark) [15] εισάγεται σε όλα τα επίπεδα ανάλυσης με σκοπό τον έλεγχο ακεραιότητας των δεδομένων και τον προσδιορισμό τυχόν αλλοιωμένων τμημάτων. Το υδατογράφημα

αυτό είναι εκ των προτέρων γνωστό στον παραλήπτη και η εξαγωγή του από την υδατογραφημένη εικόνα παρέχει πληροφορίες σχετικά με το εάν και σε ποια σημεία υπάρχει παραποίηση. Οι πληροφορίες αυτές προκύπτουν από μια εικόνα διαφοράς (difference image) που απεικονίζει τα σημεία της εικόνας που φέρουν τροποποιημένα bits του υδατογραφήματος αναφοράς, φανερώνοντας κατά συνέπεια τα τμήματα της εικόνας που έχουν ενδεχομένως υποστεί αλλοιώσεις.

Τα υδατογραφήματα ενσωματώνονται σε διαφορετικά επίπεδα ανάλυσης (decomposition levels) και σε διαφορετικές υποζώνες (subbands), ανάλογα με τον τύπο και τα χαρακτηριστικά τους, και σε θέσεις που καθορίζονται με τη χρήση τυχαίου κλειδιού. Με αυτόν τον τρόπο, τα υδατογραφήματα μπορούν να ενσωματωθούν και να ανακτηθούν ανεξάρτητα το ένα από το άλλο, χωρίς μεταξύ τους παρεμβολές. Το υδατογράφημα αναφοράς ενσωματώνεται σε συντελεστές που αντιστοιχούν σε ολόκληρη την εικόνα, με σκοπό να παράσχει τη δυνατότητα ελέγχου της ακεραιότητας του συνόλου της εικόνας, ενώ τα υδατογραφήματα υπογραφής, δείκτη και επικεφαλίδας ενσωματώνονται σε περιοχές χωρίς διαγνωστική αξία. Με αυτόν τον τρόπο, οι Περιοχές Ενδιαφέροντος φέρουν μόνο την πληροφορία που απαιτείται για τον έλεγχο ακεραιότητας, αποφεύγοντας έτσι οποιοδήποτε συμβιβασμό ως προς την ποιότητα και τη διαγνωστική αξία της εικόνας.

6.4 ΠΕΡΙΓΡΑΦΗ ΑΛΓΟΡΙΘΜΟΥ

Στην παρούσα ενότητα περιγράφεται αναλυτικά ο αλγόριθμος που σχεδιάστηκε και αναπτύχθηκε στα πλαίσια της διδακτορικής διατριβής.

Η διαδικασία εισαγωγής πολλαπλών υδατογραφημάτων βασίζεται στην κατάλληλη κβαντοποίηση επιλεγμένων συντελεστών, που έχει ως αποτέλεσμα την παραγωγή ακέραιων τιμών στο πεδίο του χώρου (pixels). Αυτό είναι εφικτό λόγω της επιλογής του κυματιδίου Haar για την ανάλυση της εικόνας· ο μετασχηματισμός κυματιδίων Haar παράγει συντελεστές που ανήκουν στους λεγόμενους «δυαδικούς ρητούς αριθμούς» (dyadic rational numbers), των οποίων οι παρονομαστές

αποτελούν δυνάμεις του 2 [16]. Η προσθαφαίρεση στους συντελεστές ενός πολλαπλάσιου του 2^l , όπου l είναι το επίπεδο ανάλυσης, έχει ως αποτέλεσμα η εφαρμογή Αντίστροφου Μετασχηματισμού Κυματιδίων να παράγει ακέραιες τιμές για τα pixels της εικόνας [17]. Η ιδιότητα αυτή αξιοποιείται στη διαδικασία ενσωμάτωσης των υδατογραφημάτων προκειμένου να αυξηθεί η ανθεκτικότητά τους. Όπως θα παρουσιαστεί πιο αναλυτικά παρακάτω, τα bits της πρόσθετης πληροφορίας ενσωματώνονται στην εικόνα με προσθαφαίρεση μιας κατάλληλης σταθεράς στους προς υδατογράφιση συντελεστές κυματιδίων. Με αυτόν τον τρόπο εξασφαλίζεται ότι η εφαρμογή Αντίστροφου Μετασχηματισμού Κυματιδίων στους τροποποιημένους συντελεστές οδηγεί σε ακέραιες τιμές που αναπαριστούν την υδατογραφημένη εικόνα, αποφεύγοντας στρογγυλοποιήσεις που θα μπορούσαν να καταστρέψουν τμήμα της πρόσθετης πληροφορίας. Η διαδικασία της ενσωμάτωσης των πολλαπλών υδατογραφημάτων περιγράφεται στη συνέχεια.

Γενικά, ένας μετασχηματισμός κυματιδίων παράγει συντελεστές λεπτομερειών (detail coefficients) που είναι πραγματικοί αριθμοί. Ο κανόνας τον οποίο ακολουθεί η διαδικασία κβαντοποίησης του αλγορίθμου έχει ως εξής: σε κάθε συντελεστή λεπτομερειών ανατίθεται μια δυαδική τιμή μέσω της συνάρτησης κβαντοποίησης:

$$Q(f) = \begin{cases} 0, & \text{if } 2k \cdot \Delta + s \leq f < (2k+1) \cdot \Delta + s \\ 1, & \text{if } (2k+1) \cdot \Delta + s \leq f < (2k+2) \cdot \Delta + s \end{cases} \quad (6.9)$$

όπου k είναι ακέραιος αριθμός, s είναι μία μετατόπιση (offset) που καθορίζεται από το χρήστη για μεγαλύτερη ασφάλεια και Δ είναι η παράμετρος κβαντοποίησης που είναι ένας θετικός πραγματικός αριθμός.

Η παραπάνω συνάρτηση κβαντοποίησης μπορεί να γραφτεί επίσης ως εξής:

$$Q(f) = \begin{cases} 0, & \text{if } \lfloor (f-s)/\Delta \rfloor \text{ άρτιος} \\ 1, & \text{if } \lfloor (f-s)/\Delta \rfloor \text{ περιττός} \end{cases} \quad (6.10)$$

Όπως προαναφέρθηκε, η προσθαφαίρεση ενός πολλαπλάσιου του 2^l στους συντελεστές Haar έχει ως αποτέλεσμα την παραγωγή ακέραιων τιμών για τα pixels της εικόνας μέσω της εφαρμογής του Αντίστροφου Μετασχηματισμού Κυματιδίων.

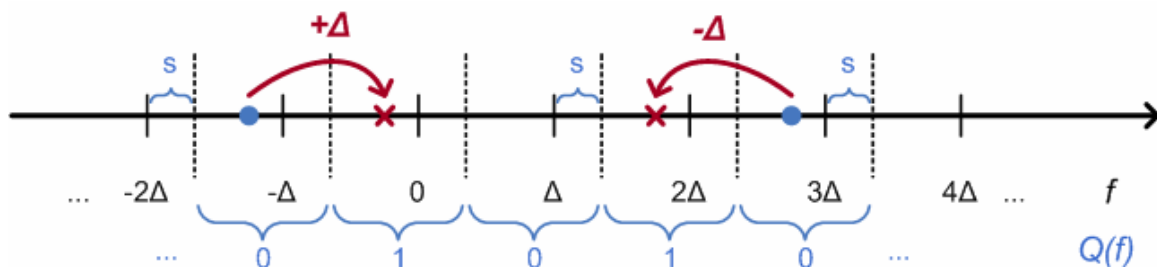
Αξιοποιώντας αυτήν την ιδιότητα, η διαδικασία εισαγωγής των υδατογραφημάτων βασίζεται στην επιλογή μιας κατάλληλης σταθεράς κβαντοποίησης, που είτε προστίθεται είτε αφαιρείται από τους συντελεστές που επιλέγονται για υδατογράφηση. Συγκεκριμένα, η παράμετρος κβαντοποίησης Δ ορίζεται ως: $\Delta = 2^l$, όπου l , όπως προαναφέρθηκε, είναι το επίπεδο ανάλυσης.

Η διαδικασία εισαγωγής πολλαπλών υδατογραφημάτων που αναπτύχθηκε περιγράφεται παρακάτω:

1. Γίνεται ανάλυση κυματιδίων Haar 4 επιπέδων, από την οποία προκύπτει μια προσέγγιση της εικόνας (image approximation) στο χαμηλότερο επίπεδο ευκρίνειας (resolution) και μια σειρά «εικόνων λεπτομερειών» (detail images), που αντιστοιχούν στις οριζόντιες, κάθετες και διαγώνιες λεπτομέρειες σε κάθε επίπεδο ανάλυσης (decomposition level).
2. Σε κάθε επίπεδο ανάλυσης, ένα bit υδατογραφήματος w_i ενσωματώνεται σε ένα συντελεστή f ως εξής:
 - Εάν $Q(f) = w_i$, δε γίνεται καμιά τροποποίηση στο συντελεστή
 - Εάν $Q(f) \neq w_i$, ο συντελεστής τροποποιείται μέσω της ακόλουθης συνάρτησης, έτσι ώστε να ισχύει $Q(f) = w_i$:

$$f = \begin{cases} f + \Delta, & \text{εάν } f \leq 0 \\ f - \Delta, & \text{εάν } f > 0 \end{cases} \quad (6.11)$$

3. Εφαρμόζεται Αντίστροφος Μετασχηματισμός Κυματιδίων Haar 4 επιπέδων για να προκύψει η υδατογραφημένη εικόνα.



Σχήμα 9: Διαδικασία κβαντοποίησης

Η διαδικασία κβαντοποίησης που περιγράφηκε παραπάνω απεικονίζεται στο Σχήμα 9. Αξίζει να σημειωθεί ότι η φύση της ανάθεσης τιμών στο συντελεστή f στην εξίσωση (6.11) έχει πειραματικά αποδειχτεί ότι προκαλεί την ελάχιστη οπτική αλλοίωση στην εικόνα [17].

Η εξαγωγή των πολλαπλών υδατογραφημάτων απαιτεί γνώση του κλειδιού που χρησιμοποιήθηκε κατά τη διαδικασία εισαγωγής τους και γίνεται με την εφαρμογή Μετασχηματισμού Κυματιδίων Haar 4 επιπέδων στην υδατογραφημένη εικόνα και εντοπισμό των θέσεων των υδατογραφημάτων με βάση το κλειδί. Τα bits των υδατογραφημάτων εξάγονται στη συνέχεια με εφαρμογή της συνάρτησης κβαντοποίησης σε κάθε υδατογραφημένο συντελεστή.

Σημειώνεται ότι στην περίπτωση που το υδατογράφημα υπογραφής αποτελείται από τον αναγνωριστικό κωδικό του γιατρού κρυπτογραφημένο με κάποιο ιδιωτικό κλειδί, θα πρέπει μετά την εξαγωγή του να χρησιμοποιηθεί το αντίστοιχο δημόσιο κλειδί για την αποκρυπτογράφηση του και για την απόκτηση τελικά των δεδομένων πιστοποίησης της πηγής προέλευσης.

6.5 ΕΠΙΛΟΓΗ ΣΥΝΤΕΛΕΣΤΩΝ ΓΙΑ ΥΔΑΤΟΓΡΑΦΗΣΗ

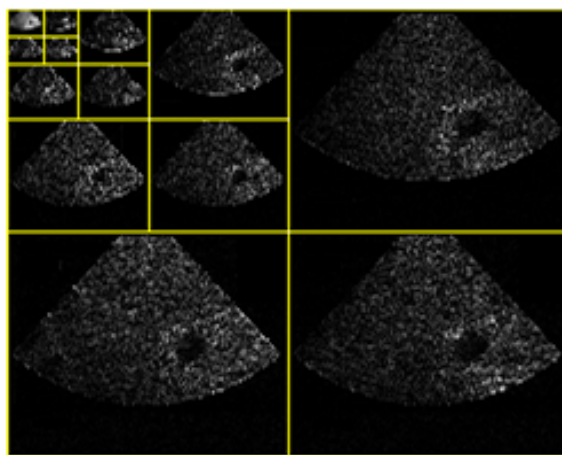
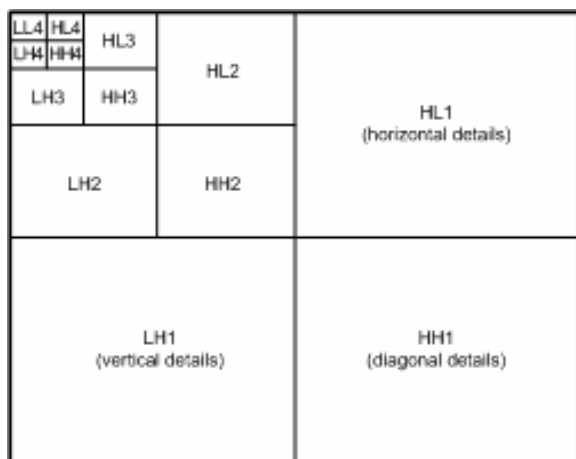
Το υδατογράφημα που περιέχει τον αναγνωριστικό κωδικό του γιατρού απαιτεί μεγάλη ανθεκτικότητα προκειμένου να εξασφαλιστεί η εξαγωγή αναλλοίωτης ψηφιακής υπογραφής, που θα επιτρέπει την ορθή πιστοποίηση. Η χωρητικότητα δεν αποτελεί βασική παράμετρο όσον αφορά το συγκεκριμένο τύπο υδατογραφήματος, δεδομένου ότι η ψηφιακή υπογραφή την οποία μεταφέρει είναι περιορισμένου μήκους. Με βάση τα παραπάνω, το υδατογραφικό σχήμα ενσωματώνει το υδατογράφημα υπογραφής στο τέταρτο επίπεδο ανάλυσης, δεδομένου ότι η ανθεκτικότητα αυξάνει όσο αυξάνει το επίπεδο ανάλυσης. Στο τέταρτο επίπεδο ανάλυσης η χωρητικότητα είναι περιορισμένη, αλλά όπως προαναφέρθηκε, αυτό δεν αποτελεί πρόβλημα για το συγκεκριμένο τύπο υδατογραφήματος.

Ανάγκη για αυξημένη ανθεκτικότητα υπάρχει και στην περίπτωση των υδατογραφημάτων δείκτη και επικεφαλίδας, αλλά όχι στο βαθμό που απαιτείται

στην προηγούμενη περίπτωση, στην οποία ακόμη και ένα λανθασμένο bit θα μπορούσε να οδηγήσει σε αποτυχία πιστοποίησης. Από την άλλη μεριά, τα υδατογραφήματα δείκτη και επικεφαλίδας έχουν συνήθως αυξημένες απαιτήσεις χωρητικότητας, καθώς σκοπός τους είναι να μεταφέρουν πολλά bits πρόσθετης πληροφορίας. Πιο συγκεκριμένα, το υδατογράφημα επικεφαλίδας προορίζεται για την εισαγωγή προσωπικών στοιχείων του ασθενή, στοιχεία εξέτασης, ιατρικό ιστορικό κ.λπ., απαιτώντας επομένως αυξημένη χωρητικότητα. Το υδατογράφημα δείκτη μεταφέρει λέξεις-κλειδιά που μπορούν να χρησιμοποιηθούν για ανάκτηση εικόνων, επομένως η ανάγκη για χωρητικότητα είναι προφανώς μικρότερη απ' ό,τι στην περίπτωση του υδατογραφήματος επικεφαλίδας, αλλά μεγαλύτερη απ' ό,τι στην περίπτωση του υδατογραφήματος υπογραφής. Λαμβάνοντας υπόψη τις παραπάνω απαιτήσεις, το υδατογράφημα δείκτη ενσωματώνεται στο τρίτο επίπεδο ανάλυσης της εικόνας, το οποίο προσφέρει έναν κατάλληλο συνδυασμό (trade-off) ανθεκτικότητας και χωρητικότητας. Το υδατογράφημα επικεφαλίδας από την άλλη πλευρά εισάγεται στο δεύτερο επίπεδο ανάλυσης, που παρέχει μεγαλύτερη χωρητικότητα. Τέλος, το πρώτο επίπεδο ανάλυσης χρησιμοποιείται για ενσωμάτωση του υδατογραφήματος αναφοράς προκειμένου να επιτρέψει έλεγχο ακεραιότητας δεδομένων. Το υδατογράφημα αναφοράς εισάγεται επίσης σε επιλεγμένους συντελεστές και των άλλων τριών επιπέδων ανάλυσης, ώστε να είναι εφικτή η εκτίμηση της αλλοίωσης του συνόλου της εικόνας [18].

Γενικά, οι οριζόντιες και οι κάθετες υποζώνες έχουν παρόμοια συμπεριφορά και χαρακτηριστικά, σε αντίθεση με τη διαγώνια υποζώνη [19]. Μια ενδεχόμενη τροποποίηση στην εικόνα είναι επομένως πολύ πιθανό να επηρεάσει τόσο τους οριζόντιους όσο και τους κάθετους συντελεστές· αυτός είναι ο λόγος για τον οποίο επιλέγονται συντελεστές από την οριζόντια και την κάθετη υποζώνη για την εισαγωγή των υδατογραφημάτων δεδομένων (υπογραφή, δείκτες, πρόσθετη πληροφορία) και των υδατογραφημάτων αναφοράς αντίστοιχα. Το Σχήμα 10 απεικονίζει την πυραμιδική δομή της ανάλυσης μιας εικόνας που προκύπτει από εφαρμογή Διακριτού Μετασχηματισμού Κυματιδίων τεσσάρων επιπέδων, η οποία παράγει μια προσέγγιση της εικόνας (coarse scale approximation) στο υψηλότερο επίπεδο ανάλυσης (LL4) και δώδεκα εικόνες λεπτομερειών που αντιστοιχούν στις

οριζόντιες (HL), κάθετες (LH) και διαγώνιες (HH) λεπτομέρειες σε καθένα από τα τέσσερα επίπεδα ανάλυσης.



(α)

(β)

Σχήμα 10: Πολυδιακριτή ανάλυση εικόνας με εφαρμογή μετασχηματισμού κυματιδίων.
(α) Πυραμидική δομή ΔΜΚ 4 επιπέδων. (β) ΔΜΚ 4 επιπέδων σε εικόνα υπερήχων.

Ο Πίνακας 2 παρουσιάζει την ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών που προκύπτουν από το διακριτό μετασχηματισμό κυματιδίων τεσσάρων επιπέδων της εικόνας αξονικής τομογραφίας που απεικονίζεται στο Σχήμα 11.

Υποζώνη	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
Προσέγγιση Εικόνας	-	-	-	440,17
Οριζόντιες Λεπτομέρειες	1,93	5,95	16,72	44,50
Κάθετες Λεπτομέρειες	1,30	3,60	9,45	26,63
Διαγώνιες Λεπτομέρειες	0,59	2,17	6,52	18,19

Πίνακας 2: Ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών Διακριτού Μετασχηματισμού Κυματιδίων 4 επιπέδων εικόνας CT



Σχήμα 11: Εικόνα αξονικής τομογραφίας (CT)

Η ενέργεια υπολογίζεται από τον ακόλουθο τύπο:

$$e_k = \frac{1}{N_k \cdot M_k} \sum_i \sum_j |I_k(i, j)| \quad (6.12)$$

όπου η μεταβλητή k δηλώνει την προσέγγιση και τις εικόνες λεπτομερειών σε καθένα από τα επίπεδα ανάλυσης, I_k είναι οι συντελεστές των εικόνων υποζωνών, και N_k, M_k είναι οι αντίστοιχες διαστάσεις. Ο Πίνακας 2 φανερώνει το γεγονός ότι η ενέργεια συγκεντρώνεται στα υψηλά επίπεδα ανάλυσης (decomposition levels) που αντιστοιχούν στους σημαντικούς αισθητικά χαμηλόσυχρους συντελεστές. Τα επίπεδα χαμηλής ανάλυσης συγκεντρώνουν ένα ελάχιστο ποσοστό ενέργειας, γεγονός που τα καθιστά ευάλωτα σε τυχόν τροποποιήσεις στην εικόνα. Ο πίνακας φανερώνει επίσης την αξιοσημείωτα μεγάλη συγκέντρωση ενέργειας στις οριζόντιες υποζώνες, σε σχέση με τις κάθετες και κυρίως με τις διαγώνιες υποζώνες. Επομένως, η ενσωμάτωση υδατογραφημάτων στις οριζόντιες υποζώνες εγγυάται αυξημένη ανθεκτικότητα, καθώς η συγκέντρωση υψηλού ποσοστού ενέργειας σε αυτές τις καθιστά λιγότερο ευάλωτες σε επιθέσεις.

Από την άλλη πλευρά, η προσέγγιση της εικόνας στο τελευταίο επίπεδο ανάλυσης (coarse scale approximation) συγκεντρώνει το μεγαλύτερο ποσοστό της συνολικής ενέργειας της εικόνας και έχει μεγάλη επίδραση στην ποιότητα της

εικόνας. Για αυτόν το λόγο αποκλείεται από τη διαδικασία υδατογράφησης, προκειμένου να αποφευχθεί οποιαδήποτε ορατή αλλοίωση της εικόνας.

Προκειμένου να αυξηθεί η ανθεκτικότητα των υδατογραφημάτων που φέρουν τα πρόσθετα δεδομένα (υπογραφή, δείκτες, στοιχεία ασθενή), αποκλείονται και οι διαγώνιες υποζώνες, οι οποίες τροποποιούνται ή εξαλείφονται με συνήθη επεξεργασία ή συμπίεση, λόγω της ελάχιστης επίδρασης που έχουν στην ποιότητα της εικόνας. Οι συντελεστές του πρώτου επιπέδου ανάλυσης τροποποιούνται επίσης εύκολα με συνηθισμένες ενέργειες επεξεργασίας της εικόνας. Για αυτόν το λόγο χρησιμοποιούνται μόνο για εισαγωγή υδατογραφημάτων αναφοράς, τα οποία επιτρέπουν τον έλεγχο της ακεραιότητας της εικόνας. Τα παραπάνω ελήφθησαν υπόψη στη σχεδίαση του υδατογραφικού σχήματος και στην κατανομή των πολλαπλών υδατογραφημάτων στην εικόνα, με σκοπό τη βέλτιστη απόδοση όσον αφορά την ανθεκτικότητα και τη διαφάνεια. Πρέπει να σημειωθεί πως παρά το γεγονός ότι η συγκέντρωση της ενέργειας ανά υποζώνη και επίπεδο ανάλυσης εξαρτάται από τα χαρακτηριστικά της εικόνας, υπάρχουν κάποιες κοινές ιδιότητες μεταξύ των διαφορετικών τύπων εικόνων, στις οποίες και βασίστηκε η κατανομή των υδατογραφημάτων στις διάφορες υποζώνες [20]. Τα ποσοστά συγκέντρωσης ενέργειας ανά υποζώνη διαφέρουν μεταξύ διαφορετικών εικόνων, αλλά τα συμπεράσματα που καταγράφηκαν παραπάνω προέκυψαν βάσει των γενικών χαρακτηριστικών και δεν προήλθαν μόνο από τη μελέτη της ενέργειας στην περίπτωση εικόνων αξονικής τομογραφίας. Αυτό θα γίνει φανερό και στο επόμενο κεφάλαιο, όπου παρουσιάζεται η κατανομή της ενέργειας ανά επίπεδο ανάλυσης και υποζώνη και για άλλους τύπους εικόνων.

Ο κίνδυνος που υπάρχει από οποιοδήποτε συμβιβασμό σε ό,τι αφορά την ποιότητα των ιατρικών εικόνων, που θα μπορούσε να οδηγήσει σε λανθασμένη διάγνωση και ακατάλληλη θεραπευτική αγωγή, έχει ως αποτέλεσμα την εφαρμογή αυστηρών περιορισμών ως προς τις αποδεκτές ενέργειες επεξεργασίας τους και ιδιαίτερα των διαγνωστικά σημαντικών τμημάτων τους. Λαμβάνοντας αυτούς τους περιορισμούς υπόψη, το υδατογραφικό σχήμα που αναπτύχθηκε επιτρέπει τον καθορισμό μιας *Περιοχής Ενδιαφέροντος* (Region of Interest, ROI) και παρέχει τη δυνατότητα υδατογράφησης της συγκεκριμένης περιοχής αποκλειστικά με το

υδατογράφημα αναφοράς, το οποίο θα αντανakλά πιθανή αλλοίωσή της. Η υπόλοιπη εικόνα, η οποία δεν υπόκειται στους αυστηρούς περιορισμούς της Περιοχής Ενδιαφέροντος, μπορεί να χρησιμοποιηθεί για την ενσωμάτωση όλων των υδατογραφημάτων. Αποτελεί άλλωστε συνήθη πρακτική να ορίζεται κάποια Περιοχή Ενδιαφέροντος κατά τη λήψη ή αρχειοθέτηση μιας ιατρικής εικόνας· σε περίπτωση που δε συμβαίνει κάτι τέτοιο, μπορεί ακόμη και κάποιος μη εξειδικευμένος χρήστης να ορίσει μια εκτεταμένη περιοχή που να καλύπτει όλα τα μέρη της εικόνας που πιθανόν να έχουν διαγνωστική αξία, ώστε να αξιοποιήσει τη δυνατότητα ελάχιστης υδατογράφησης στα κρίσιμα τμήματα. Πρέπει πάντως να σημειωθεί ότι ακόμη και στην περίπτωση κατά την οποία δεν ορίζεται Περιοχή Ενδιαφέροντος και γίνεται ενσωμάτωση των πολλαπλών υδατογραφημάτων σε ολόκληρη την εικόνα, δεν τίθεται θέμα αλλοίωσης της πιστότητας της εικόνας, γεγονός που καταδεικνύεται από τις δοκιμές που έγιναν και παρουσιάζονται στο επόμενο κεφάλαιο.

Λαμβάνοντας υπόψη ότι η ανθεκτικότητα αυξάνεται ενώ η χωρητικότητα μειώνεται στα υψηλότερα επίπεδα ανάλυσης κυματιδίων, τα υδατογραφήματα επικεφαλίδας, δείκτη και υπογραφής ενσωματώνονται σε συντελεστές οριζοντίων λεπτομερειών του δεύτερου, τρίτου και τέταρτου επιπέδου ανάλυσης αντίστοιχα, που δεν ανήκουν στην Περιοχή Ενδιαφέροντος (ROI). Το υδατογράφημα αναφοράς ενσωματώνεται σε συντελεστές κάθετων λεπτομερειών όλων των επιπέδων ανάλυσης και οι οποίοι αντιστοιχούν σε όλη την εικόνα, επιτρέποντας με αυτόν τον τρόπο καθολικό έλεγχο της εικόνας και αποτίμηση των αλλοιώσεων. Η μικρή τροποποίηση μεμονωμένων, σποραδικών συντελεστών κάθετων λεπτομερειών, που ανήκουν ακόμη και στα υψηλά επίπεδα ανάλυσης, αναμένεται να προκαλέσει μια μηδαμινή, μη ορατή αλλοίωση, που δεν επηρεάζει στο ελάχιστο την πιστότητα της Περιοχής Ενδιαφέροντος. Αυτή η υπόθεση επαληθεύτηκε στην πράξη από τις δοκιμές που έγιναν, όπως θα φανεί στο επόμενο κεφάλαιο με τα αποτελέσματα των δοκιμών σε διάφορα είδη ιατρικών εικόνων. Σε περίπτωση ανίχνευσης παραποίησης τμήματος της εικόνας, η σύγκριση του εξαγχθέντος υδατογραφήματος αναφοράς με το αρχικό σε κάθε επίπεδο ανάλυσης χωριστά, παρέχει μια λεπτομερή εικόνα των αλλοιώσεων και επιτρέπει την αποτίμησή τους.

Ο Πίνακας 3 παρουσιάζει τις υποζώνες που χρησιμοποιήθηκαν για την ενσωμάτωση των διαφόρων τύπων υδατογραφημάτων και την αντίστοιχη χωρητικότητά τους, το πλήθος δηλαδή των συντελεστών τους, το οποίο αντιπροσωπεύει το μέγιστο αριθμό των bits υδατογραφήματος που μπορούν να ενσωματώσουν. Σημειώνεται ότι η χωρητικότητα που εμφανίζεται στον Πίνακα 3 αντιστοιχεί στην περίπτωση εικόνων με διαστάσεις 256x320 pixels.

Υποζώνη	Χωρητικότητα (υδατογραφήσιμοι συντελεστές)	Υδατογράφημα	
		Τύπος	Απαίτηση Ανθεκτικότητας
LH1	20.480	Αναφοράς	Χαμηλή
HL2	5.120	Επικεφαλίδα	Υψηλή
LH2	5.120	Αναφοράς	Χαμηλή
HL3	1.280	Δείκτης	Υψηλή
LH3	1.280	Αναφοράς	Χαμηλή
HL4	320	Υπογραφή	Πολύ υψηλή
LH4	320	Αναφοράς	Χαμηλή

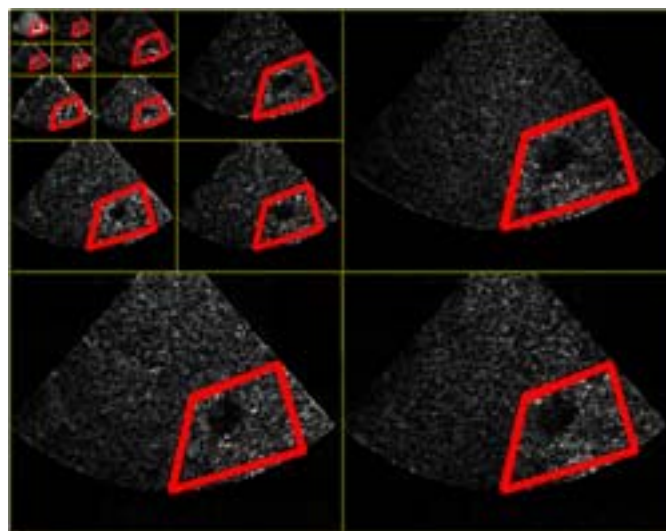
Πίνακας 3: Κατανομή πολλαπλών υδατογραφημάτων στις υποζώνες βάσει απαιτήσεων ανθεκτικότητας και χωρητικότητας

Ο πίνακας δείχνει την κατανομή των τεσσάρων τύπων υδατογραφημάτων στις επιλεγμένες υποζώνες, όπως αυτή προέκυψε με βάση τις απαιτήσεις του κάθε υδατογραφήματος ως προς την ανθεκτικότητα και τη χωρητικότητα. Πρέπει πάντως να σημειωθεί ότι η χωρητικότητα που αντιστοιχεί στις οριζόντιες υποζώνες είναι η μέγιστη δυνατή, που είναι διαθέσιμη μόνο στην περίπτωση που δεν έχει εξαιρεθεί από τη διαδικασία υδατογράφησης καμία περιοχή της εικόνας. Σε οποιαδήποτε άλλη περίπτωση, η έκταση της Περιοχής Ενδιαφέροντος είναι αυτή που καθορίζει το πλήθος των συντελεστών σε κάθε οριζόντια υποζώνη, οι οποίοι επιτρέπεται να υδατογραφηθούν με το να μην ανήκουν στην περιοχή που έχει διαγνωστική αξία.

Όπως προαναφέρθηκε, η επιλογή των συντελεστών στους οποίους ενσωματώνονται τα υδατογραφήματα γίνεται με βάση την τιμή ενός κλειδιού. Στην πραγματικότητα, το κλειδί καθορίζει ποιοι συντελεστές κάθετων λεπτομερειών θα χρησιμοποιηθούν για ενσωμάτωση του υδατογραφήματος αναφοράς, ανεξαρτήτως

του εάν ανήκουν στην Περιοχή Ενδιαφέροντος ή όχι. Στην περίπτωση των υδατογραφημάτων δεδομένων (υπογραφή, δείκτες, στοιχεία ασθενή) όμως, η επιλογή των συντελεστών οριζόντιων λεπτομερειών που θα τα ενσωματώσουν γίνεται με βάση όχι μόνο την τιμή του κλειδιού, αλλά και τον Πίνακα Περιοχής Ενδιαφέροντος (ROI map). Το κλειδί καθορίζει εάν ένας συγκεκριμένος συντελεστής θα υδατογραφηθεί, αλλά τελικά ο συντελεστής αυτός θα χρησιμοποιηθεί για ενσωμάτωση ενός bit υδατογραφήματος μόνο εάν δεν ανήκει στην Περιοχή Ενδιαφέροντος.

Ο Πίνακας Περιοχής Ενδιαφέροντος του πεδίου κυματιδίων (wavelet domain ROI map) που καθορίζει τους συντελεστές οι οποίοι επιτρέπεται να χρησιμοποιηθούν για υδατογράφιση, προκύπτει από τον Πίνακα Περιοχής Ενδιαφέροντος του χωρικού πεδίου (spatial domain ROI map), με βάση τη χωρική ομοιότητα (spatial self-similarity) που παρουσιάζουν οι υποζώνες κυματιδίων [9]. Πιο συγκεκριμένα, ο χωρικός χάρτης ROI χωρίζεται σε μπλοκ των 16x16 pixels· εάν κάποιο από τα pixels του μπλοκ ανήκει στο ROI, το αντίστοιχο μπλοκ 8x8 στο πρώτο επίπεδο ανάλυσης θα ανήκει επίσης στο ROI. Αυτό αντιστοιχεί σε ένα μπλοκ 4x4 συντελεστών του δευτέρου επιπέδου, ένα μπλοκ 2x2 στο τρίτο επίπεδο και σε ένα μόνο συντελεστή στο τέταρτο επίπεδο ανάλυσης [18]. Η αντιστοιχία ανάμεσα στους Πίνακες Περιοχής Ενδιαφέροντος μιας εικόνας υπερήχων, στην οποία εφαρμόστηκε μετασχηματισμός κυματιδίων σε τέσσερα επίπεδα, φαίνεται στο Σχήμα 12.



Σχήμα 12: Αντιστοιχία των Πινάκων Περιοχής Ενδιαφέροντος ανά υποζώνη και επίπεδο ανάλυσης

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

- [1] J. M. Shapiro, "Embedded Image Coding Using Zerotrees of Wavelet Coefficients," *IEEE Trans. Signal Processing*, vol. 41, no.12, pp. 3445-3462, Dec. 1993.
- [2] M. Unser, A. Aldroubi, "A review of wavelets in biomedical applications," in *Proc. IEEE*, vol. 84, no. 4, pp. 626-638, April 1996.
- [3] P. Meerwald, A. Uhl, "A survey of wavelet-domain watermarking algorithms," in *Proc. SPIE Security and Watermarking of Multimedia Contents III*, SPIE2001, San Jose, USA, vol. 4314, pp. 505-516, Jan. 2001.
- [4] X. G. Xia, C. G. Boncelet, G. R. Arce, "Wavelet transform based watermark for digital images," *Optics Express*, vol. 3, no. 12, pp. 497-511, Dec. 1998.
- [5] M. Barni, F. Bartolini, V. Cappelini, A. Lippi, A. Piva, "A DWT-based technique for spatio-frequency masking of digital signatures," *Proc. 11th SPIE Annual Symposium, Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, vol. 3657, pp.31-39, San Jose, CA, USA, Jan. 1999.
- [6] R. Dugad, K. Ratakonda, N. Ahuja, "A new wavelet-based scheme for watermarking images," *Proc. IEEE Int. Conf. Image Processing, ICIP'98*, Oct. 1998.
- [7] R. Martin, D. Cochran, "Generalized wavelet transforms and the cortex transform," *Proc. 28th Asilomar Conf. Signals, Systems, and Computers*, Nov. 1994.
- [8] A. B. Watson, G. Y. Yang, J.A. Solomon, J.Villasenor, "Visibility of wavelet quantization noise," *IEEE Trans. Image Processing*, no. 6, pp. 1164-1175, 1997.
- [9] P. C. Su, H. J. Wang, C. C. J. Kuo, "Digital image watermarking in regions of interest," *Proc. IS&T Conf. Image Processing, Image Quality, Image Capture Systems (PICS 99)*, pp. 295-300, Savannah Georgia, April 25-28, 1999.
- [10] X. G. Xia, C. G. Boncelet, G. R. Arce, "A multiresolution watermark for digital images," *Proc. IEEE Int. Conf. Image Processing*, v.1, pp. 548-551, Santa Barbara, CA, Oct. 26-29, 1997.
- [11] H. J. M. Wang, P. C. Su, C. C. J. Kuo, "Wavelet-based digital image watermarking," *Optics Express*, vol. 3, no. 12, pp. 491-496, Dec. 1998.

- [12] A. H. Paquet, R. K. Ward, "Wavelet-based digital watermarking for image authentication," in Proc. IEEE Canadian Conf. Electrical and Computer Engineering, CCECE 2002, Winnipeg, Canada, vol. 2, pp. 879 – 884, May 2002.
- [13] F. Hartung, M. Kutter, "Multimedia watermarking techniques", in Proc. IEEE Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1069-1107, July 1999.
- [14] D. Kundur, D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," in Proc. Intern. Conf. Acoustics, Speech and Signal Processing, ICASSP'98, Seattle, WA, vol. 5, pp. 2969-2972.
- [15] D. Kundur, D. Hatzinakos, "Improved robust watermarking through attack characterization," Optics Express, vol. 3 no. 12, pp. 485-490, Dec. 1998.
- [16] J. Tian, "Wavelet based reversible watermarking for authentication," in Proc. SPIE Security and Watermarking of Multimedia Contents IV, SPIE2002, San Jose, USA, vol. 4675, pp. 679-690, Jan. 2002.
- [17] D. Kundur, D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," in Proc. IEEE Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1167-1180, July 1999.
- [18] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple image watermarking applied to health information management", *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. 722-732, Oct. 2006.
- [19] B. S. Kim, K. K. Kwon, S. G. Kwon, K. N. Park, K. I. Song, K. I. Lee, "A robust wavelet-based digital watermarking using statistical characteristic of image and human visual system," in Proc. 17th Intern. Conf. Circuits Systems Computers and Communications, ITC-CSCC2002, Phuket, Thailand, pp. 1019-1022.
- [20] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images", *Medical & Biological Engineering & Computing*, vol. 44, no. 8, pp. 619-631, Springer Berlin / Heidelberg, August 2006. Available at: <http://dx.doi.org/10.1007/s11517-006-0081-x>

ΚΕΦΑΛΑΙΟ 7

ΑΠΟΤΙΜΗΣΗ ΥΔΑΤΟΓΡΑΦΙΚΟΥ ΣΧΗΜΑΤΟΣ

7.1 ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό παρουσιάζονται οι δοκιμές που έγιναν στον υδατογραφικό αλγόριθμο προκειμένου να αξιολογηθεί η αποδοτικότητά του ως προς την ποιότητα των υδατογραφημένων εικόνων, την ανθεκτικότητα των υδατογραφημάτων και τη δυνατότητα ελέγχου ακεραιότητας των εικόνων. Η αξιολόγηση του υδατογραφικού σχήματος βασίστηκε σε εκτενείς δοκιμές που έγιναν σε πληθώρα ιατρικών εικόνων διαφόρων τύπων, εφαρμόζοντας εναλλακτικές υλοποιήσεις του βασικού υδατογραφικού αλγορίθμου που παρουσιάστηκε στο προηγούμενο κεφάλαιο. Στις επόμενες ενότητες παρουσιάζονται αναλυτικά οι δοκιμές που έγιναν και οι οποίες επέτρεψαν τη διεξοδική αποτίμηση των εναλλακτικών υλοποιήσεων του υδατογραφικού σχήματος. Τα διάφορα είδη ιατρικών εικόνων που χρησιμοποιήθηκαν στις δοκιμές περιλαμβάνουν εικόνες υπερήχων (ultrasound), αξονικής τομογραφίας (CT), μαγνητικής τομογραφίας (MRI), μαγνητικής αγγειογραφίας (MRA) και τομογραφίας εκπομπής ποζιτρονίου (PET). Στο κεφάλαιο αυτό παρουσιάζονται επίσης τα αποτελέσματα δοκιμών που έγιναν σε διαφορετικά σενάρια εφαρμογής του σχήματος, που περιλάμβαναν καθορισμό ή μη μιας Περιοχής Ενδιαφέροντος και χρήση κώδικα διόρθωσης σφαλμάτων για αύξηση της ανθεκτικότητας των υδατογραφημάτων. Τα αποτελέσματα

περιλαμβάνουν αξιολόγηση της αλλοίωσης που προκαλείται στις εικόνες – κυρίως στις διαγνωστικά σημαντικές περιοχές – λόγω της υδατογράφησης στην οποία υπόκεινται, καθώς και αποτίμηση της ανθεκτικότητας των υδατογραφημάτων και της ικανότητας του σχήματος να ελέγξει την ακεραιότητα των εικόνων.

7.2 ΔΟΚΙΜΕΣ ΤΟΥ ΥΔΑΤΟΓΡΑΦΙΚΟΥ ΣΧΗΜΑΤΟΣ

Για την αποτίμηση του υδατογραφικού σχήματος έγιναν δοκιμές σε διαφορετικά είδη ιατρικών εικόνων και εξετάστηκαν διαφορετικά σενάρια εφαρμογής του σχήματος, που περιλάμβαναν καθορισμό ή μη μιας Περιοχής Ενδιαφέροντος και χρήση κώδικα διόρθωσης σφαλμάτων για αύξηση της ανθεκτικότητας των υδατογραφημάτων δεδομένων. Για τις δοκιμές όλων των υλοποιήσεων του αλγορίθμου, τα υδατογραφήματα υπογραφής και αναφοράς ήταν τυχαίες ακολουθίες bits που δημιουργήθηκαν από γεννήτριες τυχαίων αριθμών με ομοιόμορφη κατανομή πιθανότητας. Το υδατογράφημα επικεφαλίδας και το υδατογράφημα δείκτη προέκυψαν από τον ASCII κώδικα κειμένων που περιλάμβαναν προσωπικά στοιχεία ασθενούς / στοιχεία εξέτασης και λέξεις-κλειδιά αντίστοιχα. Τα υδατογραφήματα ενσωματώνονται σε επιλεγμένους συντελεστές λεπτομερειών (detail coefficients) της αρχικής εικόνας, οι θέσεις των οποίων καθορίζονται από την τιμή ενός κλειδιού. Για κάθε επίπεδο ανάλυσης και χωρική θέση, εάν η αντίστοιχη τιμή του κλειδιού είναι 1, επιλέγεται ο συντελεστής για υδατογράφιση, ενώ εάν η τιμή είναι 0, ο συντελεστής αγνοείται. Όπως έχει εξηγηθεί στο προηγούμενο κεφάλαιο (ενότητα 6.5), στην περίπτωση κατά την οποία έχει επιλεχθεί από το χρήστη ο καθορισμός μιας Περιοχής Ενδιαφέροντος, η οποία είτε θα αποκλειστεί από τη διαδικασία υδατογράφησης είτε θα ενσωματώσει μόνο το υδατογράφημα αναφοράς, η τελική επιλογή των συντελεστών που υδατογραφούνται βασίζεται και στον Πίνακα Περιοχής Ενδιαφέροντος.

Παρακάτω παρουσιάζονται τα αποτελέσματα των διαφόρων δοκιμών που έγιναν.

7.2.1 Δοκιμές σε Εικόνες Υπερήχων

Η πρώτη σειρά δοκιμών περιλάμβανε εικόνες υπερήχων διαστάσεων 256x320 pixels. Το δείγμα περιλάμβανε 50 εικόνες, οι οποίες συλλέχθηκαν από τον ίδιο γιατρό, με τον ίδιο εξοπλισμό και τις ίδιες ρυθμίσεις συστήματος, προκειμένου να αποφευχθούν οι αποκλίσεις στις στατιστικές κατανομές των εικόνων. Όλα τα υδατογραφήματα που χρησιμοποιήθηκαν ήταν δυαδικές ακολουθίες από το σύνολο $\{0,1\}$. Στις συγκεκριμένες δοκιμές, το υδατογράφημα υπογραφής με τον αναγνωριστικό κωδικό του γιατρού αποτελούνταν από 128 bits και προέκυψε από μια γεννήτρια ψευδοτυχαίων αριθμών με ομοιόμορφη κατανομή. Το μήκος του συγκεκριμένου υδατογραφήματος είναι αρκετό για να εξασφαλίσει μοναδικότητα στο κλειδί [1], [2]. Το υδατογράφημα αναφοράς είναι μια δυαδική ακολουθία που παράγεται επίσης από μια γεννήτρια τυχαίων αριθμών με ομοιόμορφη κατανομή πιθανότητας και έχει μεταβλητό μήκος, αρκετό να καλύψει όλους τους συντελεστές κάθετων λεπτομερειών (vertical detail coefficients) που μπορούν να επιλεγθούν για υδατογράφιση βάσει κλειδιού. Τα υδατογραφήματα δείκτη και επικεφαλίδας είναι δυαδικές ακολουθίες που προκύπτουν από την ASCII κωδικοποίηση αρχείων κειμένου που περιέχουν αντίστοιχα λέξεις-κλειδιά και στοιχεία για τον ασθενή ή / και την εξέταση. Στις συγκεκριμένες δοκιμές τα κείμενα που επιλέχθηκαν για προσομοίωση των λέξεων-κλειδιών και των στοιχείων του ασθενή περιείχαν αντίστοιχα 6 λέξεις με συνολικά 52 χαρακτήρες και 23 λέξεις με 208 χαρακτήρες στο σύνολο. Τα δυαδικά υδατογραφήματα που προέκυψαν από αυτά τα κείμενα αποτελούνταν από 364 και 1456 bits αντίστοιχα, λόγω της ανάθεσης 7 bits ανά χαρακτήρα κατά την κωδικοποίηση ASCII. Τα μήκη των υδατογραφημάτων αυτών επιλέχθηκαν αυθαίρετα για τις ανάγκες της προσομοίωσης και προφανώς η χρήση άλλων κειμένων ως λέξεων-κλειδιών και στοιχείων ασθενή για την εξαγωγή των υδατογραφημάτων δείκτη και επικεφαλίδας, θα οδηγούσε σε διαφορετικά μήκη.

Προκειμένου να βελτιωθεί η ανθεκτικότητα των ενσωματωμένων δεδομένων (υπογραφή, δείκτης, επικεφαλίδα), εφαρμόστηκε κωδικοποίηση διόρθωσης σφαλμάτων (error correction coding). Συγκεκριμένα, εφαρμόστηκαν στα τρία υδατογραφήματα σχήματα κωδικοποίησης BCH [3]. Κάθε υδατογράφημα χωρίστηκε

σε τμήματα ίδιου μήκους, τα οποία ενσωματώθηκαν στη συνέχεια σε κατάλληλα επιλεγμένους κώδικες BCH. Ο Πίνακας 4 παρουσιάζει τα σχήματα κωδικοποίησης BCH που χρησιμοποιήθηκαν για τα παραπάνω σύνολα δεδομένων, καθώς και το πλήθος των εφαρμογών τους που απαιτήθηκαν προκειμένου να καλύψουν όλα τα bits των υδατογραφήματων. Γενικά, ένας δυαδικός κώδικας BCH με παραμέτρους (n , k , l) αντιπροσωπεύει μια κωδική λέξη (codeword) μήκους n , που περιλαμβάνει k bits του υδατογραφήματος και μπορεί να διορθώσει l εσφαλμένα bits. Για παράδειγμα, το BCH(255,91,25) αποτελεί μια κωδική λέξη μήκους 255 bits, που περιλαμβάνει 91 bits του προς ενσωμάτωση υδατογραφήματος και έχει τη δυνατότητα διόρθωσης έως και 25 εσφαλμένων bits. Ενδεικτικά αναφέρεται ότι η κωδικοποίηση του υδατογραφήματος επικεφαλίδας που αποτελείται από 1456 bits με χρήση του συγκεκριμένου κώδικα BCH, απαιτεί το διαχωρισμό του υδατογραφήματος σε 16 ίσα τμήματα και την εφαρμογή σε καθένα από αυτά της κωδικοποίησης BCH(255,91,25), οδηγώντας σε ένα σύνολο 4080 bits κωδικής λέξης που πρέπει να ενσωματωθούν.

Είδος Υδατογραφήματος	Αριθμός Bits	Σχήμα BCH	Επαναλήψεις	Συνολικός Αριθμός Ενσωματωμένων Bits
Υπογραφή	128	(31,16,3)	8	248
Δείκτης	364	(255,91,25)	4	1.020
Επικεφαλίδα	1.456	(255,91,25)	16	4.080

Πίνακας 4: Σχήματα κωδικοποίησης BCH ανά υδατογράφημα

Η ενσωμάτωση των τεσσάρων υδατογραφημάτων στις εικόνες υπερήχων έγινε με βάση τον υδατογραφικό αλγόριθμο που περιγράφηκε αναλυτικά στο προηγούμενο κεφάλαιο. Στις εικόνες ορίστηκε Περιοχή Ενδιαφέροντος, η οποία χρησιμοποιήθηκε μόνο για την ενσωμάτωση του υδατογραφήματος αναφοράς – που στοχεύει στον έλεγχο ακεραιότητάς της – και εφαρμόστηκε διακριτός μετασχηματισμός κυματιδίων τεσσάρων επιπέδων. Στο Σχήμα 12 του Κεφαλαίου 6 παρουσιάζονται οι υποζώνες που προέκυψαν από το διακριτό μετασχηματισμό κυματιδίων τεσσάρων επιπέδων σε μια εικόνα υπερήχων, καθώς και η αντιστοιχία ανάμεσα στους Πίνακες Περιοχής Ενδιαφέροντος των υποζωνών.

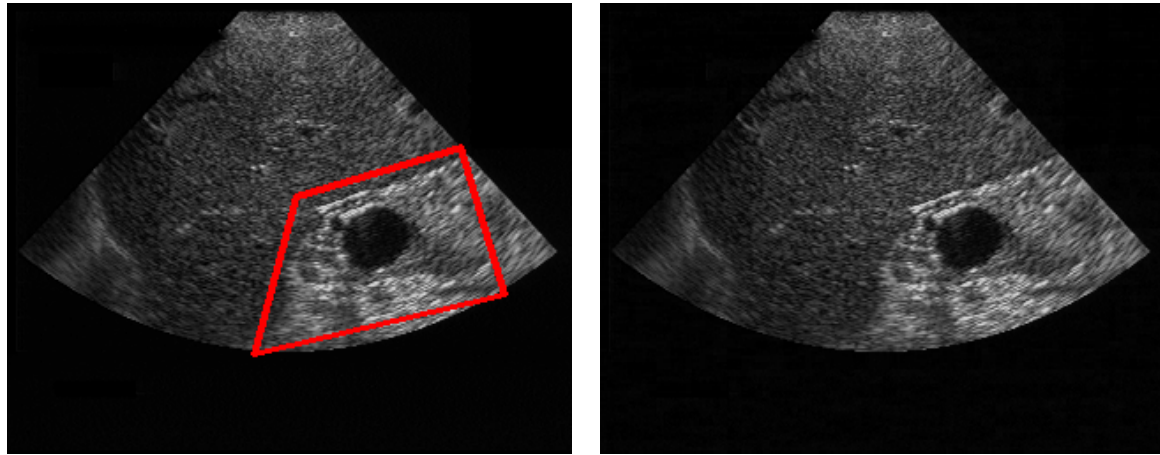
Από τις υποζώνες ανάλυσης που προέκυψαν από το μετασχηματισμό, επιλέχθηκαν για υδατογράφιση εκείνες που πληρούν τις απαιτήσεις ανθεκτικότητας, χωρητικότητας και διαφάνειας των προς ενσωμάτωση υδατογραφημάτων. Στον Πίνακα 5 παρουσιάζεται η κατανομή της ενέργειας μιας εικόνας υπερήχων ανά επίπεδο ανάλυσης και υποζώνης και φανερώνεται η συγκέντρωση μεγαλύτερου ποσοστού ενέργειας στις υποζώνες οριζόντιων λεπτομερειών σε σχέση με τις άλλες, δικαιολογώντας την επιλογή τους για ενσωμάτωση των υδατογραφημάτων που φέρουν την πρόσθετη πληροφορία και απαιτούν μεγαλύτερη ανθεκτικότητα. Σύμφωνα με την ανάλυση των χαρακτηριστικών των διαφόρων υποζωνών και των προς ενσωμάτωση υδατογραφημάτων, που παρουσιάζεται στην ενότητα 6.5, τα υδατογραφήματα υπογραφής, δείκτη και επικεφαλίδας εισάγονται αντίστοιχα στις υποζώνες οριζόντιων λεπτομερειών του τέταρτου, τρίτου και δεύτερου επιπέδου ανάλυσης (Κεφ. 6, Πίνακας 3).

Υποζώνη	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
Προσέγγιση Εικόνας	-	-	-	461,15
Οριζόντιες Λεπτομέρειες	8,50	13,27	25,85	62,70
Κάθετες Λεπτομέρειες	5,15	10,15	18,92	43,42
Διαγώνιες Λεπτομέρειες	4,91	9,30	15,01	26,27

Πίνακας 5: Ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών Διακριτού Μετασχηματισμού Κυματιδίων 4 επιπέδων εικόνας υπερήχων

Λόγω των αυστηρών απαιτήσεων όσον αφορά τις επιτρεπτές μεταβολές στις ιατρικές εικόνες, έγινε αποτίμηση της ποιότητας τόσο από άποψη σήματος, όσο και από άποψη οπτικού αποτελέσματος (perceptual quality). Η ποιοτική αξιολόγηση των εικόνων έγινε από γιατρό, ο οποίος κατέληξε στο συμπέρασμα ότι δεν υπάρχει αντιληπτή διαφοροποίηση ανάμεσα στις αρχικές και τις αντίστοιχες υδατογραφημένες εικόνες. Οι εικόνες (α) και (β) του Σχήματος 13 παρουσιάζουν μια

εικόνα υπερήχων όπου έχει καθοριστεί μια Περιοχή Ενδιαφέροντος (ROI) και την προκύπτουσα υδατογραφημένη εικόνα αντίστοιχα.



(α) (β)
Σχήμα 13: (α) Αρχική εικόνα υπερήχων με καθορισμένη Περιοχή Ενδιαφέροντος. (β) Προκύπτουσα υδατογραφημένη εικόνα.

Η ποσοτική αποτίμηση της ποιότητας των υδατογραφημένων εικόνων πραγματοποιήθηκε χρησιμοποιώντας το σηματοθορυβικό λόγο (Peak Signal to Noise Ratio – PSNR) και το σταθμισμένο σηματοθορυβικό λόγο (wPSNR – weighted PSNR). Ο σηματοθορυβικός λόγος PSNR, αν και δε συνδέεται στενά με την οπτικά αντιλαμβανόμενη ποιότητα, αποτελεί ένα αποδοτικό μέτρο της αλλοίωσης εικόνων όσον αφορά τις αριθμητικές τιμές, οι οποίες μεταφέρουν σημαντική πληροφορία στις ιατρικές εφαρμογές, όπως για παράδειγμα στην περίπτωση συστημάτων υποστήριξης διάγνωσης [4]–[6]. Ο σηματοθορυβικός λόγος μετρείται σε decibels και ορίζεται ως εξής:

$$PSNR(I, \hat{I}) = 10 \log_{10} \left[\frac{\left(\max_{\forall(m,n)} I(m,n) \right)^2}{\frac{1}{N_I} \sum_{\forall(m,n)} (\hat{I}(m,n) - I(m,n))^2} \right] \quad (7.1)$$

όπου I και $\hat{I}$ είναι η αρχική και η υδατογραφημένη εικόνα αντίστοιχα, N_I είναι το πλήθος των pixels στην εικόνα (οι δύο εικόνες έχουν τον ίδιο αριθμό pixels) και

$\max_{\forall(m,n)} I(m,n)$ είναι η μέγιστη τιμή έντασης στην αρχική εικόνα. Ο παρονομαστής του

PSNR είναι το μέσο τετραγωνικό σφάλμα.

Ο σταθμισμένος σηματοθορυβικός λόγος (weighted PSNR – wPSNR) αποτελεί ένα μέτρο ποιότητας που αναθέτει διαφορετικά βάρη σε τμήματα της εικόνας που γίνονται διαφορετικά αντιληπτά στο μάτι, βάσει της Συνάρτησης Ορατότητας Θορύβου (Noise Visibility Function – NVF) [7], [8]. Η συνάρτηση αυτή αντανακλά τις ιδιότητες κάλυψης (masking properties) του ανθρώπινου οπτικού συστήματος χρησιμοποιώντας ένα μοντέλο Gauss για τον υπολογισμό της υφής στις διάφορες περιοχές της εικόνας. Σε επίπεδες περιοχές, η τιμή της Συνάρτησης Ορατότητας Θορύβου προσεγγίζει την τιμή 1, ενώ σε περιοχές με ακμές ή έντονης υφής (edge or textured regions), προσεγγίζει το μηδέν. Το wPSNR, που επίσης μετρείται σε decibels, ορίζεται ως εξής:

$$wPSNR(I, \hat{I}) = 10 \log_{10} \left[\frac{\left(\max_{\forall(m,n)} I(m,n) \right)^2}{\frac{1}{N_I} \sum_{\forall(m,n)} [(\hat{I}(m,n) - I(m,n)) \cdot NVF(m,n)]^2} \right] \quad (7.2)$$

όπου $NVF(m,n)$ είναι η τιμή της Συνάρτησης Ορατότητας Θορύβου που αντιστοιχεί στο pixel (m,n) και οι άλλες μεταβλητές ορίζονται όπως στην Εξίσωση (7.1).

Οι δοκιμές κατέληξαν σε μέση τιμή PSNR 45.70 dB $\pm$ 0.10 dB και σε μέση τιμή wPSNR 47.41 dB $\pm$ 0.21 dB. Παρουσιάζει ενδιαφέρον η σύγκριση ανάμεσα στην αλλοίωση που προκαλείται από την υδατογράφηση και την αλλοίωση που προκύπτει από τη συμπίεση μιας εικόνας [9], [10]. Οι Πίνακες 6 και 7 παρουσιάζουν συγκριτικές αποτιμήσεις των αλλοιώσεων που προκαλούνται από την ενσωμάτωση των υδατογραφημάτων και τη συμπίεση JPEG με διάφορους συντελεστές ποιότητας, ως προς τα μέτρα ποιότητας PSNR και wPSNR αντίστοιχα. Όπως προκύπτει από τους πίνακες αυτούς, η υδατογραφική μέθοδος προκαλεί μικρότερη αλλοίωση από τη συμπίεση JPEG με συντελεστή ποιότητας έως και 95. Η ικανοποιητική οπτικά αντιλαμβανόμενη ποιότητα των υδατογραφημένων εικόνων, σε συνδυασμό με τις υψηλές τιμές PSNR και wPSNR, καταδεικνύει τη διαφάνεια του σχήματος σε εικόνες υπερέχων.

Είδος Επεξεργασίας Εικόνας	PSNR (dB)
Υδατογράφιση	$45,70 \pm 0,10$
JPEG 95	$44,70 \pm 0,50$
JPEG 90	$39,99 \pm 0,78$
JPEG 85	$37,37 \pm 0,92$
JPEG 80	$35,65 \pm 1,02$
JPEG 75	$34,38 \pm 1,10$

Πίνακας 6: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων υπερήχων ως προς το PSNR

Είδος Επεξεργασίας Εικόνας	wPSNR (dB)
Υδατογράφιση	$47,41 \pm 0,21$
JPEG 95	$47,09 \pm 0,37$
JPEG 90	$43,54 \pm 0,60$
JPEG 85	$41,39 \pm 0,73$
JPEG 80	$40,02 \pm 0,80$
JPEG 75	$39,06 \pm 0,83$

Πίνακας 7: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων υπερήχων ως προς το wPSNR

Στα πλαίσια των δοκιμών, εξετάστηκε και το σενάριο κατά το οποίο δεν ορίζεται Περιοχή Ενδιαφέροντος και η ενσωμάτωση των πολλαπλών υδατογραφημάτων γίνεται σε όλη την εικόνα αδιακρίτως. Χρησιμοποιώντας τα ίδια υδατογραφήματα υπογραφής, δείκτη και επικεφαλίδας όπως και στο σενάριο με ορισμό Περιοχής Ενδιαφέροντος, οι τιμές PSNR και wPSNR βρέθηκαν μέσα στα όρια της τυπικής απόκλισης των παραπάνω αποτελεσμάτων. Αυτό ήταν αναμενόμενο, καθώς η συνολική ποσότητα ενσωματωμένης πληροφορίας ήταν η ίδια στις δύο περιπτώσεις. Η μόνη διαφορά έγκειται στην κατανομή των υδατογραφημάτων που φέρουν τα δεδομένα (υπογραφή, δείκτης, επικεφαλίδα) στην εικόνα. Στην περίπτωση μη καθορισμού Περιοχής Ενδιαφέροντος, υδατογραφούνται κάποιοι συντελεστές που ανήκουν στο διαγνωστικά σημαντικό κομμάτι της εικόνας· παρόλα

αυτά, δε γίνεται αντιληπτή καμία διαφορά στην ποιότητα της εικόνας που θα μπορούσε να προκαλέσει αλλαγή στο διαγνωστικό περιεχόμενό της, σύμφωνα και με το γιαντρό που έκανε την αξιολόγηση.

Ο Πίνακας 8 παρουσιάζει την επίδραση που έχει η συμπίεση JPEG με διάφορους συντελεστές ποιότητας στις υδατογραφημένες εικόνες. Για την αποτίμηση του βαθμού αλλοίωσης επιλέχθηκε η Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance) ως κριτήριο ομοιότητας:

$$NHD(w, \tilde{w}) = \frac{1}{N_w} \sum_{i=1}^{N_w} w(i) \oplus \tilde{w}(i) \quad (7.3)$$

όπου W και $\tilde{W}$ είναι το αρχικό και το εξαγχθέν υδατογράφημα αναφοράς αντίστοιχα, N_w είναι το μήκος του υδατογραφήματος και $\oplus$ είναι ο τελεστής exclusive-OR. Η απόσταση Hamming κυμαίνεται στο διάστημα (0,1) και η απόφαση ως προς την ακεραιότητα των δεδομένων εξαρτάται από την εκάστοτε εφαρμογή. Προφανώς, σε ιατρικές εφαρμογές δεν πρέπει να υπερβαίνει μια μικρή τιμή, που θα αντιστοιχούσε σε περιορισμένες και αμελητέες αλλαγές στην εικόνα. Τυχόν αλλαγές σε συγκεκριμένες χωρικές θέσεις ή / και συχνότητες μπορούν να αποτιμηθούν μέσω της εξαγωγής του υδατογραφήματος αναφοράς μόνο από τους αντίστοιχους υδατογραφημένους συντελεστές [11].

Συντελεστής Ποιότητας Συμπίεσης JPEG Υδατογρ/νων Εικόνων	Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance)			
	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
95	0,44 ± 0,01	0,19 ± 0,01	0,09 ± 0,02	0,05 ± 0,02
90	0,48 ± 0,01	0,29 ± 0,02	0,14 ± 0,02	0,07 ± 0,03
85	0,49 ± 0,01	0,37 ± 0,02	0,16 ± 0,02	0,10 ± 0,03
80	0,50 ± 0,01	0,42 ± 0,02	0,17 ± 0,03	0,14 ± 0,04
75	0,50 ± 0,01	0,46 ± 0,02	0,24 ± 0,02	0,16 ± 0,04

Πίνακας 8: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες υπερήχων)

Όπως είναι αναμενόμενο, η συμπίεση JPEG με χαμηλότερη ποιότητα οδηγεί σε υψηλότερες τιμές Κανονικοποιημένης Απόστασης Hamming. Ο πίνακας δείχνει επίσης ότι η Κανονικοποιημένη Απόσταση Hamming μειώνεται όσο αυξάνει το επίπεδο ανάλυσης, γεγονός που φανερώνει την ενίσχυση της ανθεκτικότητας στα υψηλά επίπεδα ανάλυσης.

Το υδατογραφικό σχήμα δοκιμάστηκε επίσης ως προς την ανθεκτικότητα των υδατογραφημάτων που φέρουν τα δεδομένα (υπογραφή, δείκτης, επικεφαλίδα) στη συμπίεση JPEG. Στον Πίνακα 9 παρουσιάζεται η ανθεκτικότητα των υδατογραφημάτων αυτών, τα οποία εξήχθηκαν από μια εικόνα υπερήχων που υπέστη συμπίεση JPEG με διαφορετικούς συντελεστές ποιότητας.

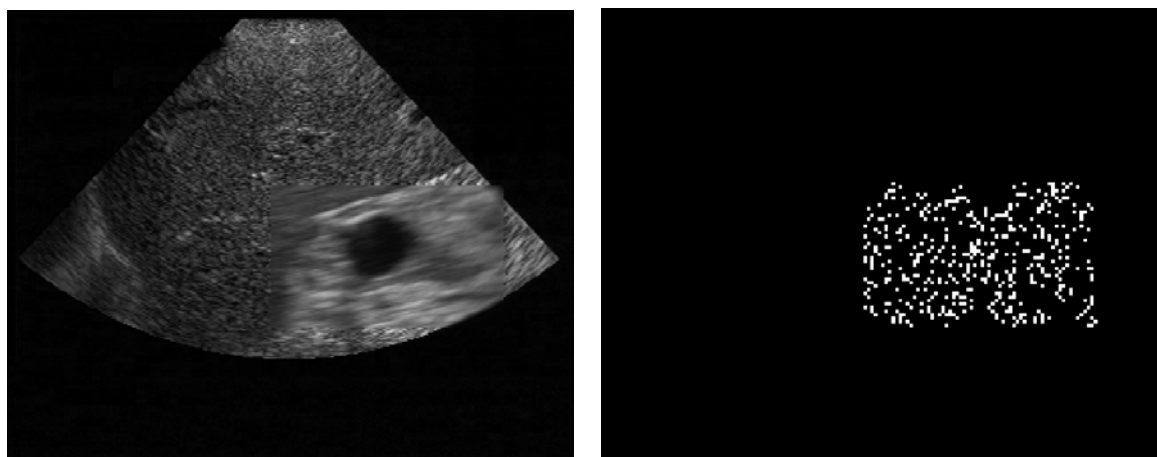
Τύπος Υδατογραφήματος	Υπογραφή	Δείκτης	Επικεφαλίδα
Επίπεδο Ενσωμάτωσης	4	3	2
95	0	0	14,90
Συντελεστής	0	5,22	26,10
Ποιότητας	0	15,93	33,17
JPEG	3,13	16,76	38,05
75	4,69	17,86	39,08

Πίνακας 9: Ποσοστό εσφαλμένων bits σε υδατογραφήματα εξαχθέντα από εικόνες υπερήχων (%)

Όπως φαίνεται και στον πίνακα, το υδατογράφημα υπογραφής που φέρει τον αναγνωριστικό κωδικό του γιατρού εξήχθη ανέπαφο μετά από συμπίεση JPEG με συντελεστή ποιότητας ίσο τουλάχιστον με 85. Όπως ήταν αναμενόμενο, η ανθεκτικότητα των υδατογραφημάτων δείκτη και επικεφαλίδας στη συμπίεση JPEG ήταν λιγότερη, λόγω του γεγονότος ότι η ανθεκτικότητα μειώνεται όσο μειώνεται το επίπεδο ανάλυσης. Πρέπει να αναφερθεί ότι, δεδομένης της χωρητικότητας που παρέχουν οι συγκεκριμένες διαστάσεις των εικόνων υπερήχων που δοκιμάστηκαν (256x320 pixels), το φορτίο (payload) που αντιστοιχεί στα σύνολα δεδομένων που χρησιμοποιήθηκαν για τις δοκιμές αυτές, μειώνει το ποσοστό διόρθωσης σφαλμάτων. Όσον αφορά τις ασυμπίεστες ή ελαφρώς συμπιεσμένες εικόνες, τα αποτελέσματα ως προς τη διόρθωση σφαλμάτων είναι ικανοποιητικά. Στην περίπτωση μεγαλύτερης συμπίεσης όμως, προκειμένου να επιτευχθεί εξαγωγή

σωστών υδατογραφημάτων, χρειάζεται μείωση του μήκους των υδατογραφημάτων και αύξηση του πλήθους των περιττών bits (redundant bits) που θα χρησιμοποιηθούν για πιο αποδοτική κωδικοποίηση BCH. Από την άλλη πλευρά, εικόνες μεγαλύτερων διαστάσεων, όπως για παράδειγμα εικόνες των 512×512 pixels, που αποτελεί ένα τυπικό μέγεθος για πολλά είδη ιατρικών εικόνων, προσφέρουν μεγαλύτερη ευελιξία στην αντιστάθμιση (trade-off) μεταξύ της ενσωμάτωσης εκτενών ακολουθιών υδατογραφημάτων και επαρκούς ποσότητας περιττών bits που προσφέρουν τη δυνατότητα βελτιωμένου ποσοστού διόρθωσης σφαλμάτων. Αυτό θα καταδειχθεί στις επόμενες ενότητες, όπου περιγράφονται τα αποτελέσματα των δοκιμών σε εικόνες μεγαλύτερων διαστάσεων.

Με σκοπό να αξιολογηθεί η ικανότητα του υδατογραφήματος αναφοράς να εντοπίσει κάποιο αλλοιωμένο τμήμα της εικόνας, εφαρμόστηκε θόλωση (blurring) σε μια εικόνα υπερήχων. Το Σχήμα 14(α) δείχνει την αρχική εικόνα της οποίας ένα τμήμα έχει υποστεί θόλωση και το Σχήμα 14(β) παρουσιάζει την ανίχνευση της μεταβολής, όπως αυτή προκύπτει από τη διαφορά ανάμεσα στο αρχικό υδατογράφημα αναφοράς και το αντίστοιχο εξαχθέν υδατογράφημα από το πρώτο επίπεδο ανάλυσης.



Σχήμα 14: (α) Εικόνα υπερήχων με θολωμένη περιοχή. (β) Ανίχνευση αλλοίωσης μέσω της εικόνας διαφορών του υδατογραφήματος αναφοράς 1ου επιπέδου ανάλυσης

Τα παραπάνω πειραματικά αποτελέσματα φανερώνουν την αποδοτικότητα του υδατογραφικού σχήματος ως προς την ανθεκτικότητα, τη διαφάνεια και την

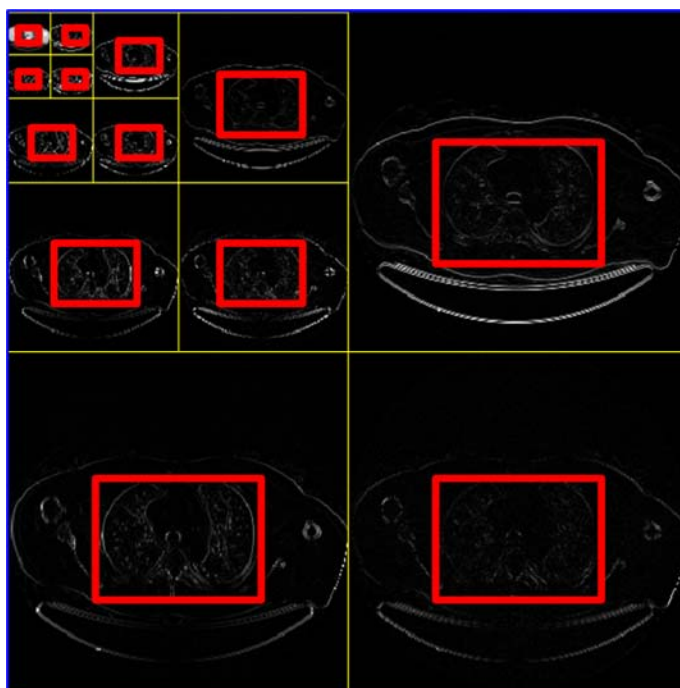
ικανότητα ελέγχου ακεραιότητας. Όπως προαναφέρθηκε, ακολουθούν στις αμέσως επόμενες ενότητες οι δοκιμές που έγιναν σε άλλα είδη ιατρικών εικόνων, των οποίων μάλιστα οι διαστάσεις επέτρεψαν την αύξηση της ανθεκτικότητας των υδατογραφημάτων δεδομένων μέσω του συνδυασμού κωδικοποίησης BCH και επαναληπτικής υδατογράφησης (repetitive embedding).

7.2.2 Δοκιμές σε Εικόνες Αξονικής Τομογραφίας (CT)

Η επόμενη σειρά δοκιμών του υδατογραφικού σχήματος που αναπτύχθηκε περιλάμβανε τη χρήση εικόνων αξονικής τομογραφίας (CT). Το δείγμα αποτελούνταν από 20 εικόνες CT, διαστάσεων 512x512 pixels. Όλα τα υδατογραφήματα που ενσωματώθηκαν ήταν δυαδικές ακολουθίες από το σύνολο {0,1} και προέκυψαν με τις διαδικασίες που περιγράφηκαν στην εισαγωγή της παρούσας ενότητας. Το μήκος του υδατογραφήματος υπογραφής επιλέχθηκε να είναι 128 bits, που αρκεί για να εξασφαλίσει μοναδικότητα στο κλειδί. Στις συγκεκριμένες δοκιμές τα κείμενα που επιλέχθηκαν για προσομοίωση των λέξεων-κλειδιών και των στοιχείων του ασθενή ήταν τα ίδια με αυτά που χρησιμοποιήθηκαν και στην περίπτωση των εικόνων υπερήχων και περιείχαν αντίστοιχα 6 λέξεις με συνολικά 52 χαρακτήρες και 23 λέξεις με 208 χαρακτήρες στο σύνολο. Τα δυαδικά υδατογραφήματα που προέκυψαν από αυτά τα κείμενα αποτελούνταν από 364 και 1456 bits αντίστοιχα, λόγω της ανάθεσης 7 bits ανά χαρακτήρα κατά την κωδικοποίηση ASCII.

Προκειμένου να βελτιωθεί η ανθεκτικότητα των ενσωματωμένων δεδομένων (υπογραφή, δείκτης, επικεφαλίδα), εφαρμόστηκε ένας τύπος υβριδικής κωδικοποίησης (hybrid coding) που περιλαμβάνει επαναληπτική ενσωμάτωση υδατογραφημάτων κωδικοποιημένων κατά BCH [12], [13]. Σημειώνεται ότι οι διαστάσεις των εικόνων CT (512x512 pixels) επέτρεψαν την επαναληπτική ενσωμάτωση των υδατογραφημάτων που επιλέχθηκαν για την προσομοίωση. Κάθε υδατογράφημα χωρίστηκε σε τμήματα ίδιου μήκους, τα οποία ενσωματώθηκαν στη συνέχεια σε κατάλληλα επιλεγμένους κώδικες BCH. Στη συνέχεια τα κωδικοποιημένα κατά BCH υδατογραφήματα ενσωματώθηκαν στην εικόνα τρεις

φορές το καθένα. Αυτή η υβριδική κωδικοποίηση παρέχει τη δυνατότητα διόρθωσης κάποιων σφαλμάτων με χρήση «αποκωδικοποίησης επαναληψιμότητας» (repetition decoding), πριν από την αποκωδικοποίηση BCH, αυξάνοντας την ανθεκτικότητα των υδατογραφημάτων [3]. Με τον όρο «αποκωδικοποίηση επαναληψιμότητας» εννοείται ουσιαστικά μια διαδικασία πλειοψηφικής επιλογής (majority vote), που περιλαμβάνει την εξαγωγή του υδατογραφήματος βάσει των πλειοψηφούντων τιμών των bits που εξάγονται από τα τρία ενσωματωμένα αντίγραφα του κάθε υδατογραφήματος. Τα σχήματα κωδικοποίησης BCH που χρησιμοποιήθηκαν για τα παραπάνω σύνολα δεδομένων, καθώς και το πλήθος των εφαρμογών τους που απαιτήθηκαν προκειμένου να καλύψουν όλα τα bits των υδατογραφημάτων, δίνονται και σε αυτήν την περίπτωση από τον Πίνακα 4.



Σχήμα 15: Αντιστοιχία των Πινάκων Περιοχής Ενδιαφέροντος ανά υποζώνη και επίπεδο ανάλυσης εικόνας CT

Η ενσωμάτωση των τεσσάρων υδατογραφημάτων στις εικόνες αξονικής τομογραφίας (CT) έγινε με εφαρμογή του υδατογραφικού αλγορίθμου που περιγράφηκε αναλυτικά στο προηγούμενο κεφάλαιο. Στις εικόνες ορίστηκε Περιοχή Ενδιαφέροντος, όπου και ενσωματώθηκε μόνο το υδατογράφημα

αναφοράς, και εφαρμόστηκε διακριτός μετασχηματισμός κυματιδίων τεσσάρων επιπέδων. Το Σχήμα 15 παρουσιάζει τις υποζώνες που προέκυψαν από το διακριτό μετασχηματισμό κυματιδίων τεσσάρων επιπέδων σε μια εικόνα αξονικής τομογραφίας, καθώς και την αντιστοιχία ανάμεσα στους Πίνακες Περιοχής Ενδιαφέροντος των υποζωνών.

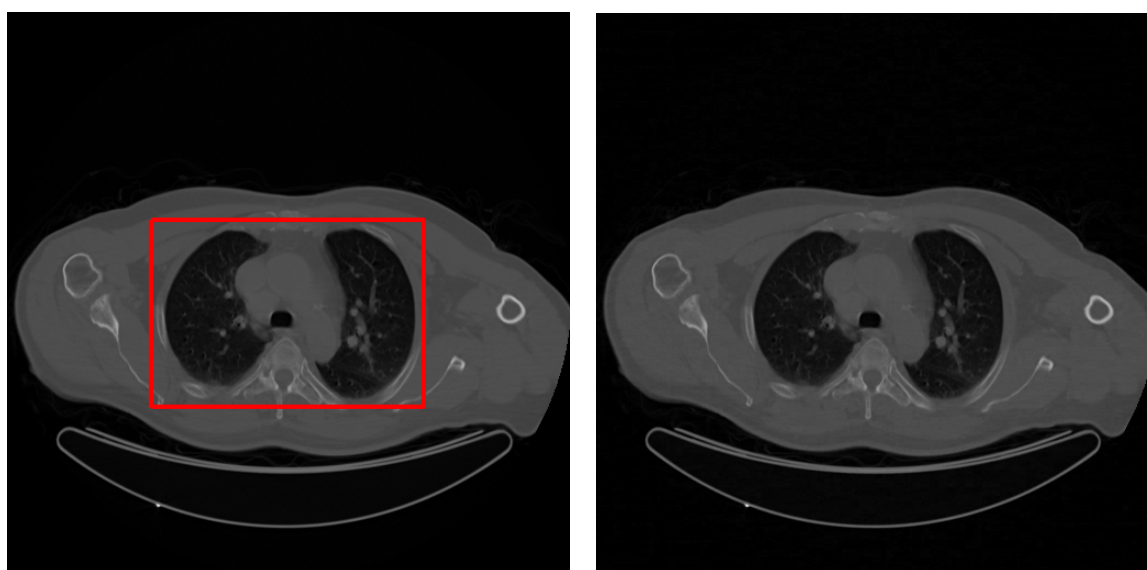
Από τις υποζώνες ανάλυσης που προέκυψαν από το μετασχηματισμό, επιλέχθηκαν για υδατογράφηση εκείνες που πληρούν τις απαιτήσεις ανθεκτικότητας, χωρητικότητας και διαφάνειας των προς ενσωμάτωση υδατογραφημάτων. Στην ενότητα 6.5 (Πίνακας 2) παρουσιάζεται η κατανομή της ενέργειας μιας εικόνας αξονικής τομογραφίας ανά επίπεδο ανάλυσης και υποζώνης και φανερώνεται η συγκέντρωση μεγαλύτερου ποσοστού ενέργειας στις υποζώνες οριζόντιων λεπτομερειών σε σχέση με τις άλλες, δικαιολογώντας την επιλογή τους για ενσωμάτωση των υδατογραφημάτων που φέρουν την πρόσθετη πληροφορία και απαιτούν μεγαλύτερη ανθεκτικότητα. Στην ίδια ενότητα περιγράφονται αναλυτικά τα χαρακτηριστικά των διαφόρων υποζωνών και οι απαιτήσεις που πρέπει να ικανοποιούνται από κάθε υδατογράφημα, καταλήγοντας τελικά βάσει αυτών στην επιλογή των υποζωνών οριζόντιων λεπτομερειών του τέταρτου, τρίτου και δεύτερου επιπέδου ανάλυσης για την ενσωμάτωση των υδατογραφημάτων υπογραφής, δείκτη και επικεφαλίδας αντίστοιχα. Το υδατογράφημα αναφοράς εισάγεται στις υποζώνες κάθετων λεπτομερειών όλων των επιπέδων ανάλυσης, όπως έχει προαναφερθεί. Ο Πίνακας 10 συνοψίζει την κατανομή των πολλαπλών υδατογραφημάτων στις διάφορες υποζώνες, όπως αυτή προέκυψε με βάση τις απαιτήσεις του κάθε υδατογραφήματος ως προς την ανθεκτικότητα και τη χωρητικότητα. Σημειώνεται ότι η χωρητικότητα που εμφανίζεται στον Πίνακα 10 αντιπροσωπεύει το πλήθος των συντελεστών των επιλεγμένων υποζωνών και άρα το μέγιστο αριθμό bits με το οποίο μπορούν αυτές να υδατογραφηθούν στην περίπτωση εικόνων με διαστάσεις 512x512 pixels, όταν δεν έχει οριστεί Περιοχή Ενδιαφέροντος. Προφανώς όταν υπάρχει καθορισμένη Περιοχή Ενδιαφέροντος, περιορίζεται η διαθέσιμη χωρητικότητα των υποζωνών οριζόντιων λεπτομερειών που υδατογραφούνται με την πρόσθετη πληροφορία (υπογραφή, λέξεις-κλειδιά, στοιχεία ασθενή): σε αυτήν την περίπτωση η διαθέσιμη χωρητικότητά τους καθορίζεται τελικά από την έκταση

της Περιοχής Ενδιαφέροντος, δεδομένου ότι οι συντελεστές που ανήκουν σε αυτήν εξαιρούνται από τη διαδικασία υδατογράφησης.

Υποζώνη	Χωρητικότητα (υδατογραφήσιμοι συντελεστές)	Υδατογράφημα	
		Τύπος	Απαίτηση Ανθεκτικότητας
LH1	65.536	Αναφοράς	Χαμηλή
HL2	16.384	Επικεφαλίδα	Υψηλή
LH2	16.384	Αναφοράς	Χαμηλή
HL3	4.096	Δείκτης	Υψηλή
LH3	4.096	Αναφοράς	Χαμηλή
HL4	1.024	Υπογραφή	Πολύ υψηλή
LH4	1.024	Αναφοράς	Χαμηλή

Πίνακας 10: Κατανομή πολλαπλών υδατογραφημάτων στις υποζώνες βάσει απαιτήσεων ανθεκτικότητας και χωρητικότητας

Λόγω των αυστηρών απαιτήσεων όσον αφορά τις τροποποιήσεις στις ιατρικές εικόνες, και σε αυτή τη σειρά δοκιμών αποτιμήθηκε η απόδοση του υδατογραφικού σχήματος ως προς τη διαφάνεια των ενσωματούμενων υδατογραφημάτων, τόσο από πλευράς αισθητικού αποτελέσματος (perceptual quality), όσο και με βάση κάποιο αντικειμενικό κριτήριο ποιότητας.



(α)

(β)

Σχήμα 16: (α) Αρχική εικόνα CT με καθορισμένη Περιοχή Ενδιαφέροντος. (β) Προκύπτουσα υδατογραφημένη εικόνα

Την ποιότητα των υδατογραφημένων εικόνων αξιολόγησε γιατρός, ο οποίος κατέληξε στο συμπέρασμα ότι δεν υπάρχει οπτική αλλοίωση που να υποβαθμίζει τη διαγνωστική αξία των εικόνων· επισημαίνεται ότι δόθηκε ιδιαίτερη βαρύτητα στην αξιολόγηση των Περιοχών Ενδιαφέροντος που φέρουν τη διαγνωστική πληροφορία. Τα Σχήματα 16(α) και 16(β) παρουσιάζουν μια εικόνα αξονικής τομογραφίας όπου διακρίνεται η Περιοχή Ενδιαφέροντος και την υδατογραφημένη εικόνα που προέκυψε από το υδατογραφικό σχήμα αντίστοιχα. Από τα σχήματα αυτά είναι φανερή η διατήρηση της ποιότητας της εικόνας και άρα του διαγνωστικού της περιεχομένου.

Το αντικειμενικό κριτήριο που χρησιμοποιήθηκε για την αποτίμηση της ποιότητας ήταν και πάλι ο σηματοθορυβικός λόγος PSNR, που ορίζεται όπως στην Εξίσωση 7.1. Φυσικά ισχύουν οι περιορισμοί ως προς τη δυνατότητα του συγκεκριμένου κριτηρίου να συνδυάσει τυχόν αποκλίσεις σε αριθμητικά δεδομένα με το οπτικά αντιλαμβανόμενο αποτέλεσμα. Οι δοκιμές κατέληξαν στο ακόλουθο αποτέλεσμα:

$$PSNR = 46.47 \text{ dB} \pm 0.06 \text{ dB}$$

Η υψηλή τιμή του PSNR σε συνδυασμό με την ικανοποιητική οπτικά αντιλαμβανόμενη ποιότητα των υδατογραφημένων εικόνων, φανερώνουν τη διαφάνεια των υδατογραφημάτων και στην περίπτωση ενσωμάτωσής τους σε εικόνες αξονικής τομογραφίας.

Η ανθεκτικότητα των υδατογραφημάτων που φέρουν την πρόσθετη πληροφορία (υπογραφή, δείκτες, στοιχεία ασθενή) αξιολογήθηκε υποβάλλοντας τις εικόνες σε συμπίεση JPEG με διάφορους συντελεστές ποιότητας. Τα υδατογραφήματα που εξάχθηκαν συγκρίθηκαν στη συνέχεια με τα αντίστοιχα αρχικά υδατογραφήματα και υπολογίστηκε το ποσοστό εσφαλμένων bits για καθένα από αυτά. Ο Πίνακας 11 παρουσιάζει την απόδοση του σχήματος σε εικόνες CT ως προς την ανθεκτικότητα των υδατογραφημάτων στη συμπίεση JPEG με διάφορους συντελεστές ποιότητας.

Τύπος Υδατογραφήματος	Υπογραφή	Δείκτης	Επικεφαλίδα
Επίπεδο Ενσωμάτωσης	4	3	2
95	0	0	2,0
Συντελεστής 90	0	0	13,5
Ποιότητας 85	0	0	20,4
JPEG 80	0	0	30,9
75	0	5,5	37,8

Πίνακας 11: Ποσοστό εσφαλμένων bits σε υδατογραφήματα εξαχθέντα από εικόνες CT (%)

Όπως φαίνεται και από τον παραπάνω πίνακα, τα αποτελέσματα από άποψη ανθεκτικότητας των υδατογραφημάτων είναι ικανοποιητικά. Ενδεικτικά αναφέρεται ότι το υδατογράφημα υπογραφής εξήχθη ακέραιο, ακόμη και όταν η υδατογραφημένη εικόνα υπέστη συμπίεση JPEG75. Το υδατογράφημα δείκτη εξήχθη αναλλοίωτο μετά από συμπίεση με συντελεστή ποιότητας έως και 80. Αντίθετα, η ανθεκτικότητα του υδατογραφήματος επικεφαλίδας στη συμπίεση JPEG ήταν μειωμένη, γεγονός αναμενόμενο λόγω του ότι η ανθεκτικότητα μειώνεται όσο μειώνεται το επίπεδο ανάλυσης.

Ο Πίνακας 12 παρουσιάζει την επίδραση που έχει η συμπίεση JPEG με διάφορους συντελεστές ποιότητας στις υδατογραφημένες εικόνες. Για την αποτίμηση του βαθμού αλλοίωσης επιλέχθηκε ως κριτήριο ομοιότητας και σε αυτήν την περίπτωση η Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance), που δίνεται από την Εξίσωση (7.3).

Συντελεστής Ποιότητας Συμπίεσης JPEG Υδατογρ/νων Εικόνων	Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance)			
	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
95	0,40 ± 0,01	0,18 ± 0,01	0,09 ± 0,01	0,03 ± 0,01
90	0,47 ± 0,01	0,25 ± 0,01	0,12 ± 0,01	0,06 ± 0,01
85	0,48 ± 0,01	0,31 ± 0,01	0,13 ± 0,01	0,08 ± 0,01
80	0,49 ± 0,01	0,38 ± 0,01	0,14 ± 0,01	0,11 ± 0,01
75	0,49 ± 0,01	0,43 ± 0,01	0,20 ± 0,01	0,12 ± 0,02

Πίνακας 12: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες CT)

Ο παραπάνω πίνακας επιβεβαιώνει το γεγονός ότι η συμπίεση JPEG με χαμηλότερο συντελεστή ποιότητας οδηγεί σε υψηλότερες τιμές Κανονικοποιημένης Απόστασης Hamming. Ο πίνακας φανερώνει επίσης την αυξημένη ανθεκτικότητα στα υψηλότερα επίπεδα ανάλυσης, όπως προκύπτει από τη μειωμένη τιμή της Κανονικοποιημένης Απόστασης Hamming σε αυτά.

Τα παραπάνω πειραματικά αποτελέσματα φανερώνουν την αποδοτικότητα και την εφαρμοσιμότητα του υδατογραφικού σχήματος και στην περίπτωση των εικόνων CT. Σημειώνεται μάλιστα ότι η σύγκριση του Πίνακα 11 που παρουσιάζει το ποσοστό εσφαλμένων bits των εξαχθέντων υδατογραφημάτων έπειτα από συμπίεση JPEG στην περίπτωση των εικόνων CT με τον Πίνακα 9 που αντιστοιχεί στις εικόνες υπερήχων, καταδεικνύει τη σημαντική βελτίωση της ανθεκτικότητας των υδατογραφημάτων λόγω της εφαρμογής της υβριδικής κωδικοποίησης. Θυμίζουμε ότι για το ίδιο σύνολο δεδομένων που ενσωματώθηκαν στις δύο διαφορετικές σειρές δοκιμών, οι μεγαλύτερες διαστάσεις των προς εξέταση εικόνων CT επέτρεψαν την επαναληπτική ενσωμάτωση των υδατογραφημάτων. Η βελτίωση της ανθεκτικότητας μέσω της υβριδικής κωδικοποίησης θα φανεί και στις αμέσως επόμενες ενότητες, όπου παρουσιάζονται τα αποτελέσματα εφαρμογής του σχήματος και σε άλλα είδη εικόνων.

7.2.3 Δοκιμές σε Εικόνες Μαγνητικής Τομογραφίας (MRI)

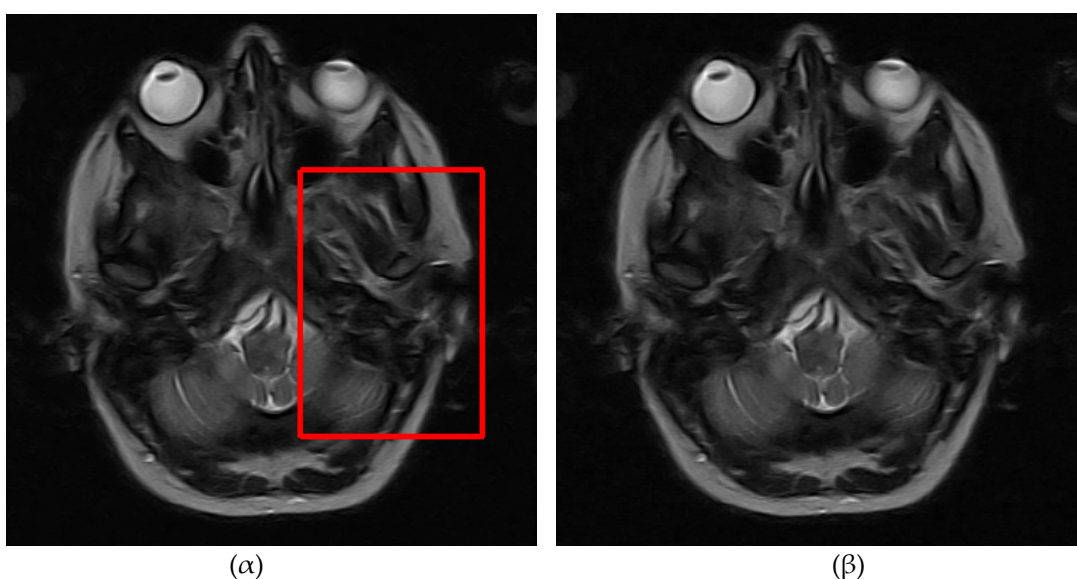
Η επόμενη σειρά δοκιμών του υδατογραφικού σχήματος περιλάμβανε τη χρήση εικόνων μαγνητικής τομογραφίας (MRI). Το δείγμα αποτελούνταν από 20 εικόνες MRI, διαστάσεων 512x512 pixels. Τα υδατογραφήματα που χρησιμοποιήθηκαν ήταν τα ίδια με αυτά των προηγούμενων δοκιμών και ενσωματώθηκαν με τον ίδιο υδατογραφικό αλγόριθμο και στις υποζώνες που περιγράφηκαν στην ενότητα 6.5. Ο Πίνακας 13 παρουσιάζει την κατανομή της ενέργειας μιας εικόνας MRI, δικαιώνοντας και σε αυτήν την περίπτωση την επιλογή των συγκεκριμένων υποζωνών. Και σε αυτή τη σειρά δοκιμών εφαρμόστηκε η υβριδική κωδικοποίηση, η επαναληπτική δηλαδή ενσωμάτωση των κωδικοποιημένων κατά BCH υδατογραφημάτων που φέρουν τα πρόσθετα δεδομένα

(υπογραφή, δείκτης, επικεφαλίδα). Για τα υδατογραφήματα χρησιμοποιήθηκαν επίσης τα σχήματα κωδικοποίησης BCH που παρουσιάζονται στον Πίνακα 4. Η διαδικασία που αφορά την υβριδική κωδικοποίηση περιγράφεται αναλυτικά στην προηγούμενη ενότητα.

Υποζώνη	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
Προσέγγιση Εικόνας	-	-	-	321,33
Οριζόντιες Λεπτομέρειες	2,32	6,08	16,90	47,91
Κάθετες Λεπτομέρειες	1,91	6,02	17,69	46,81
Διαγώνιες Λεπτομέρειες	0,70	2,59	8,59	25,30

Πίνακας 13: Ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών Διακριτού Μετασχηματισμού Κυματιδίων 4 επιπέδων εικόνας MRI

Η απόδοση του υδατογραφικού σχήματος όσον αφορά τη διαφάνεια των ενσωματούμενων υδατογραφημάτων σε εικόνες MRI αποτιμήθηκε ως προς το αισθητικό αποτέλεσμα από γιατρό, ο οποίος διαπίστωσε ότι δεν υπάρχει αλλοίωση των υδατογραφημένων εικόνων που να απειλεί το διαγνωστικό τους περιεχόμενο. Τα Σχήματα 17(α) και 17(β) παρουσιάζουν αντίστοιχα μια εικόνα MRI με μια Περιοχή Ενδιαφέροντος και την υδατογραφημένη εικόνα που προέκυψε.



Σχήμα 17: (α) Αρχική εικόνα MRI με καθορισμένη Περιοχή Ενδιαφέροντος. (β) Προκύπτουσα υδατογραφημένη εικόνα

Για την αποτίμηση της αλλοίωσης των υδατογραφημένων MRI εικόνων χρησιμοποιήθηκε επίσης ο σηματοθορυβικός λόγος PSNR (Εξίσωση 7.1), με τη γνωστή βέβαια αδυναμία του να αποδώσει τις επιπτώσεις των αποκλίσεων των αριθμητικών τιμών στο αισθητικό αποτέλεσμα που αντιλαμβάνεται το ανθρώπινο μάτι. Οι δοκιμές στο σύνολο των εικόνων MRI που εξετάστηκαν, κατέληξαν στο ακόλουθο αποτέλεσμα:

$$PSNR = 46.37 \text{ dB} \pm 0.05 \text{ dB}$$

Όπως γίνεται φανερό από το συνδυασμό της υψηλής τιμής του PSNR και του ικανοποιητικού αισθητικού αποτελέσματος των υδατογραφημένων εικόνων, η απόδοση του υδατογραφικού σχήματος ως προς τη διαφάνεια των υδατογραφημάτων είναι ικανοποιητική και στην περίπτωση των εικόνων MRI.

Ο Πίνακας 14 παρουσιάζει την απόδοση του σχήματος σε εικόνες MRI ως προς την ανθεκτικότητα των υδατογραφημάτων στη συμπίεση JPEG. Τα υδατογραφήματα που φέρουν την πρόσθετη πληροφορία (υπογραφή, δείκτες, στοιχεία ασθενή) εξάχθηκαν από εικόνες MRI που υπεβλήθησαν σε συμπίεση JPEG με διάφορους συντελεστές ποιότητας και στη συνέχεια υπολογίστηκε το ποσοστό εσφαλμένων bits για καθένα από αυτά.

Τύπος Υδατογραφήματος	Υπογραφή	Δείκτης	Επικεφαλίδα
Επίπεδο Ενσωμάτωσης	4	3	2
95	0	0	0
Συντελεστής	0	0	13,8
Ποιότητας	0	0	23,4
JPEG	0	0	30,5
75	0	4,4	39,3

Πίνακας 14: Ποσοστό εσφαλμένων bits σε υδατογραφήματα εξαχθέντα από εικόνες MRI (%)

Όπως προκύπτει και από τον παραπάνω πίνακα, η απόδοση του υδατογραφικού σχήματος ως προς την ανθεκτικότητα των υδατογραφημάτων στη συμπίεση JPEG σε εικόνες MRI είναι ικανοποιητική. Το υδατογράφημα υπογραφής εξήχθη χωρίς κανένα εσφαλμένο bit, ακόμα και στην περίπτωση κατά την οποία η υδατογραφημένη εικόνα υπέστη συμπίεση JPEG75. Το υδατογράφημα δείκτη από

την άλλη πλευρά αποδείχθηκε ανθεκτικό στη συμπίεση με συντελεστή ποιότητας έως και 80. Λόγω της μειωμένης ανθεκτικότητας στο δεύτερο επίπεδο ανάλυσης – στο οποίο ενσωματώθηκε το υδατογράφημα επικεφαλίδας – σε σχέση με τα υψηλότερα επίπεδα, η ανθεκτικότητα του υδατογραφήματος επικεφαλίδας στη συμπίεση JPEG παρατηρείται μειωμένη σε σύγκριση με αυτή των άλλων δύο.

Ο Πίνακας 15 παρουσιάζει την επίδραση της συμπίεσης JPEG με διάφορους συντελεστές ποιότητας στις υδατογραφημένες εικόνες MRI. Ως κριτήριο ομοιότητας για την αποτίμηση του βαθμού αλλοίωσης επιλέχθηκε και σε αυτήν την περίπτωση η Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance), που δίνεται από την Εξίσωση (7.3).

Συντελεστής Ποιότητας Συμπίεσης JPEG Υδατογρ/νων Εικόνων	Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance)			
	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
95	0,42 ± 0,01	0,16 ± 0,01	0,07 ± 0,01	0,04 ± 0,01
90	0,47 ± 0,01	0,25 ± 0,01	0,11 ± 0,01	0,06 ± 0,01
85	0,49 ± 0,01	0,33 ± 0,01	0,12 ± 0,01	0,08 ± 0,01
80	0,49 ± 0,01	0,39 ± 0,01	0,13 ± 0,01	0,11 ± 0,01
75	0,50 ± 0,01	0,42 ± 0,01	0,19 ± 0,01	0,12 ± 0,01

Πίνακας 15: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες MRI)

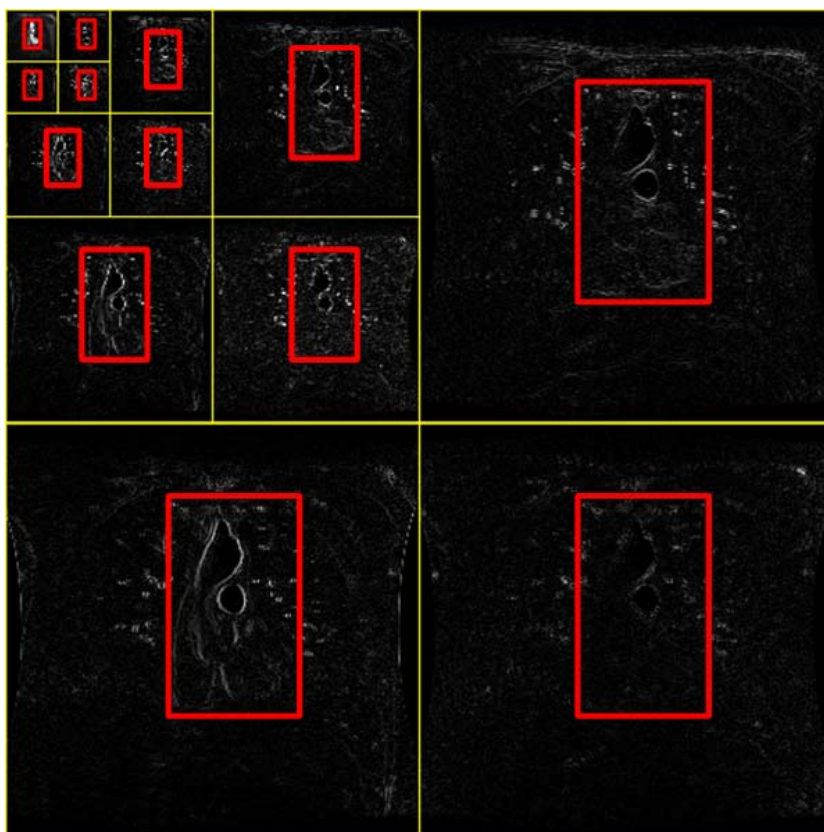
Όπως είναι αναμενόμενο, ο παραπάνω πίνακας επιβεβαιώνει το γεγονός ότι μειώνοντας το συντελεστή ποιότητας της συμπίεσης JPEG, προκύπτουν υψηλότερες τιμές Κανονικοποιημένης Απόστασης Hamming. Ο πίνακας παρουσιάζει επίσης τη μειωμένη τιμή της Κανονικοποιημένης Απόστασης Hamming στα υψηλότερα επίπεδα ανάλυσης, που αντανακλά την αυξημένη ανθεκτικότητα που παρατηρείται σε αυτά.

Από τα παραπάνω πειραματικά αποτελέσματα γίνεται φανερό η αποδοτικότητα και η εφαρμοσιμότητα του υδατογραφικού σχήματος και στην περίπτωση των εικόνων MRI. Αξίζει να σημειωθεί ότι και σε αυτή τη σειρά δοκιμών παρατηρήθηκε σημαντική βελτίωση της ανθεκτικότητας της ενσωματούμενης

πρόσθετης πληροφορίας, λόγω της επαναληπτικής (τριπλής) ενσωμάτωσης των κωδικοποιημένων κατά BCH υδατογραφημάτων.

7.2.4 Δοκιμές σε Εικόνες Μαγνητικής Αγγειογραφίας (MRA)

Το υδατογραφικό σχήμα δοκιμάστηκε και σε εικόνες μαγνητικής αγγειογραφίας (MRA)· το δείγμα περιλάμβανε 20 εικόνες MRA, διαστάσεων 512x512 pixels. Και σε αυτήν τη σειρά δοκιμών χρησιμοποιήθηκαν τα υδατογραφήματα που περιγράφονται στην ενότητα 7.2.1. και τον Πίνακα 4. Στα υδατογραφήματα που φέρουν την πρόσθετη πληροφορία (υπογραφή, δείκτης, επικεφαλίδα) εφαρμόστηκε υβριδική κωδικοποίηση που περιλάμβανε την κωδικοποίησή τους κατά BCH και την τριπλή ενσωμάτωση καθενός από αυτά στις εικόνες, προκειμένου να αυξηθεί η ανθεκτικότητά τους. Λεπτομέρειες για την υβριδική κωδικοποίηση που εφαρμόστηκε δίνονται στην ενότητα 7.2.2. Στο Σχήμα 18 φαίνονται οι υποζώνες που προέκυψαν από το διακριτό μετασχηματισμό κυματιδίων τεσσάρων επιπέδων σε εικόνα MRA.



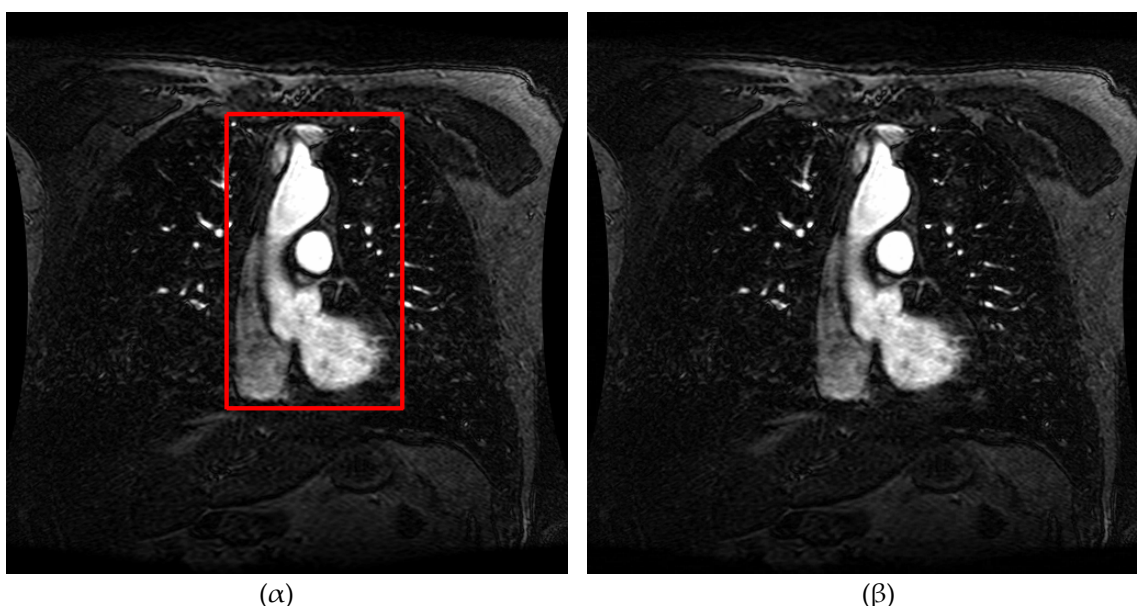
Σχήμα 18: Αντιστοιχία των Πινάκων Περιοχής Ενδιαφέροντος ανά υποζώνη και επίπεδο ανάλυσης εικόνας MRA

Στον Πίνακα 16 αποτυπώνεται η κατανομή της ενέργειας μιας εικόνας MRA, η οποία φανερώνει ότι μπορεί και σε αυτόν τον τύπο εικόνων να εφαρμοστεί το σχήμα ενσωμάτωσης των υδατογραφημάτων στις υποζώνες που παρουσιάστηκαν στην ενότητα 6.5.

Υποζώνη	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
Προσέγγιση Εικόνας	-	-	-	490,44
Οριζόντιες Λεπτομέρειες	5,67	14,75	30,40	70,94
Κάθετες Λεπτομέρειες	4,52	12,64	29,38	67,02
Διαγώνιες Λεπτομέρειες	1,96	7,57	17,98	38,07

Πίνακας 16: Ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών Διακριτού Μετασχηματισμού Κυματιδίων 4 επιπέδων εικόνας MRA

Η διαφάνεια των υδατογραφημάτων που ενσωματώνονται από το σχήμα σε εικόνες MRA αξιολογήθηκε από γιατρό, που συμπέρανε και σε αυτήν την περίπτωση ότι δεν υπάρχει αλλοίωσή τους που να μπορεί να οδηγήσει σε λανθασμένη εκτίμηση και διάγνωση. Τα Σχήματα 19(α) και 19(β) παρουσιάζουν μια εικόνα MRA όπου διακρίνεται η επιλεγμένη Περιοχή Ενδιαφέροντος και την αντίστοιχη υδατογραφημένη εικόνα.



Σχήμα 19: (α) Αρχική εικόνα MRA με καθορισμένη Περιοχή Ενδιαφέροντος. (β) Προκύπτουσα υδατογραφημένη εικόνα

Η αξιολόγηση της πιστότητας των υδατογραφημένων εικόνων MRA από άποψη αριθμητικών αποκλίσεων σε σχέση με τις αρχικές, έγινε και πάλι με χρήση του σηματοθορυβικού λόγου PSNR (Εξίσωση 7.1). Η μέση τιμή του PSNR που προέκυψε από τις δοκιμές στο σύνολο των υπό εξέταση εικόνων, υπολογίστηκε ίση με:

$$PSNR = 45.96 \text{ dB} \pm 0.04 \text{ dB}$$

Ο Πίνακας 17 παρουσιάζει μια συγκριτική αποτίμηση της αλλοίωσης που προκαλείται στις εικόνες μαγνητικής αγγειογραφίας από την εφαρμογή του υδατογραφικού σχήματος και τη συμπίεση JPEG με διάφορους συντελεστές ποιότητας ως προς το μέτρο ποιότητας PSNR.

Είδος Επεξεργασίας Εικόνας	PSNR (dB)
Υδατογράφηση	45,98 ± 0,05
JPEG 95	45,23 ± 0,54
JPEG 90	42,16 ± 0,69
JPEG 85	40,50 ± 0,71
JPEG 80	39,39 ± 0,72
JPEG 75	38,52 ± 0,71

Πίνακας 17: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων MRA ως προς το PSNR

Και στην περίπτωση των εικόνων MRA είναι φανερό η ικανοποιητική απόδοση του υδατογραφικού σχήματος ως προς τη διαφάνεια των ενσωματούμενων υδατογραφημάτων, όπως προκύπτει από το ικανοποιητικό αισθητικά αντιλαμβανόμενο αποτέλεσμα σε συνδυασμό με την υψηλή τιμή του PSNR.

Η ανθεκτικότητα των υδατογραφημάτων που φέρουν την πρόσθετη πληροφορία (υπογραφή, δείκτες, στοιχεία ασθενή) αξιολογήθηκε υποβάλλοντας τις υδατογραφημένες εικόνες MRA σε συμπίεση JPEG. Ο Πίνακας 18 παρουσιάζει το

ποσοστό εσφαλμένων bits στα υδατογραφήματα που εξάχθηκαν από τις εικόνες MRA που υπέστησαν συμπίεση JPEG με διάφορους συντελεστές ποιότητας.

Τύπος Υδατογραφήματος		Υπογραφή	Δείκτης	Επικεφαλίδα
Επίπεδο Ενσωμάτωσης		4	3	2
	95	0	0	0
Συντελεστής	90	0	0	15,9
Ποιότητας	85	0	0	25,3
JPEG	80	0	0	35,8
	75	0	0	43,6

Πίνακας 18: Ποσοστό εσφαλμένων bits σε υδατογραφήματα εξαχθέντα από εικόνες MRA (%)

Όπως διαπιστώνεται από τον παραπάνω πίνακα, η απόδοση του υδατογραφικού σχήματος ως προς την ανθεκτικότητα των υδατογραφημάτων στη συμπίεση JPEG είναι ικανοποιητική και στην περίπτωση των εικόνων MRA. Συγκεκριμένα, τόσο το υδατογράφημα υπογραφής όσο και το υδατογράφημα δείκτη εξάχθηκαν χωρίς σφάλματα ακόμη και όταν η υδατογραφημένη εικόνα υπεβλήθη σε συμπίεση JPEG75. Στον πίνακα απεικονίζεται επίσης το ποσοστό εσφαλμένων bits στην περίπτωση του υδατογραφήματος επικεφαλίδας, του οποίου η μειωμένη ανθεκτικότητα σε σχέση με τα άλλα δύο οφείλεται στη μειωμένη ανθεκτικότητα του δευτέρου επιπέδου ανάλυσης όπου και ενσωματώνεται, όπως έχει προαναφερθεί.

Η επίδραση της συμπίεσης JPEG με διάφορους συντελεστές ποιότητας στις υδατογραφημένες εικόνες MRA απεικονίζεται στον Πίνακα 19. Η Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance) που ορίζεται στην Εξίσωση 7.3 χρησιμοποιήθηκε και σε αυτήν την περίπτωση ως κριτήριο ομοιότητας για την αποτίμηση του βαθμού αλλοίωσης των εικόνων. Τα συμπεράσματα που προκύπτουν από τον Πίνακα 19 αφορούν, όπως και στις προηγούμενες σειρές δοκιμών, την αύξηση της τιμής της Κανονικοποιημένης Απόστασης Hamming κατά τη μείωση του συντελεστή ποιότητας της συμπίεσης JPEG και τη μείωση της τιμής της στα υψηλά επίπεδα ανάλυσης, όπου και παρατηρείται μεγαλύτερη ανθεκτικότητα στις τροποποιήσεις των εικόνων.

Συντελεστής Ποιότητας Συμπίεσης JPEG Υδατογραφ/νων Εικόνων	Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance)			
	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
95	0,48 ± 0,01	0,18 ± 0,01	0,06 ± 0,01	0,04 ± 0,01
90	0,50 ± 0,01	0,30 ± 0,01	0,10 ± 0,01	0,06 ± 0,01
85	0,50 ± 0,01	0,38 ± 0,01	0,13 ± 0,01	0,09 ± 0,01
80	0,50 ± 0,01	0,42 ± 0,01	0,16 ± 0,01	0,10 ± 0,02
75	0,50 ± 0,01	0,45 ± 0,01	0,20 ± 0,01	0,12 ± 0,02

Πίνακας 19: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες MRA)

Τα παραπάνω πειραματικά αποτελέσματα φανερώνουν την αποδοτικότητα και την εφαρμοσιμότητα του υδατογραφικού σχήματος και στην περίπτωση εικόνων MRA. Και σε αυτό το είδος εικόνων παρατηρήθηκε ιδιαίτερα υψηλή ανθεκτικότητα της ενσωματούμενης πρόσθετης πληροφορίας, που οφείλεται σε μεγάλο βαθμό στην επαναληπτική ενσωμάτωση των κωδικοποιημένων κατά BCH υδατογραφημάτων.

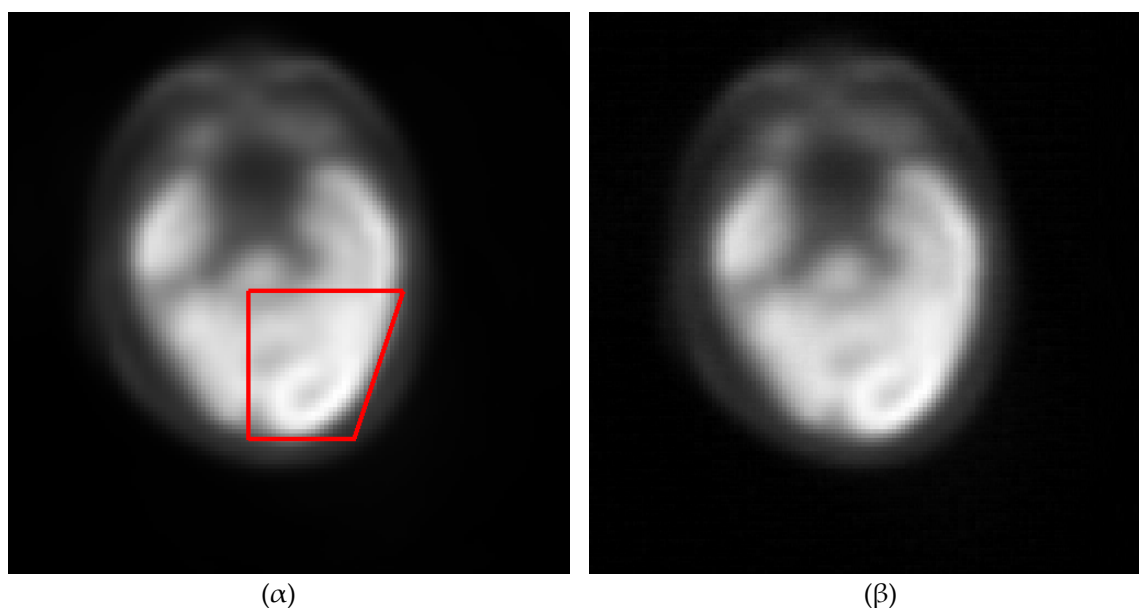
7.2.5 Δοκιμές σε Εικόνες Τομογραφίας Εκπομπής Ποζιτρονίου (PET)

Σε αυτήν την ενότητα περιγράφονται τα αποτελέσματα των δοκιμών του υδατογραφικού σχήματος σε εικόνες τομογραφίας εκπομπής ποζιτρονίου (PET). Το δείγμα αποτελούνταν από 20 εικόνες PET, διαστάσεων 512x512 pixels. Και σε αυτήν τη σειρά δοκιμών ενσωματώθηκαν τα υδατογραφήματα που χρησιμοποιήθηκαν και στις προηγούμενες δοκιμές· εφαρμόστηκε και σε αυτήν την περίπτωση υβριδική κωδικοποίηση, επαναληπτική δηλαδή ενσωμάτωση των κωδικοποιημένων κατά BCH υδατογραφημάτων που φέρουν τα πρόσθετα δεδομένα (υπογραφή, δείκτης, επικεφαλίδα). Ο Πίνακας 4 παρουσιάζει τα μήκη των υδατογραφημάτων αυτών, καθώς και τους BCH κώδικες που χρησιμοποιήθηκαν για την κωδικοποίησή τους. Λεπτομέρειες για το πώς προέκυψαν τα υδατογραφήματα που δοκιμάστηκαν στις προσομοιώσεις και για την υβριδική κωδικοποίηση, δίνονται αντίστοιχα στις ενότητες 7.2.1 και 7.2.2. Ο Πίνακας 20 απεικονίζει την κατανομή της ενέργειας μιας εικόνας PET, δικαιώνοντας την επιλογή των υποζωνών που παρουσιάστηκαν στην ενότητα 6.5.

Υποζώνη	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
Προσέγγιση Εικόνας	-	-	-	693,71
Οριζόντιες Λεπτομέρειες	2,16	8,31	31,01	108,46
Κάθετες Λεπτομέρειες	2,64	10,18	37,94	145,22
Διαγώνιες Λεπτομέρειες	0,26	1,67	9,59	46,39

Πίνακας 20: Ενέργεια της εικόνας προσέγγισης και των εικόνων λεπτομερειών Διακριτού Μετασχηματισμού Κυματιδίων 4 επιπέδων εικόνας PET

Η διαφάνεια των ενσωματούμενων υδατογραφημάτων σε εικόνες PET αξιολογήθηκε και σε αυτήν την περίπτωση από γιατρό, που διαπίστωσε τη διατήρηση του διαγνωστικού περιεχομένου στις υδατογραφημένες εικόνες. Τα Σχήματα 20(α) και 20(β) παρουσιάζουν αντίστοιχα μια εικόνα PET με καθορισμένη Περιοχή Ενδιαφέροντος και την προκύπτουσα υδατογραφημένη εικόνα.



Σχήμα 20: (α) Αρχική εικόνα PET με καθορισμένη Περιοχή Ενδιαφέροντος. (β) Προκύπτουσα υδατογραφημένη εικόνα

Η αλλοίωση που προκάλεσε η εφαρμογή του υδατογραφικού σχήματος στις εικόνες PET αποτιμήθηκε και από άποψη τροποποίησης των τιμών έντασης των pixels των εικόνων, με υπολογισμό του σηματοθορυβικού λόγου PSNR (Εξίσωση 7.1). Η μέση τιμή του PSNR που προέκυψε από το σύνολο των εικόνων PET που εξετάστηκαν είναι η εξής:

$$PSNR = 46.66 \text{ dB} \pm 0.20 \text{ dB}$$

Δεδομένης της πιστότητας των υδατογραφημένων εικόνων σε συνδυασμό με την υψηλή τιμή του PSNR, είναι φανερό η ικανοποιητική απόδοση του υδατογραφικού σχήματος ως προς τη διαφάνεια των υδατογραφημάτων και στην περίπτωση των εικόνων PET.

Το υδατογραφικό σχήμα εξετάστηκε επίσης ως προς την απόδοσή του από άποψη ανθεκτικότητας των υδατογραφημάτων που φέρουν την πρόσθετη πληροφορία (υπογραφή, λέξεις-κλειδιά, στοιχεία ασθενή). Ο Πίνακας 21 παρουσιάζει το ποσοστό εσφαλμένων bits στα υδατογραφήματα αυτά που εξάχθηκαν από υδατογραφημένες εικόνες PET, οι οποίες υπέστησαν συμπίεση JPEG με διάφορους συντελεστές ποιότητας.

Τύπος Υδατογραφήματος	Υπογραφή	Δείκτης	Επικεφαλίδα
Επίπεδο Ενσωμάτωσης	4	3	2
95	0	0	0
Συντελεστής	0	0	12,6
Ποιότητας	0	0	20,9
JPEG	0	0	30,8
75	0	0	36,0

Πίνακας 21: Ποσοστό εσφαλμένων bits σε υδατογραφήματα εξαχθέντα από εικόνες PET (%)

Ο παραπάνω πίνακας φανερώνει την ικανοποιητική απόδοση του υδατογραφικού σχήματος ως προς την ανθεκτικότητα των υδατογραφημάτων στη συμπίεση JPEG. Συγκεκριμένα, τα υδατογραφήματα υπογραφής και δείκτη εξάχθηκαν χωρίς σφάλμα, ακόμα και στην περίπτωση κατά την οποία η υδατογραφημένη εικόνα υπέστη συμπίεση JPEG75. Το υδατογράφημα επικεφαλίδας που ενσωματώθηκε στο δεύτερο επίπεδο ανάλυσης, αποδείχθηκε λιγότερο ανθεκτικό στη συμπίεση, γεγονός αναμενόμενο λόγω της μειωμένης ανθεκτικότητας που παρατηρείται στο συγκεκριμένο επίπεδο ανάλυσης σε σχέση με τα υψηλότερα.

Στον πίνακα που ακολουθεί (Πίνακας 22) απεικονίζεται η επίδραση της συμπίεσης JPEG με διάφορους συντελεστές ποιότητας στις υδατογραφημένες

εικόνες PET. Η Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance) που επιλέχθηκε ως κριτήριο ομοιότητας για την αποτίμηση του βαθμού αλλοίωσης και ορίζεται στην Εξίσωση 7.3, υπολογίστηκε για το σύνολο των εικόνων PET που εξετάστηκαν και τα αποτελέσματα που προέκυψαν είναι τα ακόλουθα:

Συντελεστής Ποιότητας Συμπίεσης JPEG Υδατογρ/νων Εικόνων	Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance)			
	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
95	0,39 ± 0,01	0,11 ± 0,01	0,04 ± 0,01	0,03 ± 0,01
90	0,48 ± 0,01	0,19 ± 0,01	0,07 ± 0,01	0,06 ± 0,01
85	0,49 ± 0,01	0,27 ± 0,01	0,08 ± 0,01	0,07 ± 0,01
80	0,50 ± 0,01	0,36 ± 0,01	0,09 ± 0,01	0,08 ± 0,02
75	0,50 ± 0,01	0,43 ± 0,01	0,14 ± 0,01	0,09 ± 0,02

Πίνακας 22: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες PET)

Ο παραπάνω πίνακας φανερώνει την αύξηση της τιμής της Κανονικοποιημένης Απόστασης Hamming που παρατηρείται για μειωμένες τιμές του συντελεστή ποιότητας της συμπίεσης JPEG. Επίσης είναι φανερό ότι προκύπτουν μειωμένες τιμές της Κανονικοποιημένης Απόστασης Hamming στα υψηλότερα επίπεδα ανάλυσης, γεγονός που συνδέεται με την αυξημένη ανθεκτικότητα στα επίπεδα αυτά.

Τα παραπάνω πειραματικά αποτελέσματα σε εικόνες PET φανερώνουν την αποδοτικότητα και εφαρμοσιμότητα του υδατογραφικού σχήματος και στο συγκεκριμένο είδος ιατρικών εικόνων. Αξίζει να επισημανθεί η αυξημένη ανθεκτικότητα των υδατογραφημάτων με την πρόσθετη πληροφορία, που επιτεύχθηκε και σε αυτήν την περίπτωση μέσω της επαναληπτικής ενσωμάτωσής τους, αφού προηγουμένως εφαρμόστηκε σε αυτά κωδικοποίηση BCH.

7.2.6 Εναλλακτικά Σχήματα Εφαρμογής Αλγορίθμου

Σε αυτήν την ενότητα περιγράφονται τα αποτελέσματα των δοκιμών που έγιναν σε προηγούμενες εκδόσεις του υδατογραφικού σχήματος, οι οποίες

υλοποιήθηκαν στα πρώτα στάδια εκπόνησης της διατριβής. Οι εκδόσεις αυτές παρουσιάζονται εδώ για λόγους πληρότητας, καθώς σε αυτές βασίστηκε η τελική έκδοση του υδατογραφικού σχήματος που περιγράφηκε στο Κεφάλαιο 6 και αποτιμήθηκε με βάση τα αποτελέσματα των δοκιμών που παρουσιάστηκαν στις προηγούμενες ενότητες.

7.2.6.1 Ενσωμάτωση τριών τύπων υδατογραφημάτων χωρίς επιλογή Περιοχής Ενδιαφέροντος

Η πρώτη υλοποίηση του βασικού υδατογραφικού σχήματος που περιγράφηκε στο Κεφάλαιο 6, περιλάμβανε την ενσωμάτωση τριών τύπων υδατογραφημάτων [14] στην εικόνα. Συγκεκριμένα, το υδατογράφημα υπογραφής με τον αναγνωριστικό κωδικό του γιατρού για την ταυτοποίησή του, το υδατογράφημα επικεφαλίδας που περιλαμβάνει προσωπικά στοιχεία ασθενούς, ιατρικό ιστορικό κ.λπ. και το υδατογράφημα αναφοράς που παρέχει πληροφορία για το εάν και σε ποια σημεία έχουν μεταβληθεί τα δεδομένα [15].

Περιγραφή υλοποίησης

Σε αυτήν την έκδοση του υδατογραφικού σχήματος, εφαρμόζεται στην εικόνα διακριτός μετασχηματισμός κυματιδίων Haar τριών επιπέδων. Το υδατογράφημα υπογραφής και το υδατογράφημα επικεφαλίδας εισάγονται σε οριζόντιους συντελεστές (horizontal detail coefficients) του δεύτερου και του τρίτου επιπέδου ανάλυσης (decomposition level) που επιλέγονται βάσει κλειδιού, ενώ το υδατογράφημα αναφοράς στους χωρικά αντίστοιχους κάθετους συντελεστές. Το υδατογράφημα αναφοράς αποτελείται σε αυτήν την περίπτωση από μια συγκεκριμένη ακολουθία bits, η οποία επαναλαμβάνεται όσες φορές χρειάζεται έως ότου το μήκος του υδατογραφήματος αναφοράς εξισωθεί με το μήκος του αντίστοιχου υδατογραφήματος δεδομένων (υπογραφή ή επικεφαλίδα). Όπως έχει αναφερθεί και στο Κεφάλαιο 6, μια ενδεχόμενη τροποποίηση στην εικόνα είναι πολύ πιθανό να επηρεάσει τόσο τους οριζόντιους όσο και τους κάθετους συντελεστές, καθώς οι αντίστοιχες υποζώνες (sub-bands) έχουν παρόμοια συμπεριφορά και

χαρακτηριστικά, σε αντίθεση με τη διαγώνια υποζώνη [16]. Στη συγκεκριμένη υλοποίηση του υδατογραφικού σχήματος επιλέχθηκαν για την εισαγωγή των υδατογραφήματων αναφοράς οι συντελεστές της κάθετης υποζώνης που αντιστοιχούν χωρικά στους οριζόντιους συντελεστές όπου εισάγονται τα υδατογραφήματα δεδομένων (υπογραφή, επικεφαλίδα). Η επιλογή αυτή στηρίχτηκε στο γεγονός ότι βάσει των παραπάνω, αναμένεται ότι τα υδατογραφήματα αναφοράς του δεύτερου και του τρίτου επιπέδου ανάλυσης θα αντανακλούν ενδεχόμενη τροποποίηση της εικόνας στα σημεία όπου ενσωματώθηκαν τα υδατογραφήματα δεδομένων και άρα θα παρέχουν μια ένδειξη του κατά πόσο έχει αλλοιωθεί η πληροφορία που μεταφέρουν τα υδατογραφήματα αυτά.

Όπως περιγράφηκε αναλυτικά στο Κεφάλαιο 6 (ενότητα 6.5), η προσέγγιση της εικόνας στο τελευταίο επίπεδο ανάλυσης (coarse scale approximation) περιέχει το μεγαλύτερο μέρος της ενέργειας της αρχικής εικόνας και άρα επηρεάζει σε μεγάλο βαθμό την ποιότητά της, οπότε εξαιρείται και σε αυτήν την περίπτωση από τη διαδικασία εισαγωγής υδατογραφήματος. Οι διαγώνιες υποζώνες εξαιρούνται επίσης, λόγω του ότι τροποποιούνται ή/και εξαλείφονται ακόμη και με συνήθη επεξεργασία ή συμπίεση, εξαιτίας της ελάχιστης επίδρασης που έχουν στην ποιότητα της εικόνας. Οι συντελεστές του πρώτου επιπέδου ανάλυσης τροποποιούνται επίσης εύκολα με συνηθισμένη επεξεργασία· γι' αυτόν το λόγο χρησιμοποιούνται μόνο για εισαγωγή του υδατογραφήματος αναφοράς που επιτρέπει τον έλεγχο της ακεραιότητας των δεδομένων. Πέρα από τα παραπάνω χαρακτηριστικά, στη συγκεκριμένη υλοποίηση του υδατογραφικού σχήματος αξιοποιήθηκε και το γεγονός ότι το ανθρώπινο οπτικό σύστημα αντιλαμβάνεται λιγότερο το θόρυβο στις ζώνες υψηλής ανάλυσης (resolution), επιτρέποντας έτσι μεγαλύτερες μεταβολές στις τιμές των αντίστοιχων συντελεστών λεπτομερειών, χωρίς αυτές να γίνονται αντιληπτές. Το χαρακτηριστικό αυτό αξιοποιήθηκε στην επιλογή του συντελεστή κβαντοποίησης Δ , όπως θα φανεί παρακάτω. Η επιλογή των παραμέτρων του σχήματος και η κατανομή των υδατογραφήματων στις διάφορες υποζώνες προέκυψε λαμβάνοντας υπόψη τα παραπάνω στοιχεία, με στόχο τη βέλτιστη απόδοση όσον αφορά την ανθεκτικότητα και τη διαφάνεια.

Με βάση τα παραπάνω, τα bits των υδατογραφημάτων επικεφαλίδας και υπογραφής εισάγονται σε συντελεστές οριζοντίων λεπτομερειών του δεύτερου και τρίτου επιπέδου ανάλυσης αντίστοιχα, και τα bits υδατογραφήματος αναφοράς στους συντελεστές κάθετων λεπτομερειών της ίδιας χωρικής θέσης. Τα bits του υδατογραφήματος αναφοράς εισάγονται επίσης σε συντελεστές κάθετων λεπτομερειών του πρώτου επιπέδου ανάλυσης με στόχο την παροχή διεξοδικού ελέγχου ακεραιότητας της εικόνας. Σημειώνεται ότι λόγω της αυξημένης ανθεκτικότητας των συντελεστών λεπτομερειών που παρατηρείται στα υψηλότερα επίπεδα ανάλυσης, ο τρόπος με τον οποίο μια αλλοίωση σε ένα τμήμα της εικόνας αποτυπώνεται στα διάφορα επίπεδα ανάλυσής της, αντανακλά τον αντίκτυπο που έχει η αλλοίωση αυτή στην ποιότητα της εικόνας. Για παράδειγμα, μια αλλοίωση που εντοπίζεται μόνο στο πρώτο επίπεδο ανάλυσης αλλά είναι εξαιρετικά περιορισμένη στα υπόλοιπα επίπεδα – τα οποία φέρουν και την περισσότερη πληροφορία της εικόνας – μπορεί τελικά να αποτιμηθεί ως μηδαμινή και να αγνοηθεί, θεωρώντας ότι δεν υποβαθμίζει τη διαγνωστική αξία της εικόνας.

Στη συγκεκριμένη έκδοση του υδατογραφικού σχήματος, η επιλογή της παραμέτρου κβαντοποίησης Δ έγινε λαμβάνοντας υπόψη τη «δυαδική ρητή μορφή» των συντελεστών κυματιδίων Haar και τη μειωμένη ευαισθησία του ματιού στο θόρυβο σε ζώνες υψηλής ανάλυσης (resolution). Βάσει αυτών, η παράμετρος κβαντοποίησης Δ ορίστηκε ως εξής:

$$\Delta = \frac{d}{2^{c+l}} \quad (7.4)$$

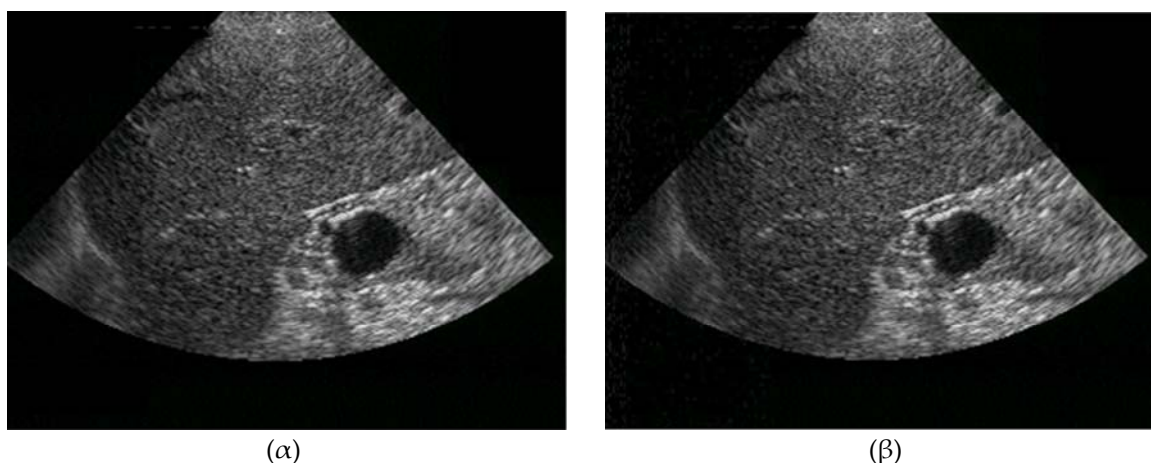
όπου c , d είναι θετικοί ακέραιοι αριθμοί που ορίζονται από το χρήστη και l είναι το επίπεδο ανάλυσης.

Αποτελέσματα

Ο αλγόριθμος δοκιμάστηκε σε ένα σύνολο 40 εικόνων υπερήχων, μεγέθους 256x320 pixels, που συλλέχθηκαν από τον ίδιο γιατρό, με τον ίδιο εξοπλισμό και τις ίδιες ρυθμίσεις συστήματος, προκειμένου να επιτευχθούν κοινά στατιστικά χαρακτηριστικά στο σύνολο των εικόνων. Το μήκος του βασικού υδατογραφήματος αναφοράς και των υδατογραφημάτων υπογραφής και επικεφαλίδας που

χρησιμοποιήθηκαν στις μετρήσεις ήταν 512, 128 και 696 bits αντιστοίχως. Δεδομένου ότι τα δύο υδατογραφήματα αναφοράς που εισάγονται στο δεύτερο και το τρίτο επίπεδο ανάλυσης, σε χωρικά αντίστοιχες θέσεις με τα υδατογραφήματα υπογραφής και επικεφαλίδας, έχουν το ίδιο πλήθος bits με τα υδατογραφήματα αυτά, το συνολικό μήκος των υδατογραφημάτων που ενσωματώθηκαν στις εικόνες ήταν 2.160 bits.

Λόγω των αυστηρών απαιτήσεων όσον αφορά τις επιτρεπτές μεταβολές στις ιατρικές εικόνες, έγινε αποτίμηση της ποιότητας τόσο από άποψη σήματος, όσο και από άποψη οπτικού αποτελέσματος (perceptual quality). Ο σηματοθορυβικός λόγος (PSNR) δίνεται από την Εξίσωση 7.1. Οι δοκιμές κατέληξαν σε μια μέση τιμή για το PSNR ίση με 41,93 dB, με τυπική απόκλιση 0,62 dB. Η οπτικά αντιλαμβανόμενη ποιότητα (perceptual quality) των υδατογραφημένων εικόνων αξιολογήθηκε από γιατρό, ο οποίος δεν παρατήρησε διαφορά ανάμεσα σε αυτές και τις αντίστοιχες αρχικές εικόνες. Στο Σχήμα 21 φαίνεται μια εικόνα υπερήχων και η αντίστοιχη υδατογραφημένη εικόνα που προέκυψε από τη συγκεκριμένη έκδοση του υδατογραφικού σχήματος.



Σχήμα 21: (α) Αρχική εικόνα υπερήχων. (β) Αντίστοιχη υδατογραφημένη εικόνα.

Ο Πίνακας 23 δίνει μια συγκριτική παρουσίαση της αλλοίωσης που εισάγεται με την εφαρμογή του συγκεκριμένου υδατογραφικού σχήματος και του αλγορίθμου συμπίεσης JPEG με διάφορους συντελεστές ποιότητας. Όπως φαίνεται και στον πίνακα, η υδατογραφική μέθοδος προκαλεί μικρότερη αλλοίωση στην εικόνα από ό,τι η συμπίεση JPEG με συντελεστή ποιότητας μέχρι και 90. Οι μεγάλες τιμές του

PSNR που προέκυψαν, σε συνδυασμό με την ικανοποιητική ποιότητα των υδατογραφημένων εικόνων, φανέρωσαν την ικανοποιητική απόδοση της συγκεκριμένης έκδοσης του αλγορίθμου ως προς τη διαφάνεια των υδατογραφημάτων.

Είδος Επεξεργασίας Εικόνας	PSNR (dB)
Υδατογράφιση	41.93 ± 0.62
JPEG 95	44.88 ± 0.68
JPEG 90	40.29 ± 0.99
JPEG 85	37.71 ± 1.15
JPEG 80	36.03 ± 1.24
JPEG 75	34.77 ± 1.30

Πίνακας 23: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων υπερήχων ως προς το PSNR

7.2.6.2 Ενσωμάτωση τεσσάρων τύπων υδατογραφημάτων χωρίς επιλογή Περιοχής Ενδιαφέροντος

Η δεύτερη έκδοση του υδατογραφικού σχήματος εμπλούτισε ουσιαστικά την υλοποίηση που περιγράφηκε στην προηγούμενη ενότητα μέσω της εισαγωγής τεσσάρων – αντί τριών της προηγούμενης έκδοσης – τύπων υδατογραφημάτων στις εικόνες: ενός υδατογραφήματος υπογραφής με τον αναγνωριστικό κωδικό του γιατρού για την ταυτοποίησή του, ενός υδατογραφήματος δείκτη με λέξεις-κλειδιά για αποδοτική αρχειοθέτηση και ανάκτηση εικόνων, ενός υδατογραφήματος επικεφαλίδας με προσωπικά στοιχεία του ασθενή και πληροφορίες για την εξέταση και ενός υδατογραφήματος αναφοράς που επιτρέπει τον έλεγχο ακεραιότητας των δεδομένων.

Περιγραφή υλοποίησης

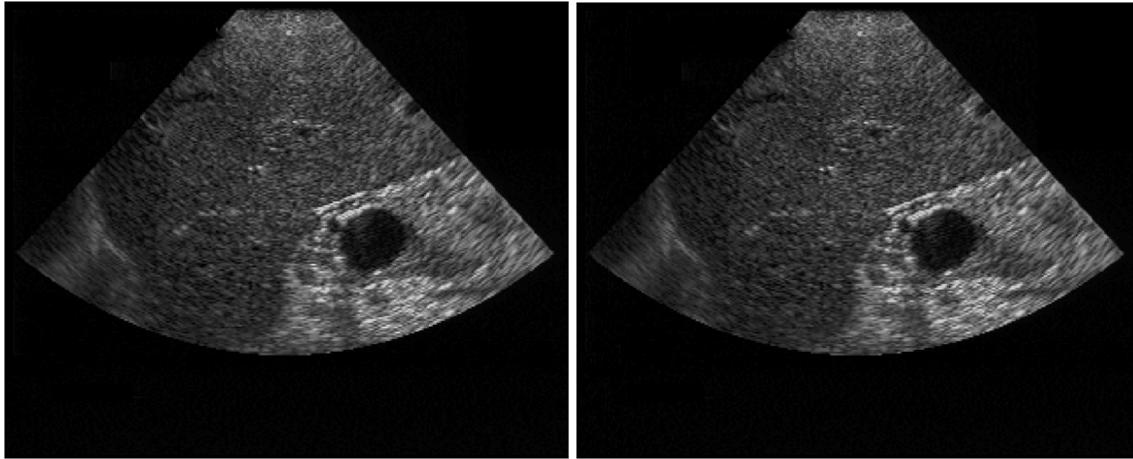
Σε αυτήν την έκδοση του υδατογραφικού σχήματος, εφαρμόστηκε στην εικόνα διακριτός μετασχηματισμός κυματιδίων Haar τεσσάρων επιπέδων. Με σκοπό

τη βέλτιστη δυνατή απόδοση όσον αφορά την ανθεκτικότητα και τη διαφάνεια, η εισαγωγή των τεσσάρων τύπων υδατογραφημάτων στις εικόνες έγινε με διαμόρφωση του υδατογραφικού σχήματος ως εξής: η εικόνα αναλύθηκε σε τέσσερα επίπεδα με χρήση διακριτού μετασχηματισμού κυματιδίων Haar. Τα υδατογραφήματα επικεφαλίδας, δείκτη και υπογραφής ενσωματώθηκαν σε επιλεγμένους βάσει κλειδιού συντελεστές οριζόντιων λεπτομερειών του δεύτερου, τρίτου και τέταρτου επιπέδου ανάλυσης αντίστοιχα. Σε κάθε ένα από αυτά αντιστοιχούσε ένα υδατογράφημα αναφοράς, το οποίο ενσωματώθηκε στους χωρικά αντιστοιχούς συντελεστές κάθετων λεπτομερειών του ίδιου επιπέδου ανάλυσης. Τα υδατογραφήματα αναφοράς αποτελούσαν στην πράξη επαναλαμβανόμενες εκδοχές μιας αρχικής ακολουθίας bits, όσες χρειαζόντουσαν προκειμένου να καλυφθούν όλοι οι προς υδατογράφιση συντελεστές. Το υδατογράφημα αναφοράς ενσωματώθηκε επίσης σε συντελεστές κάθετων λεπτομερειών του πρώτου επιπέδου ανάλυσης, επιτρέποντας έτσι καθολική αποτίμηση και ανίχνευση τυχόν αλλοίωσης στο σύνολο της εικόνας. Και σε αυτήν την έκδοση του υδατογραφικού σχήματος λήφθηκε υπόψη η «δυναμική ρητή μορφή» των συντελεστών κυματιδίων Haar και η μειωμένη ευαισθησία του ματιού στο θόρυβο σε ζώνες υψηλής ανάλυσης (resolution), οπότε και πάλι επιλέχθηκε η παράμετρος κβαντοποίησης Δ που δίνεται από την Εξίσωση (7.4).

Αποτελέσματα

Ο αλγόριθμος δοκιμάστηκε σε ένα σύνολο 100 εικόνων υπερήχων, μεγέθους 256x320 pixels, που συλλέχθηκαν από τον ίδιο γιατρό, με τον ίδιο εξοπλισμό και τις ίδιες ρυθμίσεις συστήματος, προκειμένου να επιτευχθούν κοινά στατιστικά χαρακτηριστικά στο σύνολο των εικόνων. Στις δοκιμές που έγιναν, χρησιμοποιήθηκαν 6 λέξεις-κλειδιά συνολικού πλήθους 55 χαρακτήρων, ενώ τα δεδομένα ασθενή αποτελούνταν από 10 λέξεις, 87 χαρακτήρων συνολικά. Δεδομένου ότι η κωδικοποίηση κατά ASCII αναθέτει 8 bits ανά χαρακτήρα, τα υδατογραφήματα που προέκυψαν από αυτά τα κείμενα ήταν μήκους 440 και 696 bits αντίστοιχα. Οι τυχαίες ακολουθίες bits που απαρτίζουν το εύθραυστο και το ανθεκτικό υδατογράφημα επιλέχθηκαν να είναι μήκους 1024 και 128 bits αντίστοιχα.

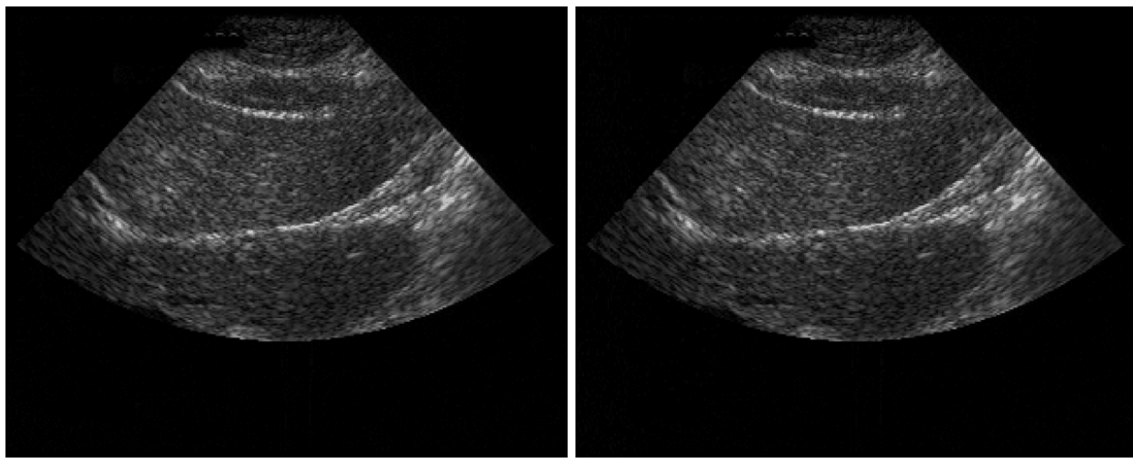
Δεδομένου ότι τα τρία υδατογραφήματα αναφοράς που εισάγονται έχουν το ίδιο πλήθος bits με τα υδατογραφήματα (ανθεκτικό, δείκτη, επικεφαλίδας) που τους αντιστοιχούν, το συνολικό μήκος των υδατογραφημάτων που ενσωματώθηκαν ήταν 3.552 bits.



(α)

(β)

Σχήμα 22: (α) Αρχική εικόνα υπερήχων. (β) Αντίστοιχη υδατογραφημένη εικόνα.



(α)

(β)

Σχήμα 23: (α) Αρχική εικόνα υπερήχων. (β) Αντίστοιχη υδατογραφημένη εικόνα.

Λόγω των αυστηρών απαιτήσεων όσον αφορά τις επιτρεπτές μεταβολές στις ιατρικές εικόνες, έγινε αποτίμηση της ποιότητας τόσο από άποψη σήματος, όσο και από άποψη οπτικού αποτελέσματος. Το αντικειμενικό κριτήριο που χρησιμοποιήθηκε για την αποτίμηση της ποιότητας ήταν και πάλι ο σηματοθορυβικός λόγος PSNR (Εξίσωση 7.1). Οι δοκιμές κατέληξαν σε μια μέση τιμή για το PSNR ίση με 51,25 dB, με τυπική απόκλιση 0,48 dB. Ο γιατρός που αξιολόγησε

την ποιότητα (perceptual quality) των υδατογραφημένων εικόνων, δεν παρατήρησε διαφορά ανάμεσα σε αυτές και τις αντίστοιχες αρχικές εικόνες. Στα Σχήματα 22 και 23 φαίνονται δύο εικόνες υπερήχων και οι αντίστοιχες υδατογραφημένες εικόνες που προέκυψαν με εφαρμογή αυτής της έκδοσης του υδατογραφικού σχήματος.

Ο Πίνακας 24 παρουσιάζει μια συγκριτική αποτίμηση της αλλοίωσης που προκαλείται στις εικόνες από το υδατογραφικό σχήμα σε σχέση με την αλλοίωση που προκύπτει από τη συμπίεσή τους με διαφορετικό συντελεστή ποιότητας (quality factor). Όπως φαίνεται και στον πίνακα, η υδατογραφική μέθοδος προκαλεί μικρότερη αλλοίωση από ό,τι η συμπίεση JPEG με συντελεστή ποιότητας 95. Ο συνδυασμός ικανοποιητικής οπτικής ποιότητας και μεγάλης τιμής PSNR για τις υδατογραφημένες εικόνες, επιβεβαίωσε την ικανοποιητική απόδοση της συγκεκριμένης έκδοσης του σχήματος ως προς τη διαφάνεια των υδατογραφημάτων.

Είδος Επεξεργασίας Εικόνας	PSNR (dB)
Υδατογράφιση	51.25 ± 0.48
JPEG 95	44.67 ± 0.58
JPEG 90	39.84 ± 0.90
JPEG 85	37.17 ± 1.06
JPEG 80	35.42 ± 1.17
JPEG 75	34.11 ± 1.25

Πίνακας 24: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων υπερήχων ως προς το PSNR

7.2.6.3 Ενσωμάτωση τεσσάρων τύπων υδατογραφημάτων με επιλογή Περιοχής Ενδιαφέροντος

Η τρίτη υλοποίηση του αλγορίθμου [17] περιλαμβάνει επίσης την ενσωμάτωση τεσσάρων υδατογραφημάτων στην εικόνα, δηλαδή των υδατογραφημάτων υπογραφής, δείκτη, επικεφαλίδας και αναφοράς, λαμβάνοντας όμως υπόψη τις περιοχές υψηλής διαγνωστικής αξίας. Πιο συγκεκριμένα, ορίζεται στην εικόνα μια Περιοχή Ενδιαφέροντος (ROI), στην οποία ενσωματώνεται μόνο το

υδατογράφημα αναφοράς προκειμένου να επιτρέψει τον έλεγχο της ακεραιότητας της περιοχής, ενώ τα άλλα τρία υδατογραφήματα εισάγονται στην υπόλοιπη εικόνα, που δεν είναι κρίσιμη από άποψη διαγνωστικής αξίας. Με αυτόν τον τρόπο ικανοποιούνται οι αυστηροί περιορισμοί ως προς την αλλοίωση των εικόνων και αποφεύγεται ο οποιοσδήποτε συμβιβασμός όσον αφορά την ποιότητά τους, που θα μπορούσε να οδηγήσει σε λανθασμένη διάγνωση και ακατάλληλη θεραπευτική αγωγή.

Περιγραφή υλοποίησης

Η εικόνα αναλύεται σε τέσσερα επίπεδα με χρήση του Διακριτού Μετασχηματισμού Κυματιδίων Haar. Λαμβάνοντας υπόψη ότι η ανθεκτικότητα αυξάνεται ενώ η χωρητικότητα μειώνεται στα υψηλότερα επίπεδα ανάλυσης, τα υδατογραφήματα επικεφαλίδας, δείκτη και υπογραφής ενσωματώνονται σε συντελεστές κυματιδίων εκτός περιοχής ενδιαφέροντος (ROI) του δεύτερου, τρίτου και τέταρτου επιπέδου αντίστοιχα. Το υδατογράφημα αναφοράς ενσωματώνεται σε συντελεστές που αντιστοιχούν σε όλη την εικόνα, επιτρέποντας με αυτόν τον τρόπο καθολικό έλεγχο της εικόνας και αποτίμηση όλων των αλλοιώσεων. Η επιλογή των συντελεστών στους οποίους ενσωματώνονται τα υδατογραφήματα γίνεται με βάση την τιμή ενός κλειδιού και τον Πίνακα Περιοχής Ενδιαφέροντος (ROI map). Το κλειδί καθορίζει εάν ένας συγκεκριμένος συντελεστής θα φέρει bit από το υδατογράφημα αναφοράς ή από το υδατογράφημα δεδομένων (υπογραφή, δείκτης, επικεφαλίδα). Στην περίπτωση των υδατογραφημάτων δεδομένων, ο συντελεστής τελικά θα χρησιμοποιηθεί για ενσωμάτωση ενός bit μόνο εάν δεν ανήκει στην περιοχή ενδιαφέροντος.

Μια οποιαδήποτε μεταβολή σε ένα συγκεκριμένο τμήμα της εικόνας εκτός της περιοχής ROI είναι πολύ πιθανό να επηρεάσει τόσο τα υδατογραφήματα δεδομένων όσο και το υδατογράφημα αναφοράς που έχουν ενσωματωθεί εκεί. Συνεπώς, η σύγκριση μεταξύ του εξαχθέντος υδατογραφήματος αναφοράς και του αρχικού παρέχει μια ενδεικτική εικόνα της αλλοίωσης των σημείων που χρησιμοποιήθηκαν για εισαγωγή δεδομένων. Επιπλέον, το γεγονός ότι το

υδατογράφημα αναφοράς ενσωματώνεται και στην περιοχή ROI επιτρέπει έναν καθολικό έλεγχο ακεραιότητας.

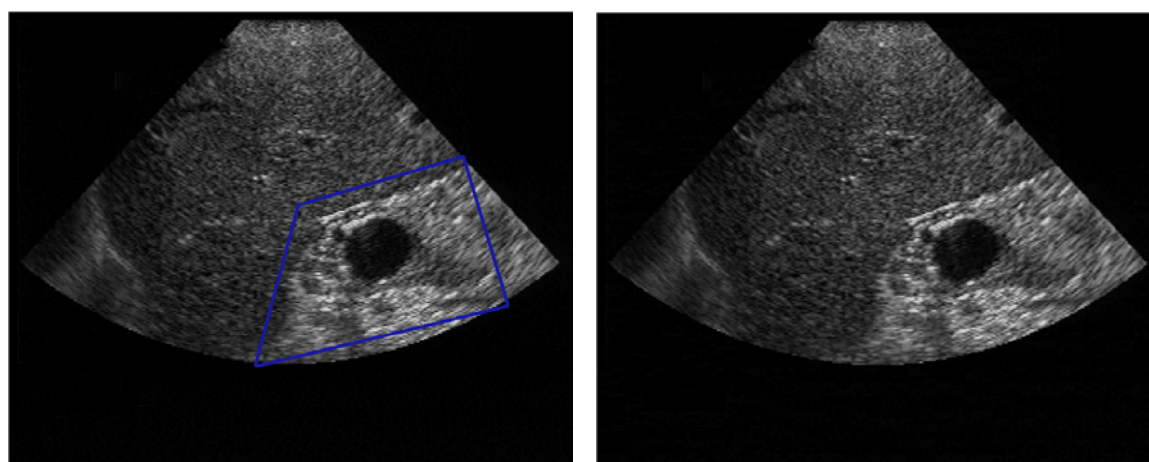
Για τον έλεγχο της αποδοτικότητας της συγκεκριμένης έκδοσης του υδατογραφικού σχήματος χρησιμοποιήθηκαν εικόνες υπερήχων, οι οποίες συγκεντρώνουν ένα σημαντικό μέρος της ενέργειας στη ζώνη των οριζόντιων λεπτομερειών σε σύγκριση με τις κάθετες και διαγώνιες. Η συγκέντρωση σημαντικής ενέργειας στη συγκεκριμένη ζώνη συνεπάγεται μεγαλύτερη ανθεκτικότητα των υδατογραφημάτων όσον αφορά επιθέσεις όπως η κοινή επεξεργασία εικόνων ή η συμπίεση, γι' αυτό το προτεινόμενο σχήμα ενσωματώνει τα υδατογραφήματα στην *οριζόντια ζώνη λεπτομερειών*. Οι συντελεστές του πρώτου επιπέδου ανάλυσης χρησιμοποιούνται μόνο για ενσωμάτωση του υδατογραφήματος αναφοράς εξαιτίας της μικρής τους επιρροής στην ποιότητα της εικόνας, χαρακτηριστικό που τους καθιστά ευάλωτους σε οποιοδήποτε είδος επεξεργασίας εικόνας.

Αποτελέσματα

Το σύνολο των εικόνων που χρησιμοποιήθηκαν για τις δοκιμές αποτελείται από 50 εικόνες υπερήχων μεγέθους 256x320 pixels, που συλλέχθηκαν από τον ίδιο γιατρό, με τον ίδιο εξοπλισμό και τις ίδιες ρυθμίσεις του συστήματος υπερήχων, με στόχο να αποφευχθούν οι αποκλίσεις στις στατιστικές κατανομές των εικόνων. Το υδατογράφημα αναφοράς παράχθηκε από μια γεννήτρια τυχαίων αριθμών ομοιόμορφης κατανομής. Τα υδατογραφήματα επικεφαλίδας και δείκτη ήταν δυαδικές ακολουθίες που προέκυψαν από την ASCII κωδικοποίηση αρχείων κειμένου και στις συγκεκριμένες δοκιμές είχαν μήκος ίσο με 696 και 440 bits αντίστοιχα. Ως υδατογράφημα υπογραφής χρησιμοποιήθηκε μια δυαδική ακολουθία 128 bits που δημιουργήθηκε τυχαία με ομοιόμορφη κατανομή πιθανότητας, ενώ η παράμετρος κβαντοποίησης Δ επιλέχτηκε να είναι ίση με $\Delta = 2^l$, όπου l το επίπεδο ανάλυσης.

Στο Σχήμα 24 παρουσιάζεται μια εικόνα υπερήχων στην οποία έχει οριστεί μια Περιοχή Ενδιαφέροντος και η αντίστοιχη υδατογραφημένη εικόνα που προέκυψε με την εφαρμογή αυτής της έκδοσης του υδατογραφικού σχήματος. Η ποιότητα των

υδατογραφημένων εικόνων αξιολογήθηκε από γιατρό, ο οποίος δε βρήκε σημαντικές διαφορές μεταξύ αυτών και των αρχικών εικόνων. Αυτή η άποψη ενισχύθηκε και από το σηματοθορυβικό λόγο PSNR (Εξίσωση 7.1) το οποίο είχε τιμή ίση με 46,66 dB και τυπική απόκλιση 0,24 dB. Όπως φαίνεται και από τον Πίνακα 25, στον οποίο παρουσιάζεται μια συγκριτική εκτίμηση των αλλοιώσεων που εισάγονται σε μια εικόνα από τη συγκεκριμένη υδατογράφιση και από τη συμπίεση JPEG με διάφορους συντελεστές ποιότητας, η μέθοδος προκαλεί μικρότερη αλλοίωση ακόμα και από τη συμπίεση με συντελεστή ποιότητας 95.



Σχήμα 24: (α) Αρχική εικόνα υπερήχων με Περιοχή Ενδιαφέροντος. (β) Αντίστοιχη υδατογραφημένη εικόνα.

Είδος Επεξεργασίας Εικόνας	PSNR (dB)
Υδατογράφιση	46.66 ± 0.24
JPEG 95	44.71 ± 0.51
JPEG 90	40.00 ± 0.77
JPEG 85	37.37 ± 0.91
JPEG 80	35.65 ± 1.01
JPEG 75	34.37 ± 1.09

Πίνακας 25: Απόδοση υδατογραφημένων και συμπιεσμένων κατά JPEG εικόνων υπερήχων ως προς το PSNR

Η επίδραση της συμπίεσης JPEG με διάφορους συντελεστές ποιότητας στις υδατογραφημένες εικόνες MRA απεικονίζεται στον Πίνακα 26. Η Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance) που ορίζεται στην Εξίσωση 7.3 χρησιμοποιήθηκε και σε αυτήν την περίπτωση ως κριτήριο ομοιότητας για την αποτίμηση του βαθμού αλλοίωσης των εικόνων.

Συντελεστής Ποιότητας Συμπίεσης JPEG Υδατογρ/νων Εικόνων	Κανονικοποιημένη Απόσταση Hamming (Normalized Hamming Distance)			
	1 ^ο Επίπεδο Ανάλυσης	2 ^ο Επίπεδο Ανάλυσης	3 ^ο Επίπεδο Ανάλυσης	4 ^ο Επίπεδο Ανάλυσης
95	0.48 ± 0.01	0.20 ± 0.04	0.11 ± 0.04	0.09 ± 0.04
90	0.49 ± 0.01	0.31 ± 0.03	0.16 ± 0.03	0.13 ± 0.05
85	0.49 ± 0.01	0.39 ± 0.02	0.26 ± 0.03	0.17 ± 0.05
80	0.50 ± 0.01	0.44 ± 0.01	0.28 ± 0.03	0.21 ± 0.06
75	0.50 ± 0.01	0.47 ± 0.01	0.30 ± 0.03	0.28 ± 0.06

Πίνακας 26: Κανονικοποιημένη απόσταση Hamming ως συνάρτηση του συντελεστή ποιότητας JPEG (εικόνες υπερήχων)

Από τον παραπάνω πίνακα προκύπτει και πάλι το συμπέρασμα ότι η τιμή της Κανονικοποιημένης Απόστασης Hamming αυξάνεται κατά τη μείωση του συντελεστή ποιότητας της συμπίεσης JPEG. Διαπιστώνεται επίσης η μείωση της τιμής της στα υψηλά επίπεδα ανάλυσης, γεγονός που φανερώνει την αυξημένη ανθεκτικότητα των επιπέδων αυτών σε τροποποιήσεις των εικόνων.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

- [1] S. Lu, H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Proc.*, vol. 10, no. 10, pp. 1579-1592, Oct. 2001.
- [2] A. H. Paquet, R. K. Ward, "Wavelet-based digital watermarking for image authentication," in *Proc. IEEE Canadian Conf. Electrical and Computer Engineering, CCECE 2002*, Winnipeg, Canada, vol. 2, pp. 879 – 884, May 2002.
- [3] S. Zinger, Z. Jin, H. Maitre, and B. Sankur, "Optimization of watermarking performances using error correcting codes and repetition", in *Proc. Joint Conf. Commun. and Mult. Security Issues of the New Century*, Darmstadt, Germany, pp. 229-240, 2001.
- [4] A. Bruckmann, A. Uhl, "Selective medical image compression using wavelet techniques," *J. Computing and Information Technology Special Issue on Biomedical Image Processing and Analysis*, vol. 6, no. 2, pp. 203-213, 1998.
- [5] Kutter, F. A. P. Petitcolas, "A fair benchmark for image watermarking systems," in *Proc. SPIE Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, San Jose, CA, USA, vol. 3657, pp. 226-239, Jan. 1999.
- [6] M. Kutter, F. Hartung, "Introduction to watermarking techniques," in *Information Hiding Techniques for Steganography and Digital Watermarking*, S. Katzenbeisser, F. A. P. Petitcolas, Eds. Norwood: Artech House Inc., 2000, pp. 97-120.
- [7] S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun, "Attack modelling: towards a second generation watermarking benchmark," *Signal Processing*, vol. 81, no.6, pp. 1177-1214, June 2001.
- [8] S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Proc. Intern. Workshop on Information Hiding*, Dresden, Germany, Sept. 29 -Oct. 1, 1999, pp. 211-236.
- [9] H. M. Chao, C. M. Hsu, S. G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Trans. Inf. Technol. Biomed.*, vol. 6, no. 1, pp. 46-53, March 2002.
- [10] G. Miaou, C. M. Hsu, Y. S. Tsai, H. M. Chao, "A secure data hiding technique with heterogeneous data combining capability for electronic patient records," in *Proc.*

- 22nd Annu. Intern. Conf. IEEE Engineering in Medicine and Biology Society, EMBC'00, Chicago, USA, vol. 1, pp. 280-283.
- [11] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple Image Watermarking Applied to Health Information Management", *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. 722-732, Oct. 2006.
- [12] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images", *Medical & Biological Engineering & Computing*, vol. 44, no. 8, pp. 619-631, Springer Berlin / Heidelberg, August 2006. Available: <http://dx.doi.org/10.1007/s11517-006-0081-x>
- [13] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Health Data Management through Multiple Watermarking of Medical Images", in IFMBE Proc. 3rd European Medical and Biological Engineering Conf., EMBEC'05, vol. 11, pp. 3093-3096, Prague, Czech Republic, November 20-25, 2005.
- [14] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "A Medical Image Watermarking Scheme Based on Wavelet Transform", *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS)*, pp. 856-859, Cancun, Mexico, September 17-21, 2003.
- [15] D. Kundur, D. Hatzinakos, "Improved robust watermarking through attack characterization," *Optics Express*, vol. 3 no. 12, pp. 485-490, Dec. 1998.
- [16] B. S. Kim, K. K. Kwon, S. G. Kwon, K. N. Park, K. I. Song, K. I. Lee, "A robust wavelet-based digital watermarking using statistical characteristic of image and human visual system," in *Proc. 17th Intern. Conf. Circuits Systems Computers and Communications, ITC-CSCC2002*, Phuket, Thailand, pp. 1019-1022.
- [17] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "A Multiple Watermarking Scheme Applied to Medical Image Management", *Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS)*, pp. 3241-3244, San Francisco, CA, USA, September 1-5, 2004.

ΚΕΦΑΛΑΙΟ 8

ΓΡΑΦΙΚΗ ΔΙΑΠΡΟΣΩΠΕΙΑ ΤΗΣ ΕΦΑΡΜΟΓΗΣ

8.1 ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό παρουσιάζονται οι γραφικές διαπροσωπείες που αποτυπώνουν τη λειτουργικότητα του υδατογραφικού συστήματος που αναπτύχθηκε στα πλαίσια της διατριβής. Συγκεκριμένα παρουσιάζονται οι γραφικές διαπροσωπείες που δίνουν τη δυνατότητα εισαγωγής και εξαγωγής πολλαπλών υδατογραφημάτων από ιατρικές εικόνες και περιγράφονται οι επιλογές που παρέχονται στο χρήστη του συστήματος. Η εφαρμογή αναπτύχθηκε με χρήση του προγραμματιστικού περιβάλλοντος του Matlab 7 και των εργαλειοθηκών Επεξεργασίας Εικόνας, Κυματιδίων, και Μετάδοσης που διαθέτει. Οι γραφικές διαπροσωπείες της εφαρμογής δημιουργήθηκαν με χρήση του Guide (graphical user interface development environment), που αποτελεί το περιβάλλον ανάπτυξης γραφικών διαπροσωπειών χρήστη του Matlab.

8.2 ΓΡΑΦΙΚΗ ΔΙΑΠΡΟΣΩΠΕΙΑ ΕΙΣΑΓΩΓΗΣ ΚΑΙ ΕΞΑΓΩΓΗΣ ΥΔΑΤΟΓΡΑΦΗΜΑΤΩΝ

Όταν ο χρήστης επιλέξει να υδατογραφήσει μια εικόνα, καλείται από το υδατογραφικό σύστημα να κάνει τις ακόλουθες ενέργειες:

α) να εισαγάγει όνομα χρήστη (username) και κωδικό (password) για την πιστοποίησή του

β) να επιλέξει την προς υδατογράφιση εικόνα

γ) να καθορίσει τις επιλογές του ως προς τις παραμέτρους ενσωμάτωσης των υδατογραφημάτων και πιο συγκεκριμένα:

- Να επιλέξει εάν θα οριστεί μια Περιοχή Ενδιαφέροντος και εάν ναι, για ποιο σκοπό (εάν δηλαδή θα εξαιρεθεί η περιοχή από τη διαδικασία υδατογράφισης ή θα ενσωματωθεί σε αυτήν το υδατογράφημα αναφοράς για έλεγχο ακεραιότητας)
- Να επιλέξει εάν θα εφαρμοστεί κωδικοποίηση διόρθωσης σφαλμάτων (ECC- error correction coding) σε υδατογραφήματα που φέρουν την πρόσθετη πληροφορία (υπογραφή, δείκτης, επικεφαλίδα) και εάν ναι, σε ποια
- Να καθορίσει το κλειδί που θα χρησιμοποιηθεί για την εισαγωγή των υδατογραφημάτων είτε επιλέγοντάς το από μια λίστα κλειδιών αποθηκευμένη στη βάση, είτε εισάγοντας καινούριο
- Να επιλέξει ποιους από τους διαθέσιμους τύπους υδατογραφημάτων επιθυμεί να ενσωματώσει στην εικόνα
- Να ορίσει την πληροφορία που θα περικλείει καθένα από υδατογραφήματα που θα εισαχθούν στην εικόνα

Όταν ο χρήστης επιλέξει να εξαγάγει τα υδατογραφήματα που έχουν ενσωματωθεί σε μια εικόνα, καλείται μέσω της γραφικής διαπροσωπείας του συστήματος να κάνει τις ακόλουθες ενέργειες:

α) να εισαγάγει όνομα χρήστη (username) και κωδικό (password) για την πιστοποίησή του

β) να επιλέξει την υδατογραφημένη εικόνα από την οποία επιθυμεί να εξαγάγει την ενσωματωμένη πληροφορία

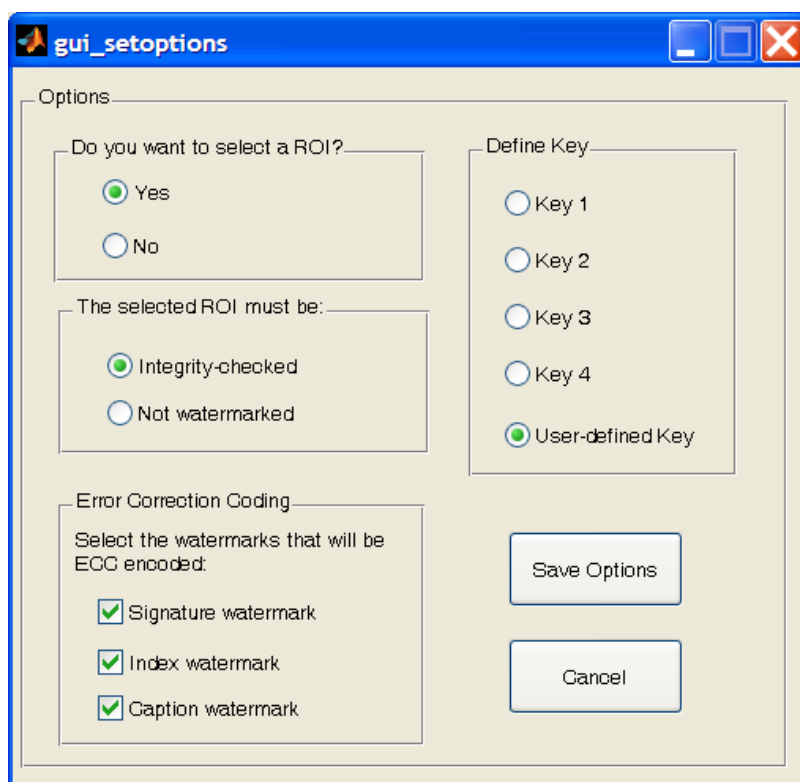
γ) να καθορίσει ποια από τα υδατογραφήματα πρόσθετης πληροφορίας (υπογραφή, δείκτης, επικεφαλίδα) επιθυμεί να εξαγάγει

- δ) να επιλέξει εάν επιθυμεί να ελέγξει την ακεραιότητα της εικόνας
- ε) στην περίπτωση που ανιχνευτεί παραποίηση της εικόνας, να επιλέξει εάν επιθυμεί τον εντοπισμό των αλλοιωμένων περιοχών της

Βάσει των παραπάνω, η εφαρμογή που επιτρέπει την υδατογράφιση των ιατρικών εικόνων απαρτίζεται από δύο φόρμες. Παρακάτω παρουσιάζονται οι φόρμες αυτές και περιγράφονται οι λειτουργίες τους και η αλληλεπίδραση του χρήστη με την εφαρμογή. Παρόμοια περιγραφή ακολουθεί τέλος και για τη φόρμα που αντιστοιχεί στην ανάκτηση της ενσωματωμένης πληροφορίας από μια υδατογραφημένη εικόνα.

8.2.1 Φόρμα Καθορισμού Επιλογών

Όταν ο χρήστης επιλέξει την εκτέλεση της εφαρμογής υδατογράφισης εικόνων, παρουσιάζεται στην οθόνη η φόρμα καθορισμού επιλογών που απεικονίζεται στο Σχήμα 25.



Σχήμα 25: Φόρμα καθορισμού επιλογών

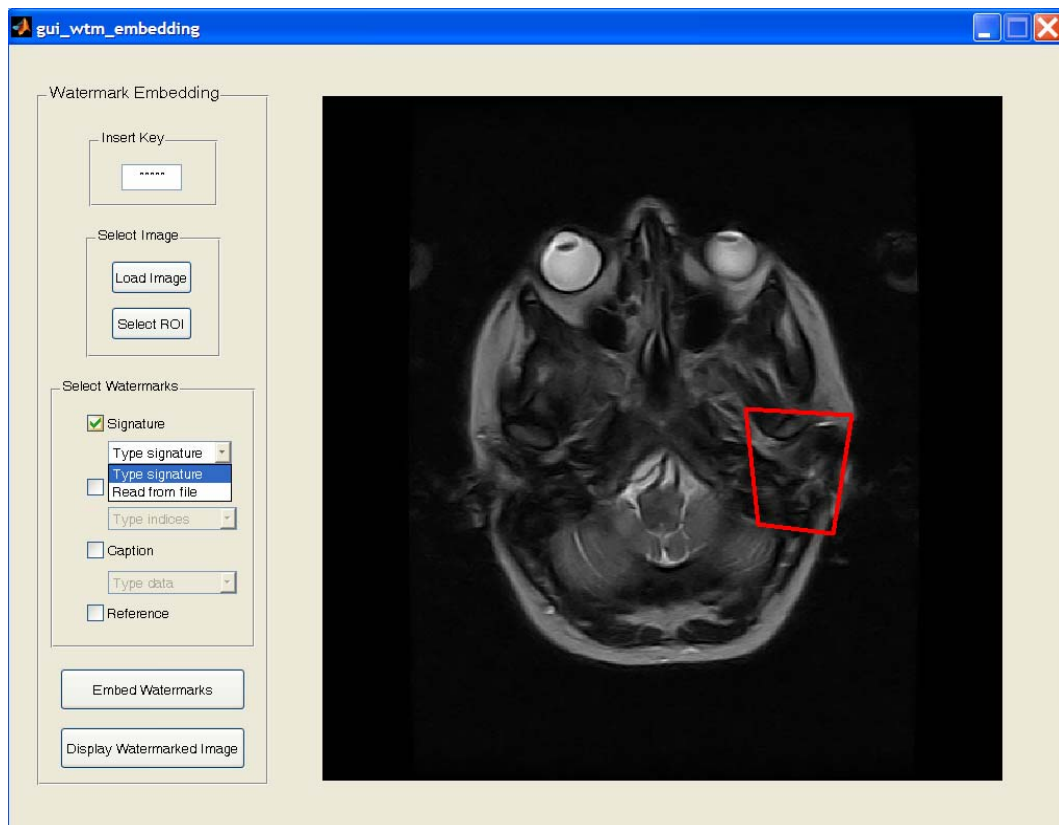
Στη φόρμα αυτή καλείται ο χρήστης να κάνει μια σειρά επιλογών, οι οποίες αποθηκεύονται στο σύστημα και καθορίζουν κάποιες βασικές παραμέτρους της διαδικασίας υδατογράφησης. Οι παράμετροι που καλείται ο χρήστης να καθορίσει είναι οι ακόλουθες:

- Εάν επιθυμεί να ορίσει μια Περιοχή Ενδιαφέροντος στην προς υδατογράφηση εικόνα.
- Σε περίπτωση που επιλέξει μια Περιοχή Ενδιαφέροντος, καλείται να επιλέξει εάν επιθυμεί να εξαιρεθεί η συγκεκριμένη περιοχή από τη διαδικασία της υδατογράφησης ή να ενσωματωθεί σε αυτήν το υδατογράφημα αναφοράς, προκειμένου να επιτραπεί στη συνέχεια ο έλεγχος της ακεραιότητάς της.
- Επιλέγει εάν και σε ποια από τα υδατογραφήματα που φέρουν την πρόσθετη πληροφορία (υπογραφή, δείκτης, επικεφαλίδα) θα εφαρμοστεί κωδικοποίηση διόρθωσης σφαλμάτων (error correction coding) για αυξημένη ανθεκτικότητα.
- Επιλέγει εάν θα χρησιμοποιηθεί για την υδατογράφηση κάποιο από τα κλειδιά που υπάρχουν ήδη αποθηκευμένα στο σύστημα ή κάποιο καινούριο κλειδί που θα οριστεί από το χρήστη στη συνέχεια.

8.2.2 Φόρμα Εισαγωγής Υδατογραφημάτων

Αφού ο χρήστης ορίσει τις επιλογές του, παρουσιάζεται στην οθόνη η φόρμα εισαγωγής υδατογραφημάτων που απεικονίζεται στο Σχήμα 26. Η φόρμα αυτή καλεί το χρήστη να καθορίσει τα εξής:

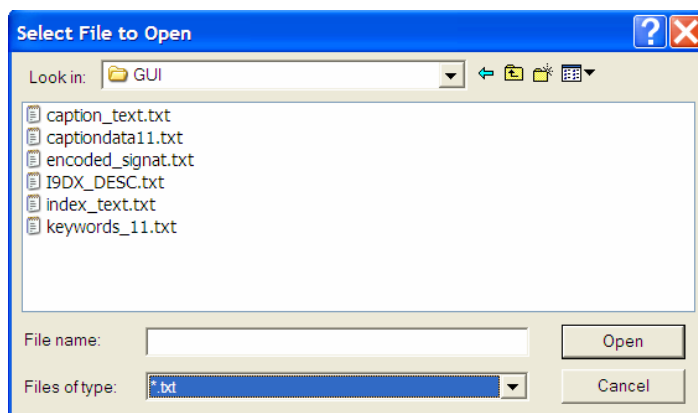
- Σε περίπτωση που ο χρήστης έχει επιλέξει στη Φόρμα Καθορισμού Επιλογών να χρησιμοποιηθεί για την ενσωμάτωση των υδατογραφημάτων στην εικόνα ένα διαφορετικό κλειδί από αυτά που είναι ήδη αποθηκευμένα στο σύστημα, καλείται να εισαγάγει το νέο κλειδί.
- Στη συνέχεια καλείται να επιλέξει την εικόνα που επιθυμεί να υδατογραφήσει.



Σχήμα 26: Φόρμα εισαγωγής υδατογραφημάτων

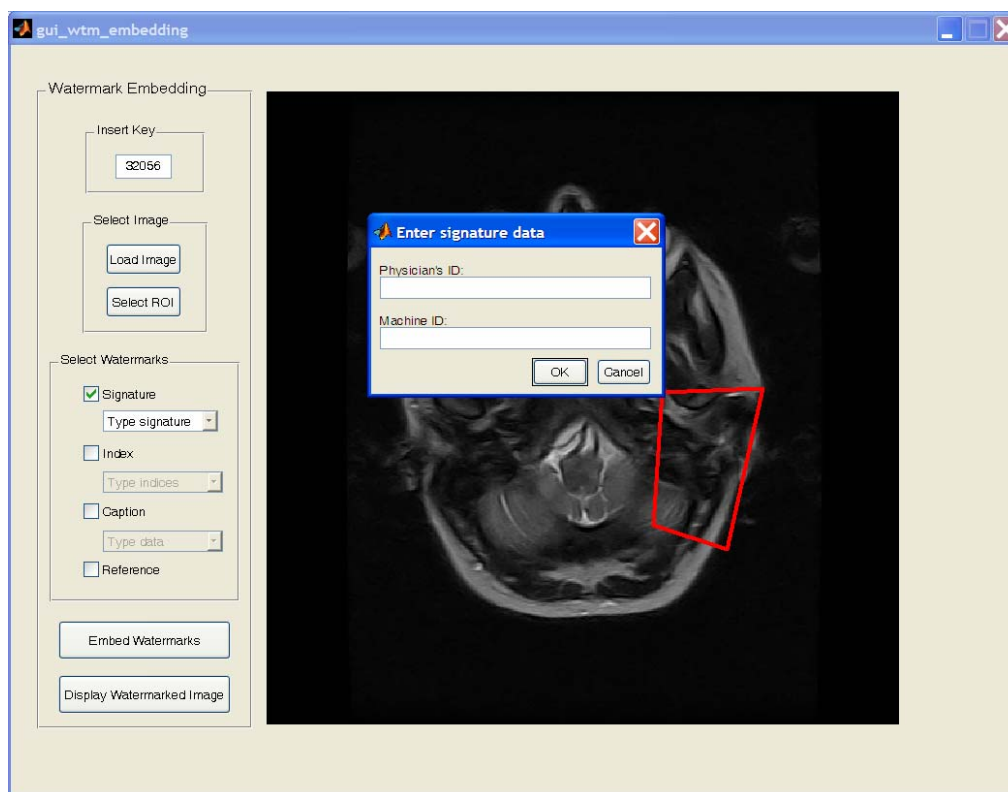
- Στην περίπτωση που έχει επιλέξει στη Φόρμα Καθορισμού Επιλογών τη χρήση Περιοχής Ενδιαφέροντος, καλείται να καθορίσει αυτήν την περιοχή πάνω στην εικόνα.
- Ακολουθεί η επιλογή των τύπων υδατογραφημάτων που θα ενσωματωθούν στην προς υδατογράφηση εικόνα. Για κάθε τύπο υδατογραφήματος που επιλέγεται – εκτός από το υδατογράφημα αναφοράς που είναι συγκεκριμένο και εκ των προτέρων γνωστό και στο σημείο εξαγωγής των υδατογραφημάτων – εμφανίζεται μια λίστα (pop-up list), στην οποία καλείται ο χρήστης να καθορίσει με ποιον τρόπο θα προσδιοριστούν τα προς ενσωμάτωση δεδομένα. Πιο συγκεκριμένα, για τους τρεις τύπους υδατογραφημάτων που φέρουν τα πρόσθετα δεδομένα (υπογραφή, δείκτης, επικεφαλίδα) οι αντίστοιχες επιλογές είναι οι ακόλουθες:
 - Υδατογράφημα υπογραφής: ο χρήστης επιλέγει εάν θα εισαγάγει ο ίδιος τα προς ενσωμάτωση δεδομένα ή θα γίνει η ανάγνωσή τους από κάποιο αρχείο κειμένου. Στο Σχήμα 27 φαίνεται το πλαίσιο διαλόγου (dialog box)

που καλεί το χρήστη να καθορίσει το αρχείο κειμένου από το οποίο θα διαβαστούν τα δεδομένα.



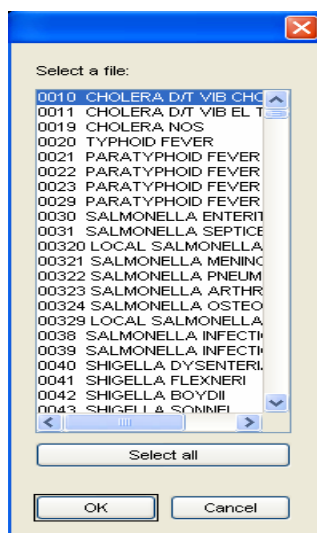
Σχήμα 27: Εισαγωγή δεδομένων για το υδατογράφημα υπογραφής από αρχείο κειμένου

Στο Σχήμα 28 παρουσιάζεται το πλαίσιο διαλόγου που εμφανίζεται όταν ο χρήστης επιλέξει την εισαγωγή δεδομένων από τον ίδιο και στο οποίο του ζητείται να εισαγάγει τον αναγνωριστικό κωδικό του ιδίου ή/και του μηχανήματος.



Σχήμα 28: Εισαγωγή δεδομένων για το υδατογράφημα υπογραφής από το χρήστη

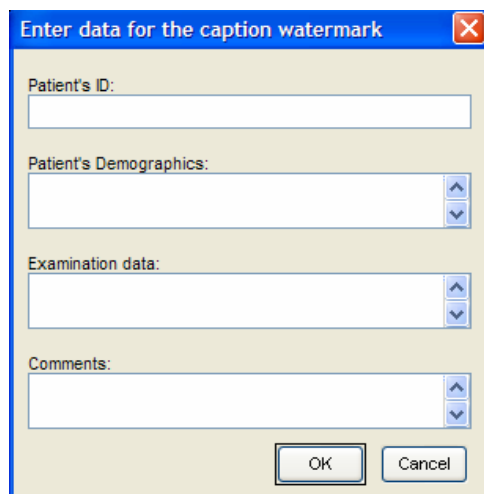
- *Υδατογράφημα δείκτη*: σε αυτήν την περίπτωση ο χρήστης καλείται να επιλέξει μεταξύ τριών τρόπων καθορισμού του προς υδατογράφιση κειμένου. Συγκεκριμένα, ο χρήστης έχει τη δυνατότητα να επιλέξει την εισαγωγή των δεδομένων από τον ίδιο, από ένα αρχείο κειμένου, ή από μια λίστα με κωδικούς ασθενειών κατά ICD9/10. Στις δύο πρώτες περιπτώσεις εμφανίζονται πλαίσια διαλόγου αντίστοιχα με αυτά των Σχημάτων 27 και 28, που αντιστοιχούν στην περίπτωση του υδατογραφήματος υπογραφής. Στο Σχήμα 29 φαίνεται το πλαίσιο διαλόγου που επιτρέπει στο χρήστη να επιλέξει δείκτες από τη λίστα ICD9/10.



Σχήμα 29: Επιλογή δεδομένων για το υδατογράφημα δείκτη από τη λίστα ICD9/10

- *Υδατογράφημα επικεφαλίδας*: ο χρήστης επιλέγει εάν θα εισαγάγει ο ίδιος τα προς ενσωμάτωση δεδομένα ή θα γίνει η ανάγνωσή τους από κάποιο αρχείο κειμένου. Στην περίπτωση που ο χρήστης επιλέξει να εισαγάγει ο ίδιος τα δεδομένα, εμφανίζεται στην οθόνη το πλαίσιο διαλόγου που απεικονίζεται στο Σχήμα 30. Ο χρήστης έχει τη δυνατότητα να επιλέξει ποια από τα πεδία του πλαισίου διαλόγου θα συμπληρώσει, τα οποία περιλαμβάνουν: τον αναγνωριστικό κωδικό του ασθενή, δημογραφικά στοιχεία του, στοιχεία για την εξέταση και πρόσθετα σχόλια. Το πλαίσιο διαλόγου που καλεί το χρήστη να καθορίσει το αρχείο κειμένου από το

οποίο θα διαβαστούν τα δεδομένα που θα ενσωματωθούν στο υδατογράφημα επικεφαλίδας είναι αντίστοιχο με αυτό του Σχήματος 27.



Σχήμα 30: Εισαγωγή δεδομένων για το υδατογράφημα επικεφαλίδας από το χρήστη

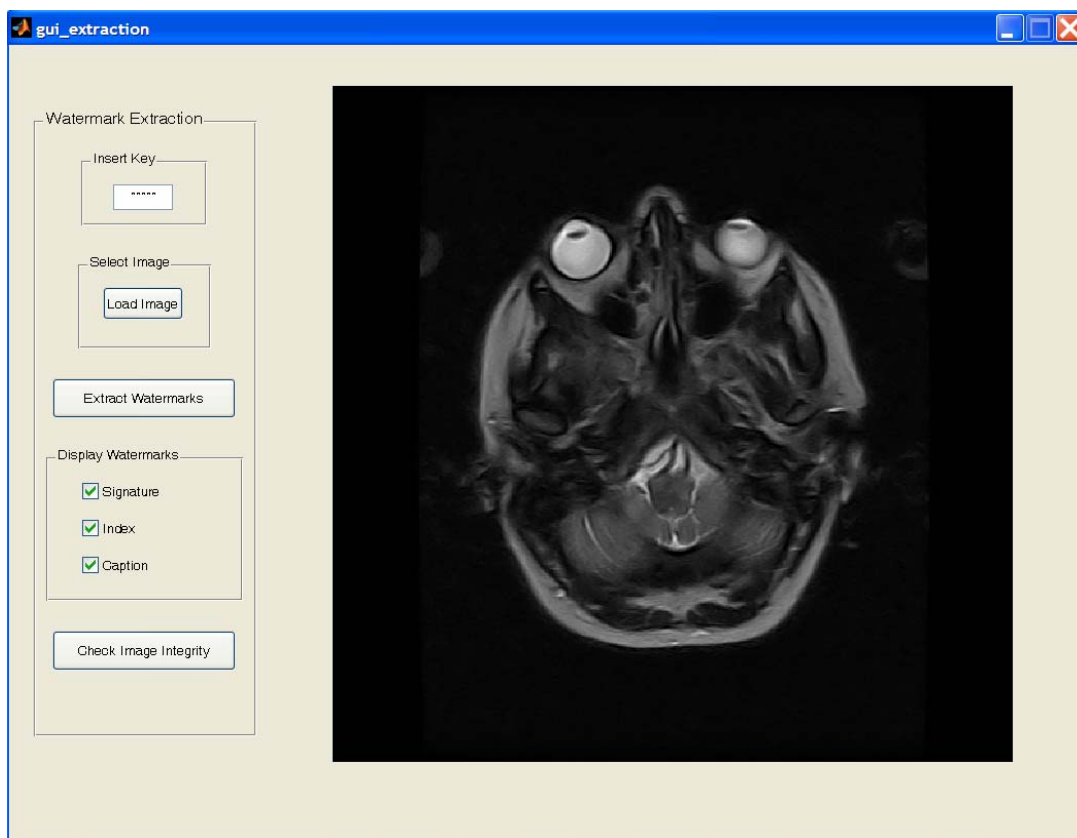
- Αφού έχουν οριστεί τα δεδομένα που θα ενσωματωθούν την εικόνα μέσω των υδατογραφημάτων, ο χρήστης ενεργοποιεί τη διαδικασία υδατογράφησης.
- Μετά το πέρας της διαδικασίας, ο χρήστης μπορεί να επιλέξει την εμφάνιση της υδατογραφημένης εικόνας σε ένα νέο παράθυρο, προκειμένου να τη συγκρίνει με την αρχική εικόνα.

8.2.3 Φόρμα Εξαγωγής Υδατογραφημάτων

Όταν ο χρήστης επιλέξει την εκτέλεση της εφαρμογής εξαγωγής των υδατογραφημάτων, παρουσιάζεται στην οθόνη η φόρμα εξαγωγής υδατογραφημάτων που φαίνεται στο Σχήμα 31. Η φόρμα αυτή προτρέπει το χρήστη να κάνει μια σειρά ενεργειών:

- Να εισαγάγει το κατάλληλο κλειδί για την εξαγωγή των υδατογραφημάτων
- Να επιλέξει την εικόνα από την οποία επιθυμεί να εξαγάγει τα υδατογραφήματα
- Να ενεργοποιήσει τη διαδικασία εξαγωγής των υδατογραφημάτων

- Να επιλέξει τα υδατογραφήματα των οποίων η πληροφορία θα εμφανιστεί στην οθόνη
- Να ελέγξει την ακεραιότητα της υδατογραφημένης εικόνας. Σε περίπτωση που ανιχνευτεί κάποια αλλοίωση, το σύστημα εμφανίζει τις παραποιημένες περιοχές της εικόνας.



Σχήμα 31: Φόρμα εξαγωγής υδατογραφημάτων

Όπως προαναφέρθηκε, η τρέχουσα υλοποίηση της γραφικής διαπροσωπείας της εφαρμογής έχει αναπτυχθεί στο προγραμματιστικό περιβάλλον Matlab και έχει στόχο την ανάδειξη της λειτουργικότητας που παρέχεται από το σύστημα μέσω της φιλικής για το χρήστη γραφικής διαπροσωπείας. Αναμένεται πάντως ότι η υλοποίηση της γραφικής διαπροσωπείας με χρήση Microsoft .NET Framework (v2.0) θα βελτιώσει τη λειτουργικότητα της εφαρμογής και θα διευκολύνει την ολοκλήρωσή της σε συστήματα διαχείρισης ιατρικών εικόνων [1].

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

- [1] A. Giakoumaki, A. Tagaris, D. Koutsouris, "Implementation of a user-friendly GUI for a multiple image watermarking tool addressing healthcare applications", to appear in *Proc. 2006 IEEE EMBS International Conference on Information Technology Applications in Biomedicine (ITAB 2006)*, Ioannina, Greece, October 26-28, 2006.

ΚΕΦΑΛΑΙΟ 9

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΣΥΖΗΤΗΣΗ - ΠΡΟΟΠΤΙΚΕΣ

9.1 ΕΙΣΑΓΩΓΗ

Στο παρόν κεφάλαιο παρουσιάζονται τα συμπεράσματα και η αξιολόγηση της διατριβής ως προς την καινοτομία της και τη συνεισφορά της στον τομέα της ασφάλειας και της αποδοτικής διαχείρισης ιατρικής πληροφορίας.

Στην επόμενη ενότητα γίνεται συνοπτική παρουσίαση της ερευνητικής εργασίας που πραγματοποιήθηκε στα πλαίσια της διδακτορικής διατριβής και αποτίμηση των αποτελεσμάτων σε σχέση με τους αρχικούς στόχους. Στη συνέχεια γίνεται αξιολόγηση του προτεινόμενου συστήματος ως προς την καινοτομία του και τη συνεισφορά του στην ιατρική πληροφορική. Ακολουθεί η παρουσίαση των μελλοντικών προοπτικών του συστήματος και παρουσιάζονται τα ανοικτά θέματα και οι προτάσεις για μελλοντικές επεκτάσεις και βελτιώσεις του.

9.2 ΣΥΝΟΨΗ ΕΡΕΥΝΗΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Στόχος της ερευνητικής εργασίας που πραγματοποιήθηκε στα πλαίσια της παρούσας διδακτορικής διατριβής ήταν η διερεύνηση των προοπτικών της ψηφιακής υδατογραφίας στον τομέα της ασφαλούς και αποδοτικής διαχείρισης της πληροφορίας σε συστήματα υπηρεσιών υγείας. Η ερευνητική εργασία

επικεντρώθηκε στη σχεδίαση και υλοποίηση ενός υδατογραφικού συστήματος, με στόχο την παροχή συμπληρωματικών ή / και εναλλακτικών λύσεων σε μια σειρά κρίσιμων θεμάτων που αφορούν τα συστήματα διαχείρισης ιατρικής πληροφορίας, λαμβάνοντας υπόψη τις ιδιαίτερες απαιτήσεις και τα χαρακτηριστικά που διέπουν τις ιατρικές εικόνες. Προκειμένου να διερευνηθούν αποτελεσματικά οι προοπτικές της ψηφιακής υδατογραφίας στον τομέα της ιατρικής πληροφορικής, πραγματοποιήθηκε εκτενής μελέτη των εφαρμογών στις οποίες έχει μέχρι σήμερα αξιοποιηθεί η συγκεκριμένη τεχνολογία, καθώς και των βασικών υδατογραφικών τεχνικών που έχουν προταθεί στη βιβλιογραφία. Η μελέτη εστιάστηκε στη συνέχεια στις ερευνητικές προσπάθειες που έχουν ήδη καταγραφεί όσον αφορά την εφαρμογή υδατογραφικών τεχνικών σε ιατρικά δεδομένα. Αξίζει να σημειωθεί ότι ενώ πριν από μερικά χρόνια η σχετική αρθρογραφία ήταν εξαιρετικά περιορισμένη, την τελευταία πενταετία εμπλουτίζεται συνεχώς, γεγονός που φανερώνει τη δυναμική της εν λόγω τεχνολογίας στο συγκεκριμένο πεδίο [1]-[25].

Στη συνέχεια η ερευνητική προσπάθεια επικεντρώθηκε στη σχεδίαση και ανάπτυξη ενός υδατογραφικού σχήματος που θα ανταποκρίνεται στις ιδιαίτερες απαιτήσεις των ιατρικών εικόνων, ενώ παράλληλα θα αναδειξεί και θα αξιοποιήσει τις δυνατότητες που προσφέρει η υδατογραφία σε πληθώρα εφαρμογών που εμπίπτουν στο πεδίο της διαχείρισης ιατρικής πληροφορίας. Η σχεδίαση του υδατογραφικού σχήματος έγινε με γνώμονα δύο βασικές επιδιώξεις, συγκεκριμένα τη βελτίωση της ασφάλειας σε ιατρικά πληροφοριακά συστήματα και την αποδοτικότερη διαχείριση της πληροφορίας που διακινείται στα συστήματα αυτά. Το θέμα της ασφάλειας περιλαμβάνει την ενίσχυση του ιατρικού απορρήτου και την προστασία των ευαίσθητων προσωπικών δεδομένων από μη εξουσιοδοτημένους χρήστες, μέσω μηχανισμών ελέγχου πρόσβασης και αυθεντικοποίησης. Ένα άλλο βασικό ζήτημα ασφάλειας είναι όμως και ο έλεγχος της ακεραιότητας και γνησιότητας των ιατρικών δεδομένων, που αποτελεί κρίσιμη παράμετρο καθώς σε αυτά βασίζονται κατά κύριο λόγο οι ιατρικές διαγνώσεις και κατά συνέπεια οι θεραπευτικές αγωγές που ακολουθούνται. Τέλος, στο θέμα της ασφάλειας εμπίπτει και η εξασφάλιση άρρηκτης σύνδεσης μεταξύ του ασθενούς και των ιατρικών του δεδομένων, προκειμένου και σε αυτήν την περίπτωση να αποφευχθεί το ενδεχόμενο

λανθασμένης διάγνωσης. Πέρα όμως από το κρίσιμο θέμα της ασφάλειας, η σχεδίαση του υδατογραφικού σχήματος έγινε με βάση και την επιδίωξη να προσφέρει ένα εργαλείο προστιθέμενης αξίας στη διαχείριση πληροφορίας σε ιατρικά πληροφοριακά συστήματα, αξιοποιώντας τη δυνατότητα της υδατογραφίας να διευκολύνει την αρχειοθέτηση και ανάκτηση δεδομένων και να εμπλουτίσει τις εικόνες με πρόσθετη πληροφορία, βοηθητική για τη διάγνωση ή για μελλοντική χρήση.

Βασική προϋπόθεση για την επίτευξη των παραπάνω στόχων αποτελεί η σχεδίαση ενός υδατογραφικού σχήματος που να επιτρέπει την ταυτόχρονη εισαγωγή διαφορετικών τύπων υδατογραφημάτων σε μία εικόνα, τα οποία είναι μεταξύ τους ανεξάρτητα και μπορούν να εξαχθούν χωριστά και να χρησιμοποιηθούν για διαφορετικούς σκοπούς. Βάσει αυτής της προϋπόθεσης, το υδατογραφικό σχήμα που σχεδιάστηκε και αναπτύχθηκε εφαρμόζει πολλαπλή υδατογράφιση σε ιατρικές εικόνες, επιτρέποντας την ταυτόχρονη εισαγωγή σε αυτές ποικίλων δεδομένων διαφορετικής φύσης, χαρακτηριστικών και απαιτήσεων, που προορίζονται για διαφορετικούς σκοπούς. Σε συμφωνία με τους αρχικούς στόχους, το υδατογραφικό σχήμα παρέχει εναλλακτικές ή / και συμπληρωματικές λύσεις για την προστασία του ιατρικού απορρήτου, τον έλεγχο πρόσβασης και ακεραιότητας των δεδομένων, την αποδοτική διαχείριση και ανάκτηση ιατρικής πληροφορίας, ικανοποιώντας παράλληλα την αυστηρή απαίτηση για διατήρηση της διαγνωστικής αξίας των ιατρικών εικόνων.

Το υδατογραφικό σχήμα επιτρέπει την εισαγωγή τεσσάρων διαφορετικών τύπων υδατογραφημάτων, ο ρόλος των οποίων και η πληροφορία που ενσωματώνουν συνοψίζονται στον Πίνακα 27. Τα υδατογραφήματα που επιλέγονται τελικά από τους διαθέσιμους τέσσερις τύπους, καθώς και η πληροφορία που θα φέρει καθένα από αυτά, εξαρτώνται από την αντίστοιχη εφαρμογή. Το υδατογραφικό σχήμα που αναπτύχθηκε ανήκει στην κατηγορία των συστημάτων «τυφλής ανίχνευσης» (oblivious systems), δηλαδή για την εξαγωγή των υδατογραφημάτων δεν απαιτείται η αρχική, μη υδατογραφημένη εικόνα. Κάθε υδατογράφημα ενσωματώνεται και εξάγεται από την εικόνα ανεξάρτητα από τα υπόλοιπα, γεγονός που επιτρέπει την εισαγωγή και ανάκτηση των δεδομένων που

περιέχει καθένα από αυτά σε διαφορετικές φάσεις διαχείρισης της εικόνας, ανάλογα με το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν.

Τύπος Υδατογραφήματος	Δεδομένα προς Ενσωμάτωση	Πεδίο Εφαρμογής
Υδατογράφημα Υπογραφής	- Όνομα διαγνωστικού κέντρου - Υπογραφή γιατρού - Αναγνωριστικός κωδικός ιατρικού απεικονιστικού μηχανήματος ή κινητού τηλεϊατρικού σταθμού κ.λπ.	Αναγνώριση πηγής προέλευσης εικόνων
Υδατογράφημα Δείκτη	- Κωδικοί ασθενειών - Κωδικός εξέτασης - Κωδικός ασθενή κ.λπ.	Αρχειοθέτηση και ανάκτηση ιατρικών δεδομένων
Υδατογράφημα Επικεφαλίδας	- Ονοματεπώνυμο ασθενή - Ημερομηνία εξέτασης - Νοσηλευτικό κέντρο - Τύπος ιατρικού απεικονιστικού μηχανήματος - Διάγνωση - Σχόλια / βοηθητική πληροφορία - Σύνοψη ιατρικού ιστορικού κ.λπ	- Προστασία ευαίσθητων προσωπικών και ιατρικών δεδομένων (έλεγχος πρόσβασης) - Επισημάνση χαρακτηριστικών (για καθοδήγηση άλλων γιατρών ή μελλοντική αναφορά)
Υδατογράφημα Αναφοράς	Προκαθορισμένη ακολουθία bits (εκ των προτέρων διαθέσιμη και στο σύστημα εξαγωγής των υδατογραφημάτων)	Έλεγχος ακεραιότητας εικόνας

Πίνακας 27: Συγκεντρωτικός πίνακας διαθέσιμων τύπων υδατογραφημάτων, της πληροφορίας που φέρουν και του ρόλου που εξυπηρετούν.

Ανταποκρινόμενο στις αυστηρές απαιτήσεις που υπάρχουν ως προς τη διασφάλιση της ακεραιότητας της διαγνωστικής πληροφορίας των ιατρικών εικόνων, το υδατογραφικό σύστημα επιτρέπει την επιλογή μιας Περιοχής Ενδιαφέροντος. Η περιοχή αυτή μπορεί είτε να εξαιρεθεί από τη διαδικασία της υδατογράφησης, είτε να χρησιμοποιηθεί αποκλειστικά για την ενσωμάτωση του υδατογραφήματος αναφοράς με στόχο τον έλεγχο της ακεραιότητάς της. Οι άλλοι τρεις τύποι υδατογραφημάτων ενσωματώνονται σε περιοχές που δεν είναι κρίσιμες από άποψη διαγνωστικής αξίας, αποφεύγοντας έτσι την περαιτέρω επιβάρυνση των διαγνωστικά σημαντικών περιοχών. Τονίζεται πάντως ότι τα αποτελέσματα της αξιολόγησης του συστήματος ως προς την ποιότητα των υδατογραφημένων εικόνων κρίθηκαν απολύτως ικανοποιητικά, ακόμη και στις περιοχές όπου ενσωματώθηκαν όλοι οι τύποι υδατογραφημάτων. Το συμπέρασμα αυτό φανερώνει την καταλληλότητα του συστήματος για χρήση σε ιατρικές εφαρμογές, βάσει και της επικρατούσας άποψης ότι αναμένεται ευρεία αποδοχή και εφαρμογή υδατογραφικών τεχνικών σε ιατρικά δεδομένα, με την προϋπόθεση ότι αυτά αποδεδειγμένα δεν προκαλούν αλλοίωση της διαγνωστικής πληροφορίας [1]. Όπως παρουσιάστηκε αναλυτικά στο Κεφάλαιο 7, οι δοκιμές που πραγματοποιήθηκαν στο σύστημα απέδειξαν πέραν της ικανοποίησης της απαίτησης για διαφάνεια, την αποδοτικότητα ως προς την παρεχόμενη ανθεκτικότητα των υδατογραφημάτων σε ενδεχόμενες επιθέσεις στην εικόνα, αλλά και τη δυνατότητά του συστήματος να απεικονίσει τυχόν αλλοιώσεις μέσω του υδατογραφήματος αναφοράς.

9.3 ΑΞΙΟΛΟΓΗΣΗ ΣΥΣΤΗΜΑΤΟΣ – ΚΑΙΝΟΤΟΜΙΑ ΚΑΙ ΣΥΝΕΙΣΦΟΡΑ

Τα πλεονεκτήματα που προσφέρει το υδατογραφικό σχήμα σε συστήματα διαχείρισης ιατρικής πληροφορίας, μπορούν να συνοψιστούν στα εξής:

- Πρόσθετο επίπεδο ασφάλειας σε ιατρικά πληροφοριακά συστήματα. Επισημαίνεται ότι η χρήση υδατογραφήματος που φέρει πληροφορία ως προς την πηγή προέλευσης των ιατρικών δεδομένων προσφέρει ένα συμπληρωματικό μέτρο προστασίας στα ήδη υπάρχοντα συστήματα ασφαλείας που ταυτοποιούν τις

εμπλεκόμενες οντότητες. Η πληροφορία αυτή μπορεί να συνδυαστεί με την ένθεση μιας χρονικής σφραγίδας (time-stamp), συμβάλλοντας με αυτόν τον τρόπο στην αποφυγή αποποίησης (non-repudiation) συναλλαγών μεταξύ οντοτήτων, που αποτελεί άλλωστε μια από τις βασικές απαιτήσεις ασφάλειας.

– *Προστασία ιατρικού απορρήτου και ευαίσθητων προσωπικών δεδομένων.* Το υδατογραφικό σύστημα παρέχει τη δυνατότητα απόκρυψης της ευαίσθητης πληροφορίας μέσα στις εικόνες και κατά συνέπεια λειτουργεί ως μηχανισμός ελέγχου πρόσβασης. Σημειώνεται μάλιστα ότι το εν λόγω σύστημα επιτρέπει την ιεραρχική πρόσβαση στα δεδομένα σύμφωνα με το ρόλο του χρήστη (role-based access control), καθώς προσφέρει τη δυνατότητα χρήσης διαφορετικών υδατογραφικών κλειδιών για την αποκάλυψη διαφορετικών πληροφοριών. Απουσία των κατάλληλων κλειδιών, οι εικόνες είναι απο-προσωποποιημένες και μπορούν να χρησιμοποιηθούν για ερευνητικούς ή εκπαιδευτικούς σκοπούς, χωρίς τον κίνδυνο παραβίασης του ιατρικού απορρήτου.

– *Μείωση κινδύνου λανθασμένης διάγνωσης και ακατάλληλης θεραπευτικής αγωγής,* μέσω της μόνιμης σύνδεσης των ιατρικών εικόνων και δεδομένων με τον ασθενή στον οποίο αντιστοιχούν. Η υδατογράφιση των εικόνων με τον αναγνωριστικό κωδικό του ασθενή εγγυάται την ορθή αντιστοίχιση δεδομένων και ατόμων και κατά συνέπεια την αποφυγή λανθασμένων διαγνώσεων.

– *Έλεγχος ακεραιότητας και γνησιότητας ιατρικών εικόνων.* Το σύστημα προσφέρει την επιλογή ενσωμάτωσης ενός υδατογραφήματος αναφοράς στην εικόνα, το οποίο επιτρέπει την ανίχνευση εσκεμμένων ή μη αλλοιώσεων που ενδέχεται να σημειωθούν κατά τη μετάδοση ή αποθήκευσή της. Το εν λόγω υδατογράφημα ενσωματώνεται με τέτοιο τρόπο στην εικόνα, ώστε όχι μόνο να ανιχνεύει την ύπαρξη αλλοίωσης, αλλά και να εντοπίζει τις παραποιημένες περιοχές. Επίσης, η κατανομή του συγκεκριμένου υδατογραφήματος σε διαφορετικά επίπεδα ανάλυσης στο πεδίο μετασχηματισμού, επιτρέπει την περαιτέρω αξιολόγηση τυχόν αλλοίωσης, αποτυπώνοντας το βαθμό στον οποίο επηρεάζεται από αυτήν το αισθητικό και κυρίως το διαγνωστικό αποτέλεσμα. Σημειώνεται ότι η ενσωμάτωση του υδατογραφήματος αναφοράς με χρήση του αλγορίθμου που αναπτύχθηκε στα

πλαίσια της διατριβής, αποτελεί ουσιαστικά μια προσέγγιση «ημι-εύθραυστης» (semi-fragile) τεχνικής, καθώς δεν περιορίζεται στην ανίχνευση ενδεχόμενης παραποίησης της εικόνας, αλλά επιτρέπει τη διάκριση των αλλοιώσεων που δεν επηρεάζουν το αισθητικό αποτέλεσμα από εκείνες που υποβαθμίζουν τη διαγνωστική αξία.

- *Αρχειοθέτηση και ανάκτηση ιατρικών δεδομένων μέσω δεικτοδότησης (indexing).* Το σύστημα παρέχει έναν εναλλακτικό μηχανισμό δεικτοδότησης ιατρικών εικόνων, μέσω του υδατογραφήματος δείκτη, ο οποίος διευκολύνει την αποδοτική αρχειοθέτηση των εικόνων σε βάσεις δεδομένων. Επιτρέπει επιπλέον την εύκολη ανάκτηση τόσο των εικόνων αυτών, όσο και άλλων δεδομένων που είναι επίσης αποθηκευμένα στη βάση δεδομένων και συνδέονται με αυτές. Ενδεικτικά αναφέρεται το παράδειγμα της ανάκτησης του ιατρικού φακέλου του ασθενή ή βοηθητικών πληροφοριών από παρόμοια περιστατικά, στην περίπτωση που το υδατογράφημα δείκτη περιέχει τον αναγνωριστικό κωδικό του ασθενή ή τον κωδικό της ασθένειας αντίστοιχα.

- *Εμπλουτισμός εικόνας με στοιχεία που βοηθούν στη διάγνωση ή για μελλοντική αναφορά και καθοδήγηση.* Το σύστημα επιτρέπει την ενσωμάτωση στην εικόνα πληροφορίας που βοηθά στη σωστή διάγνωση και κατάλληλη θεραπευτική αγωγή, περιλαμβάνοντας στοιχεία για το ιατρικό ιστορικό του ασθενή, σχόλια για την εξέταση και για τμήματα της εικόνας σημαντικά από άποψη διαγνωστικής αξίας, την αρχική διάγνωση κ.λπ.

Το υδατογραφικό σύστημα επιτυγχάνει τα παραπάνω μέσω της ταυτόχρονης ενσωμάτωσης στις εικόνες πολλαπλών τύπων υδατογραφημάτων, που διαθέτουν διαφορετικά ή/και αντιφατικά χαρακτηριστικά και φέρουν πληροφορία διαφορετικής φύσης και απαιτήσεων. Αξιοποιώντας τις ιδιότητες των υποζωνών που προκύπτουν κατά την ανάλυση της εικόνας με μετασχηματισμό κυματιδίων και λαμβάνοντας υπόψη τις απαιτήσεις ως προς την ανθεκτικότητα και τη χωρητικότητα για κάθε τύπο υδατογραφήματος, το σύστημα επιτρέπει την ενσωμάτωση πολλαπλών τύπων υδατογραφημάτων μέσα στην ίδια εικόνα. Τα υδατογραφήματα αυτά εισάγονται και εξάγονται ανεξάρτητα από τα υπόλοιπα και

μπορούν να χρησιμοποιηθούν σε διαφορετικές φάσεις διαχείρισης των εικόνων, καλύπτοντας με αυτόν τον τρόπο το προαναφερόμενο εύρος εφαρμογών.

Παρά το προοδευτικά αυξανόμενο ενδιαφέρον της ερευνητικής κοινότητας για την υιοθέτηση της ψηφιακής υδατογραφίας σε ιατρικές εφαρμογές, η προσέγγιση της πολλαπλής υδατογράφησης ιατρικών εικόνων με στόχο την ταυτόχρονη κάλυψη ποικίλων εφαρμογών αποτελεί μια καινοτόμα προσέγγιση. Τμήματα της ερευνητικής εργασίας που πραγματοποιήθηκε στα πλαίσια της διατριβής έχουν δημοσιευτεί σε μια σειρά άρθρων σε αναγνωρισμένα διεθνή περιοδικά και πρακτικά συνεδρίων, εμπλουτίζοντας έτσι σημαντικά το μέχρι πρόσφατα εξαιρετικά περιορισμένο πλήθος σχετικών αναφορών στη βιβλιογραφία [26]-[38]. Αξίζει μάλιστα να σημειωθεί ότι η καινοτομία της προσέγγισης και η συνεισφορά της στο σχετικό ερευνητικό πεδίο διαφαίνεται και από το γεγονός ότι σε αρκετά πρόσφατα άρθρα άλλων ερευνητών γίνεται αναφορά σε τμήματα της εργασίας που πραγματοποιήθηκε στα πλαίσια εκπόνησης της παρούσας διατριβής [18]-[25].

9.4 ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ ΚΑΙ ΠΡΟΟΠΤΙΚΕΣ

Στο μέλλον, το σύστημα θα μπορούσε να επιδεχθεί τροποποιήσεις και βελτιώσεις, προκειμένου να διευρυνθεί το φάσμα εφαρμογών του και να βελτιωθεί η αποδοτικότητά του. Ακολουθεί η παρουσίαση κάποιων προτάσεων για μελλοντική έρευνα:

- Ενσωμάτωση του υδατογραφήματος αναφοράς με τεχνική αντιστρεπτής υδατογράφησης: δεδομένης της αυστηρής απαίτησης για διασφάλιση της ακεραιότητας των διαγνωστικά κρίσιμων περιοχών των εικόνων, είναι σημαντικό να υπάρχει ένας μηχανισμός εξέτασής τους, ο οποίος θα επιτρέπει την ανίχνευση τυχόν αλλοιώσεων και την αποτίμησή τους. Όπως έχει προαναφερθεί, η επικρατούσα άποψη που εκφράζεται από ερευνητές οι οποίοι ασχολούνται με το συγκεκριμένο πεδίο, είναι ότι η καθιέρωση της υδατογραφίας σε ιατρικές εφαρμογές θα αποτελεί σε λίγα χρόνια γεγονός και θα αρθούν οι όποιοι ενδοιασμοί σχετίζονται με το κατά πόσο επιτρέπεται η οποιασδήποτε μορφής επεξεργασία των ιατρικών

εικόνων, εφόσον βέβαια πρόκειται για υδατογραφήματα που αφήνουν αναλλοίωτο το αισθητικό αποτέλεσμα [1]. Ωστόσο, προκειμένου το υδατογραφικό σύστημα να ικανοποιήσει τις απαιτήσεις ακόμη και των πιο σκεπτικιστών, θα μπορούσε να χρησιμοποιεί για την εισαγωγή του υδατογραφήματος αναφοράς έναν αλγόριθμο αντιστρεπτής υδατογράφησης, ο οποίος θα επιτρέπει την αφαίρεση του συγκεκριμένου υδατογραφήματος από την εικόνα και την επαναφορά των περιοχών διαγνωστικής αξίας στην αρχική τους κατάσταση [39], [40]. Υπενθυμίζεται ότι οι αλγόριθμοι αντιστρεπτής υδατογράφησης έχουν το μειονέκτημα της μειωμένης διαθέσιμης χωρητικότητας, θα μπορούσε όμως να εξεταστεί η εφαρμοσιμότητά τους σε ένα περιορισμένο τμήμα της εικόνας, το οποίο περικλείει τη διαγνωστική πληροφορία. Μια εναλλακτική προσέγγιση θα ήταν η ενσωμάτωση του υδατογραφήματος αναφοράς με τεχνική που ανήκει στην κατηγορία αντικατάστασης του ελάχιστου σημαντικού ψηφίου (LSB). Δεδομένης όμως της υπερβολικής ευθραυστότητας τέτοιων τεχνικών, θα πρέπει να διερευνηθεί η δυνατότητά τους να παράσχουν αξιόπιστη πληροφορία ως προς τις αλλοιωμένες περιοχές και να αξιολογηθεί η καταλληλότητά τους για το συγκεκριμένο σκοπό, σε σχέση με την τρέχουσα προσέγγιση ημι-εύθραυστης τεχνικής.

- Δοκιμή εναλλακτικών σχημάτων κωδικοποίησης διόρθωσης σφαλμάτων: θα μπορούσαν να δοκιμαστούν εναλλακτικά σχήματα κωδικοποίησης διόρθωσης σφαλμάτων πέραν του σχήματος BCH που εφαρμόστηκε για την κωδικοποίηση των υδατογραφήματων, προκειμένου να εξεταστεί εάν μπορεί να βελτιωθεί περαιτέρω η αποδοτικότητα του συστήματος.

- Επέκταση εφαρμογής σε έγχρωμες εικόνες: το υδατογραφικό σχήμα έχει προς το παρόν εφαρμογή σε ασπρόμαυρες (grayscale) εικόνες, καλύπτοντας έτσι ένα ευρύ φάσμα ιατρικών απεικονιστικών μηχανημάτων. Η επέκταση του σε έγχρωμες εικόνες θα επιτρέψει την κάλυψη και μιας σειράς άλλων κλινικών εφαρμογών, όπως για παράδειγμα την ασφαλή διαχείριση δερματολογικών εικόνων. Για το σκοπό αυτό, θα μπορούσε να δοκιμαστεί η μετατροπή των συνιστωσών RGB των pixels της εικόνας σε συνιστώσες του χρωματικού μοντέλου YIQ. Το μοντέλο YIQ έχει την ιδιότητα να αποσυνδέει τη φωτεινότητα από τη χρωματική πληροφορία,

αναπαριστώντας το χρώμα των pixels της εικόνας σε τρεις συνιστώσες, τη φωτεινότητα (Y), τη χροιά (I) και τον κορεσμό (Q). Αξιοποιώντας αυτήν την ιδιότητα, θα μπορούσε να εφαρμοστεί ο προτεινόμενος αλγόριθμος απευθείας στη φωτεινότητα, σε πλήρη αντιστοιχία με την υπάρχουσα εφαρμογή του στις ασπρόμαυρες εικόνες (grayscale), χωρίς να χρειαστεί περαιτέρω τροποποίηση. Στη συνέχεια, η μετασχηματισμένη από τον αλγόριθμο συνιστώσα φωτεινότητας Y που θα φέρει πλέον τα υδατογραφήματα, θα χρησιμοποιηθεί σε συνδυασμό με τις άθικτες συνιστώσες I και Q , προκειμένου να προκύψει και πάλι η εικόνα σε μορφή RGB. Θα μπορούσε επίσης να δοκιμαστεί για τον ίδιο σκοπό η χρήση αντιστρεπτού σχήματος μετατροπής χρώματος (reversible color conversion transform), που έχει το πλεονέκτημα ότι αντιστοιχεί τις συνιστώσες RGB των pixels της εικόνας σε συνιστώσες που είναι επίσης ακέραιες τιμές, αποφεύγοντας στρογγυλοποιήσεις στις τιμές των συνιστωσών και αφήνοντας περιθώρια στην παρούσα υλοποίηση να συμπεριλάβει αντιστρεπτά σχήματα υδατογράφησης. Ένα αντιστρεπτό σχήμα μετατροπής χρώματος που θα μπορούσε να δοκιμαστεί κάτω από αυτό το πρίσμα αποτελεί μια τροποποιημένη εκδοχή του μοντέλου YCrCb που περιγράφεται στο [41].

– *Επέκταση εφαρμογής σε βίντεο:* το προτεινόμενο σύστημα θα μπορούσε να επεκταθεί και στην υδατογράφιση βίντεο, προκειμένου να εφαρμοστεί σε ιατρικά δεδομένα που αποτελούνται από ακολουθίες εικόνων (π.χ. ηχοκαρδιογράφημα, μαγνητική αγγειογραφία, αποτελέσματα ενδοσκοπικών εξετάσεων όπως γαστροσκόπηση, κ.λπ) και να καλύψει εφαρμογές που αφορούν λήψη εικόνων βίντεο ασθενούς, όπως για παράδειγμα στην περίπτωση μετάδοσης βίντεο από τηλεϊατρικό σύστημα.

Όπως προαναφέρθηκε, το υδατογραφικό σύστημα που αναπτύχθηκε στα πλαίσια της διατριβής έχει την προοπτική να παράσχει υπηρεσίες προστιθέμενης αξίας σε ιατρικά πληροφοριακά συστήματα [26], [27], [30]. Κατά τη φάση σχεδίασής του λήφθηκαν υπόψη διάφορες περιπτώσεις χρήσης του, προκειμένου να καθοριστεί ένα πλαίσιο προδιαγραφών τις οποίες χρειάζεται να καλύπτει, ώστε να είναι εφικτή η ενσωμάτωσή του σε συστήματα διαχείρισης ιατρικής πληροφορίας. Πρέπει να

σημειωθεί ότι έχει δοθεί ιδιαίτερη έμφαση στις προοπτικές ολοκλήρωσης του υδατογραφικού σχήματος σε τηλεϊατρικά συστήματα και έχουν μάλιστα ξεκινήσει ήδη οι πρώτες προσπάθειες προς αυτήν την κατεύθυνση [29]. Πέρα από τις προοπτικές του σχήματος σε τηλεϊατρικές εφαρμογές, εκτιμάται ότι μπορεί να συμβάλει ουσιαστικά στην αναβάθμιση της ασφάλειας και της διαχειριστικής ικανότητας των ιατρικών πληροφοριακών συστημάτων, ειδικά σε περίπτωση ενσωμάτωσής του σε ιατρικά απεικονιστικά μηχανήματα.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

- [1] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, "Relevance of watermarking in medical imaging," in *Proc. 3rd Conf. Information Technology Applications in Biomedicine, ITAB'00*, Arlington, USA, pp. 250-255.
- [2] A. Wakatani, "Digital watermarking for ROI medical images by using compressed signature image," presented at the 35th Annu. Hawaii Intern. Conf. System Sciences, HICSS'02, Big Island, HI, USA.
- [3] G. Coatrieux, H. Maitre, B. Sankur, "Strict integrity control of biomedical images," in *Proc. SPIE Security and Watermarking of Multimedia Contents III, SPIE2001*, San Jose, USA, vol. 4314, pp. 229-240, Jan. 2001.
- [4] H. M. Chao, C. M. Hsu, S. G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Trans. Inf. Technol. Biomed.*, vol. 6, no. 1, pp. 46-53, March 2002.
- [5] S. G. Miaou, C. M. Hsu, Y. S. Tsai, H. M. Chao, "A secure data hiding technique with heterogeneous data combining capability for electronic patient records," in *Proc. 22nd Annu. Intern. Conf. IEEE Engineering in Medicine and Biology Society, EMBS'00*, Chicago, USA, vol. 1, pp. 280-283.
- [6] U. Rajendra Acharya, D. Anand, P. Subbanna Bhat, U.C. Niranjan, "Compact storage of medical images with patient information," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 4, pp. 320-323, Dec. 2001.
- [7] R. U. Acharya, P. S. Bhat, S. Kumar, L. Choo Min, "Transmission and storage of medical images with patient information," *Computers in Biology and Medicine*, no. 33, pp. 303-310, 2003.
- [8] R. U. Acharya, U.C. Niranjan, S.S. Iyengar, N. Kannathal, L. C. Min, "Simultaneous storage of patient information with medical images in the frequency domain," *Computer Methods and Programs in Biomedicine*, no. 76, pp.13-19, 2004.
- [9] Jagadish Nayak, Subbanna P. Bhat, Rajendra U. Acharya, Niranjan U. Cholaayya, "Simultaneous storage of medical images in the spatial and frequency domain: A comparative study," *BioMedical Engineering OnLine*, Jun 05, 2004, 3(1):17.

- [10] X. Q. Zhou, H. K. Huang, S. L. Lou, "Authenticity and integrity of digital mammography images," *IEEE Trans. Medical Imaging*, vol. 20, no. 8, pp. 784-791, Aug. 2001.
- [11] B. Macq, F. Dewey, "Trusted Headers for Medical Images," *Proc. DFG VIII-DII Watermarking Workshop*, Erlangen, Germany, Oct. 1999.
- [12] H. Trichili, M. Boubel, N. Derbel, L. Kamoun, "A new medical image watermarking scheme for a better telediagnosis," *Proc. IEEE International Conference on Systems, Man and Cybernetics*, vol. 1, pp. 556-559, Oct. 6-9, 2002.
- [13] X. Kong, R. Feng, "Watermarking medical signals for telemedicine," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 3, pp. 195-201, Sept. 2001.
- [14] Y. Yang, F. Bao, "An invertible watermarking scheme for authentication of Electronic Clinical Brain Atlas", *Proc. IEEE Intern. Conf. on Acoustics, Speech, and Signal Processing (ICASSP '03)*, vol. 3, pp. 533-536, April 6-10, 2003.
- [15] W. Puech, J. M. Rodrigues, "A new crypto-watermarking method for medical images safe transfer", *Proc. 12th Europ. Signal Processing Conf. (EUSIPCO'04)*, pp. 1481-1484, Vienna, Austria, Sept. 6-10, 2004.
- [16] D. Osborne, D. Abbott, M. Sorell, D. Rogers, "Multiple embedding using robust watermarks for wireless medical images," *Proc. 3rd Intern. Conf. Mobile and Ubiquitous Multimedia*, College Park, Maryland, USA, pp. 245-250, 2004.
- [17] F. Bao, R.H. Deng, B. Chin Ooi, Y. Yang, "Tailored reversible watermarking schemes for authentication of Electronic Clinical Atlas", *IEEE Trans. Information Technology in Biomedicine*, vol. 9, no. 4, Dec. 2005, pp. 554-563.
- [18] H.-K. Lee, H.-J. Kim, K.-R. Kwon, J.-K. Lee, "Digital watermarking of medical image using ROI information", *Proc. 7th Intern. Workshop Enterprise Networking and Computing in Healthcare Industry (HEALTHCOM)*, 2005.
- [19] C.-S. Woo, J. Du, B. Pham, "Multiple watermark method for privacy control and tamper detection in medical images", *Proc. APRS Workshop on Digital Image Computing, Pattern Recognition and Imaging for Medical Applications*, Brisbane, Queensland, Australia, February 21, 2005.
- [20] B. Planitz, A. Maeder, "Medical image watermarking: a study on image degradation", *Proc. APRS Workshop on Digital Image Computing, Pattern Recognition*

- and Imaging for Medical Applications*, February 21, 2005, Brisbane, Queensland, Australia.
- [21] H.-K. Lee, H.-J. Kim, K.-R. Kwon, J.-K. Lee, "ROI medical image watermarking using DWT and bit-plane", *Proc. Asia-Pacific Conference on Communications*, pp. 512-515, Perth, Western Australia, Oct. 3-5, 2005.
- [22] B. M. Planitz, A. J. Maeder, "A Study of block-based medical image watermarking using a perceptual similarity metric, *Proc. IEEE Digital Imaging Computing: Techniques and Applications (DICTA 2005)*, Cairns, Queensland, Australia, Dec. 6-8, 2005.
- [23] H. M. Desai, M. S. Raval, A. I. Trivedi, "Correlation-based reversible watermarking technique for medical images", *Proc. National Conference on Image Processing*, Bangalore, India, March 23-25, 2005.
- [24] G. Coatrieux, L. Lecornu, B. Sankur, Ch. Roux, "A review of image watermarking applications in healthcare", *Proc. 28th IEEE Annual Intern. Conf. of the Engineering in Medicine and Biology Society (EMBC'06)*, pp. 4691-4694, New York City, USA, Aug. 30-Sept. 3, 2006.
- [25] G. Boato, F. G. B. De Natale, C. Fontanari, "Digital image tracing by sequential multiple watermarking", *IEEE Transactions on Multimedia*, to be published.
- [26] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple image watermarking applied to health information management", *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. 722-732, Oct. 2006.
- [27] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images", *Medical & Biological Engineering & Computing*, vol. 44, no. 8, pp. 619-631, Springer Berlin / Heidelberg, August 2006. Available: <http://dx.doi.org/10.1007/s11517-006-0081-x>
- [28] A. Giakoumaki, A. Tagaris, D. Koutsouris, "Implementation of a user-friendly GUI for a multiple image watermarking tool Addressing healthcare applications", to appear in *Proc. 2006 IEEE EMBS International Conference on Information Technology Applications in Biomedicine (ITAB 2006)*, Ioannina, Greece, October 26-28, 2006.
- [29] A. Giakoumaki, K. Perakis, A. Tagaris, D. Koutsouris, "Digital watermarking in telemedicine applications – Towards enhanced data security and accessibility", *Proc.*

- 28th IEEE Annual Intern. Conf. of the Engineering in Medicine and Biology Society (EMBC'06), pp. 6328-6331, New York, USA, Aug. 30 – Sept. 3, 2006.
- [30] A. Tagaris, A. Giakoumaki, L. Karle, D. Koutsouris, "Watermarking SDK implementation to facilitate integration in a secure healthcare environment", *Proc. 28th IEEE Annual Intern. Conf. of the Engineering in Medicine and Biology Society (EMBC'06)*, pp. 3262-3265, New York, USA, Aug. 30 – Sept. 3, 2006.
- [31] Kostas Perakis, Aggeliki Giakoumaki, Tassos Tagaris, Dimitris Koutsouris, "Enhancement of security and accessibility in telemedical applications using digital watermarking", *Proc. 4th International Conference on Information Communication Technologies in Health (ICICTH'06)*, Samos Island, Greece, July 13-15, 2006.
- [32] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Health Data Management through Multiple Watermarking of Medical Images", in *IFMBE Proc. 3rd European Medical and Biological Engineering Conf., EMBEC'05*, vol. 11, pp. 3093-3096, Prague, Czech Republic, November 20-25, 2005.
- [33] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple Digital Watermarking Applied to Medical Imaging", *Proceedings of the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS)*, pp. 3444-3447, Shanghai, China, September 1-4, 2005.
- [34] Aggeliki Giakoumaki, Sotiris Pavlopoulos, Dimitris Koutsouris, "Digital Watermarking Perspectives in Health Information Management," *Proceedings of the 3rd International Conference on Information Communication Technologies in Health, ICICTH'05*, pp. 316-321, Samos Island, Greece, July 7-9, 2005.
- [35] Aggeliki Giakoumaki, Sotiris Pavlopoulos, Dimitris Koutsouris, "Digital Watermarking Perspectives in Health Information Management," *Journal for Quality of Life Research*, volume 3, issue 2, supplement 1, pp. 145-149, May-June 2005.
- [36] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "A Multiple Watermarking Scheme Applied to Medical Image Management", *Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS)*, pp. 3241-3244, San Francisco, CA, USA, September 1-5, 2004.
- [37] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "A Medical Image Watermarking Scheme Based on Wavelet Transform", *Proceedings of the 25th Annual International*

- Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS), pp. 856-859, Cancun, Mexico, September 17-21, 2003
- [38] Giakoumaki A., Pavlopoulos S., Koutsouris D., “A wavelet-based watermarking scheme appropriate for medical images”, Proceedings of the 1st International Conference on Information Communication Technologies in Health, Samos, Greece, July 11-13, 2003
- [39] J. Fridrich, M. Goljan, R. Du, “Lossless data embedding for all image formats,” in Proc. SPIE Photonics West, Security and Watermarking of Multimedia Contents, San Jose, CA, vol. 4675, pp. 572-583, Jan. 2002.
- [40] J. Fridrich, M. Goljan, R. Du, “Invertible authentication,” in Proc. SPIE Photonics West, Security and Watermarking of Multimedia Contents, San Jose, CA, vol. 3971, pp. 197-208, 2001.
- [41] J. Tian, “Wavelet based reversible watermarking for authentication,” in Proc. SPIE Security and Watermarking of Multimedia Contents IV, SPIE2002, San Jose, USA, vol. 4675, pp. 679-690, Jan. 2002.

ΚΑΤΑΛΟΓΟΣ ΔΗΜΟΣΙΕΥΣΕΩΝ

Κατά τη διάρκεια της έρευνας που διεξήχθη στα πλαίσια της παρούσας διατριβής προέκυψαν οι παρακάτω δημοσιεύσεις σε διεθνή περιοδικά και συνέδρια:

Διεθνή Περιοδικά (με διαδικασία κρίσης)

- [J1] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple Image Watermarking Applied to Health Information Management", IEEE Transactions on Information Technology in Biomedicine, vol. 10, no. 4, pp. 722-732, Oct. 2006.
- [J2] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Secure and Efficient Health Data Management through Multiple Watermarking on Medical Images", Medical & Biological Engineering & Computing, vol. 44, no. 8, pp. 619-631, Springer Berlin / Heidelberg, Aug. 2006.
- [J3] Aggeliki Giakoumaki, Sotiris Pavlopoulos, and Dimitris Koutsouris, "Digital Watermarking Perspectives in Health Information Management," Journal for Quality of Life Research, vol. 3, no. 2, suppl. 1, pp. 145-149, May-June 2005.

Διεθνή Συνέδρια (με διαδικασία κρίσης)

- [C1] A. Giakoumaki, A. Tagaris, D. Koutsouris, "Implementation of a User-friendly GUI for a Multiple Image Watermarking Tool Addressing Healthcare Applications", Proc. 2006 IEEE EMBS International Conference on Information Technology Applications in Biomedicine (ITAB 2006), Ioannina, Greece, October 26-28, 2006.
- [C2] A. Giakoumaki, K. Perakis, A. Tagaris, D. Koutsouris, "Digital Watermarking in Telemedicine Applications – Towards Enhanced Data Security and Accessibility", Proc. 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS), pp. 6328-6331, New York, USA, Aug. 30 – Sept. 3, 2006.
- [C3] A. Tagaris, A. Giakoumaki, L. Karle, D. Koutsouris, "Watermarking SDK Implementation to Facilitate Integration in a Secure Healthcare Environment", Proc. 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS), pp. 3262-3265, New York, USA, Aug. 30 – Sept. 3, 2006.
- [C4] Kostas Perakis, Aggeliki Giakoumaki, Tassos Tagaris, Dimitris Koutsouris, "Enhancement of security and accessibility in telemedical applications using digital watermarking", Proc. 4th International Conference on

Information Communication Technologies in Health, ICICTH'06, Samos Island, Greece, July 13-15, 2006.

- [C5] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Health Data Management through Multiple Watermarking of Medical Images", in IFMBE Proc. 3rd European Medical and Biological Engineering Conf., EMBEC'05, vol. 11, pp. 3093-3096, Prague, Czech Republic, Nov. 20-25, 2005.
- [C6] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple Digital Watermarking Applied to Medical Imaging", Proc. 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS), Shanghai, China, September 1-4, 2005.
- [C7] Aggeliki Giakoumaki, Sotiris Pavlopoulos, Dimitris Koutsouris, "Digital Watermarking Perspectives in Health Information Management," Proceedings of the 3rd International Conference on Information Communication Technologies in Health, ICICTH'05, pp. 316-321, Samos Island, Greece, July 7-9, 2005.
- [C8] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "A Multiple Watermarking Scheme Applied to Medical Image Management", Proc. 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS), pp. 3241-3244, San Francisco, CA, USA, Sept. 1-5, 2004.
- [C9] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "A Medical Image Watermarking Scheme Based on Wavelet Transform", Proc. 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE-EMBS), pp. 856-859, Cancun, Mexico, Sept. 17-21, 2003.
- [C10] Giakoumaki A., Pavlopoulos S., Koutsouris D., "A Wavelet-based Watermarking Scheme Appropriate for Medical Images", Proc. 1st International Conference on Information Communication Technologies in Health, Samos, Greece, July 11-13, 2003.