Πανεπιστήμιο Πατρών
Πολυτεχνική Σχολή
Τμήμα Μηχανικών Η/Υ
και Πληροφορικής

**Μέθοδοι Απόκρυψης Πληροφορίας και Υδατογράφηση
ως Τεχνικές Προστασίας Πνευματικών Δικαιωμάτων και
Πιστοποίησης της Αυθεντικότητας**

Διδακτορική Διατριβή
Σπυριδούλας Μ. Αρμένη

Υπεύθυνος Καθηγητής
Δημήτριος Ν. Χριστοδουλάκης

Πάτρα 2004

**Σε όλους όσους έκαναν
πολυετείς προσπάθειες
για την επίτευξη
ενός σκοπού**

Επταμελής Επιτροπή

Ι. Γαροφαλάκης

Επίκουρος Καθηγητής
Τμήματος Μηχανικών Η/Υ & Πληροφορικής
Πανεπιστήμιο Πατρών

Κ. Μπερμπερίδης

Αναπληρωτής Καθηγητής
Τμήματος Μηχανικών Η/Υ & Πληροφορικής
Πανεπιστήμιο Πατρών

Μ. Ξένος

Λέκτορας
Ελληνικού Ανοικτού Πανεπιστημίου

Γ. Παυλίδης

Καθηγητής
Τμήματος Διοίκησης Επιχειρήσεων
Πανεπιστήμιο Πατρών

Ι. Σταματίου

Επίκουρος Καθηγητής
Τμήματος Μαθηματικών
Πανεπιστήμιο Αιγαίου

ΑΘ. Στουραϊτης

Καθηγητής
Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών
Πανεπιστήμιο Πατρών

Επιβλέπων Καθηγητής

Δ. Χριστοδουλάκης

Καθηγητής
Τμήματος Μηχανικών Η/Υ & Πληροφορικής
Πανεπιστήμιο Πατρών

Ευχαριστίες

Για τη διεκπεραίωση της παρούσας διδακτορικής διατριβής θα ήθελα να εκφράσω τις θερμές ευχαριστίες μου στον Καθηγητή Δημήτριο Χριστοδουλάκη, για την πολύτιμη προσφορά του και τη δυνατότητα συνεργασίας που μου παρείχε, μέσω των μελών της ομάδας του.

Επιπλέον επιθυμώ να ευχαριστήσω το Διδάκτορα και Επίκουρο καθηγητή Ιωάννη Σταματίου, για την πολύτιμη βοήθειά του και συνεργασία του σε θέματα τεχνικών απόκρυψης δεδομένων.

Θέλω να ευχαριστήσω επίσης τα μέλη του εργαστηρίου, το Λέκτορα Μιχάλη Ξένο, και το Διδάκτορα Ιωάννη Κωστόπουλο για τη συμβολή τους, η οποία είχε ενισχυτικό ρόλο στην πραγματοποίηση της παρούσας διδακτορικής διατριβής.

Θερμές ευχαριστίες σε όλα τα μέλη της εξεταστικής επιτροπής, κ. Δ. Χριστοδουλάκη, Επιβλέποντα Καθηγητή, Τμήματος Μηχανικών Η/Υ & Πληροφορικής, Πανεπιστημίου Πατρών, κ. Γ. Παυλίδη, Καθηγητή, Τμήματος Διοίκησης Επιχειρήσεων, Πανεπιστημίου Πατρών, κ. Αθ. Στουραϊτή, Καθηγητή, Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστημίου Πατρών, κ. Κ. Μπερμπερίδη, Αναπληρωτή Καθηγητή, Τμήματος Μηχανικών Η/Υ & Πληροφορικής, Πανεπιστημίου Πατρών, κ. Γ. Σταματίου, Επίκουρο Καθηγητή, Τμήματος Μαθηματικών, Πανεπιστημίου Αιγαίου, κ. Ι. Γαροφαλάκη, Επίκουρο Καθηγητή, Τμήματος Μηχανικών Η/Υ & Πληροφορικής, Πανεπιστημίου Πατρών, και κ. Μ. Ξένο, Λέκτορα, Ελληνικού Ανοικτού Πανεπιστημίου, για τα πολύτιμα σχόλια τους.

Θα ήθελα ομοίως να ευχαριστήσω τους τωρινούς πτυχιούχους και τότε φοιτητές του τμήματος: Πολυχρόνη Κούντρια και Μαρκέλλα Σηφακάκη, στους οποίους είχα αναλάβει την συνεπίβλεψη των διπλωματικών τους εργασιών και μέσα από τις δικές τους απορίες έγιναν πιο κατανοητές βασικές έννοιες στο χώρο της Ψηφιακής Υδατογράφησης και της Απόκρυψης Πληροφορίας.

Τέλος θα ήθελα να ευχαριστήσω τους γονείς μου και τα αδέρφια μου που με ανέχτηκαν και ενίσχυσαν όλα αυτά τα χρόνια τις προσπάθειες μου για την αποπεράτωση αυτής της διδακτορικής διατριβής.

[σύνολο σελίδων 0⇒120=121]

Σπυριδούλα Μ. Αρμένη

περιεχόμενα

Ευχαριστίες	4
περιεχόμενα	6
περιεχόμενα εικόνων	8
περιεχόμενα πινάκων	9
Αρκτικόλεξα	10
Πρόλογος.....	11
Preface	13
Κεφάλαιο 1	15
Αρχές απόκρυψης πληροφορίας:	15
Τεχνικές & επιδιώξεις	15
1.1. Εισαγωγή	15
1.2. Γενική θεώρηση του προβλήματος	17
1.3. Η συνεισφορά μας	18
1.4. Περιληπτική σκιαγράφηση.....	20
Κεφάλαιο 2	25
Φιλοσοφική υπόσταση των συστημάτων ασφαλείας στα πληροφοριακά συστήματα	25
2.1. Εισαγωγή	25
2.2. Κρυπτογραφία.....	27
2.3. Ψηφιακές υπογραφές.....	30
2.4. Ψηφιακές τεχνικές υδατογράφησης.....	31
2.5. Ηθικοί αντίκτυποι.....	36
2.6. Συμπεράσματα	37
Κεφάλαιο 3	38
Υδατογράφηση: από τη δεοντολογία στην πράξη	38
3.1. Εισαγωγή	38
3.2. Δικαιώματα πνευματικής ιδιοκτησίας.....	40
3.3. Το Διαδίκτυο	43
3.4. Θέματα υδατογράφησης	47
3.4.1 Υδατογράφηση κειμένου	47
3.4.2 Υδατογράφηση ήχου	48
3.4.3 Υδατογράφηση εικόνας.....	48
3.4.4 Υδατογράφηση βίντεο.....	49
3.5. Γιατί υδατογράφηση;	49
3.5.1 Απόδειξη γνησιότητας.....	49
3.5.2 Προστασία πνευματικών δικαιωμάτων	50
3.5.3 Δακτυλικό αποτύπωμα	50
3.5.4 Προστασία αντιγραφής	51
3.6. Συμπεράσματα	51
Κεφάλαιο 4	53
Τεχνική απόκρυψης βασιζόμενη σε υπολογιστικά δύσκολα προβλήματα	53
4.1. Εισαγωγή	53
4.2. Προστασία με χρήση συμβολοσειρών - υπογραφών	54
4.3. Γενική περιγραφή της προτεινόμενης μεθόδου	55
4.4. Στοιχεία θεωρίας NP-Completeness	59

4.4.1 Ορισμός κλάσης NP	59
4.4.2 NP-πληρότητα	61
4.5. Παραγωγή τυχαίων στιγμιότυπων του προβλήματος 3-χρωματισμού γράφων	63
4.6. Διαντιδραστικές αποδείξεις μηδενικής γνώσης για 3-χρωματισμό	68
4.7. Αναγνώριση του νόμιμου κατόχου.....	70
4.8. Διαδικασία απόκρυψης δεδομένων	72
4.9. Ένθεση τρία-χρωματίσιμου γράφου.....	75
4.10. Εξαγωγή του τρία-χρωματίσιμου γράφου	77
4.11. Θέματα ποιότητας και αντοχής της μεθόδου.....	78
4.12. Συμπεράσματα.....	81
Κεφάλαιο 5	83
Μέθοδος υδατογράφησης στο χωρικό πεδίο	83
5.1. Εισαγωγή	83
5.2. Μοντέλο υδατογράφησης.....	84
5.2.1 Διαδικασία υδατογράφησης	84
5.2.2 Ανάκτηση υδατογραφήματος	86
5.2.3 Αξιολόγηση της μεθόδου.....	87
5.3. Αποτελέσματα	88
5.3.1 Μετρήσεις PSNR	88
5.3.2 Μετρήσεις ομοιότητας.....	89
5.3.3 Ανθρώπινο οπτικό σύστημα (HVS).....	90
5.3.4 Επιθέσεις και ανάκτηση.....	93
5.3.5 Μεμονωμένα παραδείγματα	94
5.4. Συμπεράσματα	95
Κεφάλαιο 6	97
Μέθοδος υδατογράφησης στο πεδίο συχνοτήτων	97
6.1. Εισαγωγή	97
6.2. Μετασχηματισμός Wavelet	98
6.3. Η τεχνική υδατογράφησης	99
6.3.1 Διαδικασία κωδικοποίησης.....	100
6.3.2 Διαδικασία αποκωδικοποίησης.....	102
6.4. Πειραματικά αποτελέσματα.....	103
6.5. Συμπεράσματα	106
Κεφάλαιο 7	108
Μελλοντική έρευνα.....	108
7.1. Ερευνητικά ζητήματα	108
Βιβλιογραφία	112

περιεχόμενα εικόνων

Εικόνα 2.1: Διάγραμμα συμμετρικής κρυπτογραφίας	28
Εικόνα 2.2: Κρυπτογραφικό σύστημα δημόσιου κλειδιού (<i>public key</i>)	29
Εικόνα 4.1: Παράγοντες που επιδρούν στην απόκρυψη πληροφορίας	73
Εικόνα 4.2: Ο γράφος που χρησιμοποιήθηκε (με μορφή εικόνας)	75
Εικόνα 4.3: Διαδικασία ένθεσης.....	76
Εικόνα 4.4: Διαδικασία εξαγωγής.....	77
Εικόνα 4.5: Αρχική (αριστερά) και υδατογραφημένη (δεξιά) εικόνα	79
Εικόνα 5.1: Κατανομή εικόνων για διάφορες μετρήσεις PSNR	89
Εικόνα 5.2: Αρχική εικόνα – Υδατογραφημένη εικόνα.....	91
Εικόνα 5.3: Αρχική εικόνα – Υδατογραφημένη εικόνα.....	91
Εικόνα 5.4: Αρχική εικόνα – Υδατογραφημένη εικόνα.....	92
Εικόνα 5.5: Εφαρμογή υδατογράφησης.....	92
Εικόνα 6.1: Ένα επίπεδο αποσύνθεσης Wavelet	99
Εικόνα 6.2: Γενικό διάγραμμα των τεχνικών υδατογράφησης	99
Εικόνα 6.3: Διαδικασία ένθεσης.....	101
Εικόνα 6.4: Η διαδικασία υδατογράφησης.....	102
Εικόνα 6.5: (a) Η αρχική εικόνα, (b) το υδατογράφημα και (c) η υδατογραφημένη εικόνα	103
Εικόνα 6.6: Ομοιότητα έναντι της συμπίεσης JPEG	104
Εικόνα 6.7: (a) Η υδατογραφημένη εικόνα με κωδικοποίηση JPEG (ποιότητα 70%), (b) η υδατογραφημένη εικ. με Gaussian θόρυβο και (c) η υδατογραφημένη εικ. με φωτεινά εφέ.....	105
Εικόνα 6.8: SNR έναντι JPEG συμπίεσης.....	105

περιεχόμενα πινάκων

Εικόνα 2.1: Διάγραμμα συμμετρικής κρυπτογραφίας	28
Εικόνα 2.2: Κρυπτογραφικό σύστημα δημόσιου κλειδιού (<i>public key</i>)	29
Εικόνα 4.1: Παράγοντες που επιδρούν στην απόκρυψη πληροφορίας	73
Εικόνα 4.2: Ο γράφος που χρησιμοποιήθηκε (με μορφή εικόνας)	75
Εικόνα 4.3: Διαδικασία ένθεσης.....	76
Εικόνα 4.4: Διαδικασία εξαγωγής.....	77
Εικόνα 4.5: Αρχική (αριστερά) και υδατογραφημένη (δεξιά) εικόνα	79
Εικόνα 5.1: Κατανομή εικόνων για διάφορες μετρήσεις PSNR	89
Εικόνα 5.2: Αρχική εικόνα – Υδατογραφημένη εικόνα.....	91
Εικόνα 5.3: Αρχική εικόνα – Υδατογραφημένη εικόνα.....	91
Εικόνα 5.4: Αρχική εικόνα – Υδατογραφημένη εικόνα.....	92
Εικόνα 5.5: Εφαρμογή υδατογράφησης.....	92
Εικόνα 6.1: Ένα επίπεδο αποσύνθεσης Wavelet	99
Εικόνα 6.2: Γενικό διάγραμμα των τεχνικών υδατογράφησης	99
Εικόνα 6.3: Διαδικασία ένθεσης.....	101
Εικόνα 6.4: Η διαδικασία υδατογράφησης.....	102
Εικόνα 6.5: (a) Η αρχική εικόνα, (b) το υδατογράφημα και (c) η υδατογραφημένη εικόνα	103
Εικόνα 6.6: Ομοιότητα έναντι της συμπίεσης JPEG	104
Εικόνα 6.7: (a) Η υδατογραφημένη εικόνα με κωδικοποίηση JPEG (ποιότητα 70%), (b) η υδατογραφημένη εικ. με Gaussian θόρυβο και (c) η υδατογραφημένη εικ. με φωτεινά εφέ.....	105
Εικόνα 6.8: SNR έναντι JPEG συμπίεσης.....	105

Αρκτικόλεξα

DVD	Digital Video Disk
DWT	Discrete Wavelet Transform
HVS	Human Visual System
IP	Internet Protocol
IPRs	Intellectual Property Rights
MRA	Multi-Resolution Analysis
NP	Non-deterministically Polynomial
Pixel	Picture Element
PSNR	Peak Signal to Noise Ratio
RSA	Rivest Shamir Adleman
SAT	Satisfiability
SNR	Signal to Noise Ratio
URL	Uniform Resource Locator
WWW	World Wide Web
ZKIP	Zero Knowledge Interactive Proof Protocol

Πρόλογος

Η προστασία των πνευματικών δικαιωμάτων και η απόδειξη γνησιότητας του κατόχου, επομένως και η πιστοποίηση της αυθεντικότητας των ψηφιακών αντικειμένων είναι ένα πολύ καυτό ζήτημα και για την επίλυσή του επιστρατεύονται μέθοδοι απόκρυψης πληροφορίας και τεχνικές υδατογράφησης. Η δυσκολία τού προβλήματος δεν έγκειται μόνο στην εύρεση καλών μεθόδων και τεχνικών, αλλά και στη ομαλή συνεργασία πολλών ειδικών, όπως νομικών με τεχνικό επιστημονικό προσωπικό. Σε αυτήν τη διδακτορική διατριβή, εκτός από τη φιλοσοφική αντιμετώπιση του θέματος, προτείνονται μια μέθοδος απόκρυψης πληροφορίας και δύο τεχνικές υδατογράφησης, με σκοπό την προστασία των πνευματικών δικαιωμάτων και την πιστοποίηση της αυθεντικότητας των ψηφιακών αντικειμένων.

Η μέθοδος απόκρυψης πληροφορίας δανείζεται έννοιες από την κρυπτογραφία και εφαρμόζεται σε μεγάλες εικόνες εισάγοντας ένα δύσκολο στιγμιότυπο, δηλαδή έναν τρία χρωματίσιμο γράφο. Ο γράφος μαζί με το χρωματισμό του αποτελεί το κλειδί. Για να μην αποκαλυφθεί όλος ο χρωματισμός του γράφου σε μια πιθανή διαμάχη, εφαρμόζεται το πρωτόκολλο των διαντιδραστικών αποδείξεων μηδενικής γνώσης (ZKIP) για δύσκολα υπολογιστικά προβλήματα. Η διαδικασία της ένθεσης έγινε με χρήση του μετασχηματισμού wavelets, παρέχοντας καλή ποιότητα των παραγόμενων εικόνων και ανθεκτικότητα σε περιπτώσεις επιθέσεων.

Οι δύο τεχνικές υδατογράφησης εφαρμόζονται μία στο χωρικό πεδίο και μία στο πεδίο συχνοτήτων. Η τεχνική που εφαρμόστηκε στο χωρικό πεδίο εκμεταλλεύεται τυχόν ομοιότητες του υδατογραφήματος με τις αρχικές εικόνες για να επιλεγούν οι θέσεις ένθεσης. Αντίθετα στην τεχνική υδατογράφησης που εφαρμόστηκε στο πεδίο συχνοτήτων έγινε χρήση του μετασχηματισμού wavelet και επιχειρήθηκε η ένθεση της πλεονάζουσας πληροφορίας σε διαφορές τής εικόνας ώστε να μη γίνει αντιληπτή.

Σε όλες τις τεχνικές παρατηρήθηκαν ικανοποιητικά αποτελέσματα μετά την ένθεση της εισαγόμενης πληροφορίας έτσι ώστε να μη γίνεται οπτικά αντιληπτή. Επίσης εξετάστηκε και η ανθεκτικότητα της εισαγόμενης πληροφορίας στις εικόνες ύστερα από πιθανές επιθέσεις και επιβεβαιώθηκε ότι επιζεί ένα αρκετά μεγάλο ποσοστό της εισαγόμενης πληροφορίας, γεγονός που καταξιώνει τις προτεινόμενες μεθόδους.

Preface

The copyright protection and the authentication of digital objects is a very hot topic and for its solution are called up data hiding methods and watermarking techniques. The hardness of the problem is not just how to find out good methods and techniques, but also how well could collaborate many experts, for example lawyers with technical scientific staff. In this doctorship apart from the philosophical confrontation of the subject, there are proposed a data hiding method and two watermarking techniques that aim to copyright protect and the authenticate digital objects.

The data hiding technique combines concepts from cryptography and it can be applied to large images by inserting a hard instance, i.e. a 3-colorable graph. The graph itself with its coloring compose the key. In order not to reveal all its coloring in a possible conflict, the Zero Knowledge Interactive Proof Protocol (ZKIP) is applied. The insertion process has been done using wavelets transformation, offering good quality of the produced images and robustness against possible attacks.

The two watermarking techniques are applied one in spatial domain and one in frequency domain. The technique that was applied in spatial domain is exploiting any similarity between the watermark and the initial images so that to select at best the insertion positions. On the contrary, in the watermarking technique that is applied in the frequency domain, wavelets transformation has been used and the watermark was inserted in the differential coefficients of the image, in order to be imperceptible.

To all the above techniques, it has been observed sufficient results after the insertion of the redundant information, so that it turned to be visible imperceptibly. Moreover, the robustness of the redundant information was each time after possible attacks examined, and it was confirmed that a rather big percentage of the redundant information is survived, making more reliable the proposed techniques.

Κεφάλαιο 1

Αρχές απόκρυψης πληροφορίας:

Τεχνικές & επιδιώξεις

1.1. Εισαγωγή

Οι τεχνικές απόκρυψης πληροφορίας είναι πολλές. Μερικές από τις μεθόδους των συστημάτων απόκρυψης πληροφορίας είναι οι εξής [Kat2000]:

- ✓ Τα μυστικά κανάλια (*covert channels*) τα οποία ορίστηκαν από τον Lampson στο γενικό πλαίσιο των πολυεπίπεδων συστημάτων ασφαλείας ως μονοπάτια επικοινωνίας (*communication paths*) που ούτε είναι σχεδιασμένα, ούτε πρόκειται να μεταφέρουν καθόλου πληροφορία.
- ✓ Η ανωνυμία (*anonymity*) είναι η εύρεση τρόπων να αποκρύπτει κανείς το μετα-περιεχόμενο (*metacontent*) των μηνυμάτων, δηλαδή του αποστολέα και των αποδεκτών ενός μηνύματος. Οι εφαρμογές στο WEB εστιάζουν στην ανωνυμία του δέκτη (*receiver anonymity*), ενώ οι χρήστες του ηλεκτρονικού ταχυδρομείου ενδιαφέρονται για την ανωνυμία του αποστολέα (*sender anonymity*).

- ✓ Η κρυπτογραφία (*cryptography*) είναι η τέχνη, η μελέτη και η εργασία της κρυφής γραφής. Σε γενικές γραμμές συγκαλύπτει το νόημα ενός μυστικού μηνύματος.
- ✓ Οι ψηφιακές υπογραφές (*digital signatures*) είναι ψηφιακοί κώδικες που επισυνάπτονται σε μια ηλεκτρονική μεταφορά ενός μηνύματος, που όμως εξακριβώνει μοναδικά την ταυτότητα του αποστολέα. Αυτό επιτυγχάνεται είτε με ένθεση της ψηφιακής υπογραφής κατευθείαν στην επικεφαλίδα του αρχείου, είτε συσχετίζοντας ένα κλειδί με τα αρχικά δεδομένα για την παραγωγή μιας ψηφιακής υπογραφής και εισάγοντάς την στο αρχείο.
- ✓ Μια άλλη βασική τεχνική απόκρυψης πληροφορίας είναι η στεγανογραφία (*steganography*). Ενώ η κρυπτογραφία προστατεύει το περιεχόμενο ενός μηνύματος, η στεγανογραφία αποκαλύπτει την ύπαρξή του. Ο όρος στεγανογραφία προέρχεται από τις ελληνικές λέξεις "στεγανό-ς" και "γραφ-ειν" που σημαίνουν "καλυμμένη γραφή" και συνήθως μεταφράζονται ως η απόκρυψη πληροφορίας σε άλλη πληροφορία. Σε γενικούς όρους είναι η συγκαλύψη της ύπαρξης ενός μυστικού μηνύματος, και ορίζεται ως η τέχνη, η μελέτη και η εργασία της κρυφής γραφής [JoN2004].
- ✓ Η υδατογράφηση, αντίθετα προς τη στεγανογραφία, έχει την επιπλέον απαίτηση της ανθεκτικότητας (*robustness*) απέναντι σε πιθανές επιθέσεις. Εδώ ο όρος "ανθεκτικότητα" δεν είναι πολύ ξεκάθαρος, εξαρτάται κυρίως από την εφαρμογή, αλλά μια πετυχημένη επίθεση θα προσπαθήσει να σβήσει το υδατογράφημα. Τα υδατογραφήματα δεν απαιτούνται πάντα να είναι κρυμμένα, μια και μερικά συστήματα χρησιμοποιούν ορατά υδατογραφήματα, αλλά τα περισσότερα στη βιβλιογραφία επικεντρώνονται σε αόρατα, διάφανα, ή ανεπαίσθητα σε ήχο, αναφορικά με τη φύση των ψηφιακών αντικειμένων, ψηφιακά υδατογραφήματα.

Κρυπτογραφία έναντι Στεγανογραφίας

Η Κρυπτογραφία "ανακατεύει" ένα μήνυμα έτσι ώστε να μην είναι γνωστό το νόημά του. Αν ένα κρυπτογραφημένο μήνυμα υποκλαπεί, μπορεί να εκτιμηθεί ότι είναι ένα κρυπτογραφημένο μήνυμα και να οδηγήσει κάποιον σε κρυπτανάλυση (*cryptanalysis* - σπάσιμο του κώδικα).

Από την άλλη μεριά η στεγανογραφία κρύβει την ύπαρξη ενός μηνύματος, έτσι ώστε αν ο φορέας του μηνύματος (*cover*) υποκλαπεί, να μην αποκαλύψει την ύπαρξη του συγκαλυμμένου μηνύματος.

Στεγανογραφία έναντι Υδατογράφησης

Το αόρατο υδατογράφημα και η στεγανογραφία αντιλαμβάνονται συχνά ως συναφείς διαδικασίες, αλλά διαφέρουν βασικά ως προς το σκοπό της χρήσης. Ένα υδατογράφημα μπορεί να γίνει αντιληπτό σαν ένα χαρακτηριστικό του φορέα (*carrier - cover*). Μπορεί να περιέχει πληροφορία όπως είναι τα δικαιώματα πνευματικής ιδιοκτησίας, η εξουσιοδότηση, η πορεία της πληροφορίας και η πατρότητα ενός συγγράμματος. Στη στεγανογραφία όμως το μήνυμα που εντίθεται μπορεί να μην έχει καμία σχέση με το φορέα του μηνύματος.

Οι τεχνικές στεγανογραφίας και υδατογραφήματος τείνουν να έχουν συγκρουόμενους σκοπούς. Στη στεγανογραφία ένα θέμα που μας αφορά είναι το εύρος ζώνης (*bandwidth*) του ωφέλιμου φορτίου (*payload*), δηλαδή του κρυφού μηνύματος, ενώ η ανθεκτικότητα αφορά κυρίως τεχνικές υδατογράφησης. Γι' αυτόν το λόγο, πολλές τεχνικές υδατογράφησης εκμεταλλεύονται τα μη σημαντικά δυαδικά ψηφία και το θόρυβο, για να αποκρύψουν πληροφορία, ενώ τα υδατογραφήματα ενθέτονται στις πιο ευδιάκριτες ή αισθητές (*perceptible*) περιοχές του φορέα σαν ένα μέσο προστασίας ως προς διάφορους μετασχηματισμούς. Τα υδατογραφήματα είναι συνήθως υπεράριθμα διασκορπισμένα μέσα στο φορέα για να βοηθήσουν στην προστασία από αποκοπή του αρχείου (*cropping*).

1.2. Γενική Θεώρηση του προβλήματος

Η παρούσα διδακτορική διατριβή διαπραγματεύεται το ζήτημα της προστασίας των πνευματικών δικαιωμάτων των δημιουργών, καθώς και την απόδειξη γνησιότητας των ψηφιακών αντικειμένων και επικεντρώνεται κυρίως σε ψηφιακές εικόνες ή σαρωμένα έγγραφα.

Το ζήτημα αυτό είναι πολύ παλιό και ξεκινάει από την εποχή που υπήρχε η πρώτη ανάγκη για προστασία των πνευματικών δικαιωμάτων και για απόδειξη γνησιότητας αντικειμένων που ήταν τυπωμένα σε χαρτί. Για τις ανάγκες εκείνης της εποχής είχαν προταθεί τεχνικές υδατογράφησης σε χαρτί που χρησιμοποιούνται ακόμα και σήμερα σε ανάλογες περιπτώσεις. Με την εξέλιξη όμως της τεχνολογίας

τα έγγραφα και οι εικόνες έπαψαν να βρίσκονται αποκλειστικά και μόνο τυπωμένα σε χαρτί και άρχισαν να υπάρχουν σε ψηφιακή μορφή, γεγονός που απαιτούσε νέες μεθόδους προστασίας. Κατ' αναλογία των παλιών υδατογραφημάτων προτάθηκαν νέες μέθοδοι ψηφιακής υδατογράφησης, μεταφέροντας πληροφορία όπως είναι τα δικαιώματα πνευματικής ιδιοκτησίας, η εξουσιοδότηση, η πορεία της πληροφορίας και η πατρότητα ενός συγγράμματος.

1.3. Η συνεισφορά μας

Με το πέρασμα των αιώνων και κυρίως με τη συμβολή της τεχνολογίας το πρόβλημα έγινε πολύ πιο σύνθετο από παλιά. Δεν είναι λίγες οι φορές που στη βιβλιογραφία προτείνεται μονομερής αντιμετώπιση του θέματος, επιχειρώντας να επεκτείνουν τα παλιά υδατογραφήματα χαρτιού σε μοντέρνα ψηφιακά υδατογραφήματα. Η ευστοχία της παρούσας διδακτορικής διατριβής είναι ότι αντιμετωπίζει το ζήτημα σφαιρικά, χωρίς να αγνοεί ότι ακόμα και η πιο τέλεια τεχνική για την προστασία των πνευματικών δικαιωμάτων είναι άχρηστη, όταν δεν συνοδεύεται από εκούσια συμμετοχή και συνεργασία όλων των χρηστών του ψηφιακού δικτυακού τόπου.

Συνεπώς εφαρμόζονται δύο ειδών προσεγγίσεις: μια ανθρωποκεντρική και μια τεχνοκεντρική θεώρηση του προβλήματος. Στην πρώτη μορφή αντιμετώπισης του προβλήματος γίνεται λόγος για τη διαφορετική συμπεριφορά που επιδεικνύουν πολλοί χρήστες του διαδικτύου, καθώς και οι συνθήκες που τους οδηγούν σε ενέργειες, αγνοώντας τα πνευματικά δικαιώματα. Εντοπίζεται η ανάγκη για κατάλληλη διαπαιδαγώγηση των χρηστών και μάλιστα από μικρή ηλικία, αφήνοντας στους κοινωνιολόγους το πώς θα μπορούσε να γίνει κάτι τέτοιο με τον πιο ανώδυνο τρόπο. Περιγράφονται επιπλέον κάποιοι κώδικες δεοντολογίας που ήδη διέπουν τη συμπεριφορά των χρηστών στο διαδίκτυο και γίνεται σύνδεση αυτών με τεχνικές υδατογράφησης και κρυπτογραφίας.

Στη δεύτερη μορφή αντιμετώπισης του προβλήματος ερευνούνται ισχυρές τεχνικές προστασίας. Υπάρχουν στη βιβλιογραφία πάμπολλες αξιόλογες τεχνικές με μεγάλη ποικιλία και με ευρεία γκάμα εφαρμογής τους. Αυτές χωρίζονται σε τεχνικές απόκρυψης πληροφορίας και σε τεχνικές υδατογράφησης. Στις πρώτες ο όγκος της πληροφορίας που ενθέτεται είναι αρκετά μεγάλος, δεν είναι ανθεκτικές σε επιθέσεις και εφαρμόζονται για προσδιορισμό ταυτότητας, για σχολιασμό, για ανίχνευση πλαστογράφησης ή παραποίησης και λιγότερο για προστασία πνευματικών

δικαιωμάτων. Αντίθετα στις τεχνικές υδατογράφησης, ο όγκος της πληροφορίας που ενθέτεται είναι μικρός, υπάρχει πολλαπλή ένθεση, θεωρούνται ανθεκτικές και εφαρμόζονται για πιστοποίηση αυθεντικότητας των ψηφιακών αντικειμένων, για αναγνώριση του δημιουργού, για προστασία έναντι παραβιάσεων πνευματικής ιδιοκτησίας, για πιστοποίηση των νόμιμων κατόχων και για την παρεμπόδιση κάποιων από την ιδιοποίηση ξένης πνευματικής ιδιοκτησίας.

Το πρόβλημα που συνήθως αντιμετωπίζουν οι περισσότερες τεχνικές για την προστασία των πνευματικών δικαιωμάτων είναι ότι αν για κάποιο λόγο η υπογραφή ή το υδατογράφημα εξαχθεί ή υποκλαπεί μπορεί να χρησιμοποιηθεί άνετα από μη εξουσιοδοτημένους χρήστες. Το πρόβλημα αυτό δεν μας οδήγησε στην κατάργηση των τεχνικών υδατογράφησης αλλά στην ενίσχυση τους με μεθόδους απόκρυψης πληροφορίας, εισάγοντας πολλαπλή προστασία. Επιλύουμε συνεπώς το πρόβλημα αυτό συνδυάζοντας χαρακτηριστικά από τεχνικές απόκρυψης πληροφορίας με χαρακτηριστικά τεχνικών ψηφιακής υδατογράφησης και εισάγοντας σαν υπογραφή ένα δύσκολο στιγμιότυπο και πιο συγκεκριμένα έναν τρία χρωματίσιμο γράφο. Ως εκ τούτου, ακόμα και αν υποκλαπεί ο γράφος, ο νόμιμος κάτοχος είναι μόνο αυτός που γνωρίζει τον τρία χρωματισμό του.

Αναζητώντας παρόμοιες εργασίες που έχουν γίνει στο παρελθόν συναντάμε στο [QuG1998] τους Qu και Potkonjak που πρότειναν μια μέθοδο υδατογράφησης για το πρόβλημα του χρωματισμού των γράφων, πράγμα που σχετίζεται με γράφους και την υδατογράφηση, αλλά είναι πολύ διαφορετικό από τη χρήση των ίδιων των γράφων για την υδατογράφηση εικόνων. Δύο χρόνια νωρίτερα από τους Qu και Potkonjak, είχε κάνει την εμφάνισή του ο Hirotsugu [Hir1996], οποίος δημιουργούσε ένα γράφο από μια εικόνα και απέκρυπτε έναν ισομορφικό γράφο στην ίδια εικόνα. Στη συνέχεια εκτελούσε το πρωτόκολλο των διαντιδραστικών αποδείξεων μηδενικής γνώσης για επιβεβαίωση των πνευματικών δικαιωμάτων. Και τρία χρόνια μετά τον Hirotsugu δημοσιεύει ο Craver [Cra1999] μια εργασία, στην οποία αναφέρεται πως θα μπορούσε να εφαρμοστεί το πρωτόκολλο των διαντιδραστικών αποδείξεων μηδενικής γνώσης για τον ισομορφισμό των γράφων και επιπλέον παρουσιάζει πως θα μπορούσαν να υπάρχουν τεχνικές υδατογράφησης με εφαρμογή του πρωτοκόλλου των διαντιδραστικών αποδείξεων μηδενικής γνώσης σε δύσκολα προβλήματα, αναφέροντας το πρόβλημα της εύρεσης της Χαμιλτόνιας πορείας σε ένα γράφο. Σύμφωνα με τα προηγούμενα είναι ισχυρή η πεποίθηση ότι η εργασία που παρουσιάζεται εδώ σε τεχνικό επίπεδο είναι πρωτότυπη και πολύ πιο απλή και εφαρμόσιμη από τις τεχνικές που έχουν ήδη προταθεί, αφήνοντας μάλιστα

περιθώρια έρευνας για δημιουργία ακόμα πιο δύσκολων τρία χρωματίσιμων γράφων. Για βέλτιστη προστασία, προτείνεται η ταυτόχρονη χρήση περισσοτέρων της μιας τεχνικής προστασίας πνευματικών δικαιωμάτων. Συνεπώς, η προαναφερθείσα τεχνική απόκρυψης πληροφορίας θα μπορούσε να συνδυαστεί κάλλιστα με μια ή περισσότερες κλασσικές μεθόδους υδατογράφησης.

Μέσα από την ερευνητική αυτή εργασία γίνεται φανερή η ανάγκη θέσπισης νόμων που θα συνταιριάζει τα ηλεκτρονικά συστήματα διαχείρισης πνευματικών δικαιωμάτων, καθώς και η καθιέρωση κάποιων κοινά αποδεκτών τεχνικών για την προστασία των πνευματικών δικαιωμάτων. Περαιτέρω έρευνα στο συγκεκριμένο σημείο όμως δεν άπτεται της παρούσας διδακτορικής διατριβής.

1.4. Περιληπτική σκιαγράφηση

Η παρούσα διδακτορική διατριβή διαπραγματεύεται τεχνικές απόκρυψης πληροφορίας συμπεριλαμβανομένης και της υδατογράφησης που σκοπό έχουν την προστασία των πνευματικών δικαιωμάτων, καθώς και την απόδειξη γνησιότητας των ψηφιακών αντικειμένων.

Στο δεύτερο κεφάλαιο ερευνώνται κώδικες δεοντολογίας που είναι κρυμμένοι πίσω από διαφορετικούς τύπους μηχανισμών ασφαλείας [ArC2002]. Οι ανθρώπινες σχέσεις βασίζονται κυρίως σε κώδικες δεοντολογίας (*ethics*). Ο ρόλος του κώδικα δεοντολογίας θα πρέπει να είναι συμβουλευτικός και όχι επιβλητικός. Η επιβολή θα πρέπει να αφεθεί στους νόμους, ενώ οι κώδικες δεοντολογίας θα πρέπει να έχουν το προβάδισμα έναντι των νόμων, αφήνοντας τους ανθρώπους να οριοθετήσουν τη συμπεριφορά τους.

Υπάρχουν τρεις κύριες κατευθύνσεις για την ασφάλεια των ψηφιακών αντικειμένων. Αυτές είναι η κρυπτογραφία, ψηφιακές υπογραφές και η ψηφιακή υδατογράφηση. Η κρυπτογραφία αναφέρεται στην τέχνη της επιστήμης για την μετάφραση απλής πληροφορίας σε ακατανόητη και για την επαναφορά της σε κατανοητή, οι ψηφιακές υπογραφές εστιάζουν στην ακεραιότητα των δεδομένων, ενώ οι τεχνικές υδατογράφησης, προσθέτοντας μια επιπλέον πληροφορία στα δεδομένα παρέχουν προστασία των πνευματικών δικαιωμάτων και απόδειξη γνησιότητας του περιεχομένου.

Η υιοθέτηση μιας εκ των τριών τεχνικών που εξετάστηκαν αφορά καθαρά την εφαρμογή και την πρόθεση αυτών που θα κάνουν την επιλογή. Τα κρυπτογραφικά

συστήματα χρησιμοποιούνται μόνο για συγκεκριμένες εφαρμογές, κυρίως δε για τη μεταφορά εμπιστευτικών μηνυμάτων και θεωρούνται οι πιο *αυστηρές* από όλες τις τεχνικές. Μια ψηφιακή υπογραφή είναι ένας ψηφιακός κώδικας που επισυνάπτεται σε μια ηλεκτρονική μεταφορά του μηνύματος, που όμως εξακριβώνει μοναδικά την ταυτότητα του αποστολέα. Αν τα προϊόντα αυτά τροποποιηθούν τότε δε δίνεται εγγύηση για την επιβεβαίωση του κατόχου, ούτε και της ακεραιότητας των δεδομένων. Στις ψηφιακές υπογραφές ο χρήστης είναι εντελώς ελεύθερος να διαβάσει το αρχείο, αλλά και να τις καταστρέψει, γι' αυτό και οι ψηφιακές υπογραφές θεωρούνται πολύ *φιλελεύθερες*. Αντίθετα κατά την υδατογράφιση, ο καθένας μπορεί να διαβάσει και να επεξεργάζεται τα προστατευμένα αρχεία με τη μόνη διαφορά ότι τα υδατογραφήματα μπορούν να αποδείξουν και να προστατεύσουν τον κάτοχο, οπότε κατά μια έννοια η υδατογράφιση ισορροπεί ανάμεσα στην *αυστηρότητα* και την *απόλυτη ελευθερία*.

Στο τρίτο κεφάλαιο επιχειρείται σύνδεση της έρευνας με τη φιλοσοφία [ArL2002]. Σύμφωνα με τον Καντ «ένα αντίγραφο είναι εργασία της δουλειάς του συγγραφέα». Η πνευματική ιδιοκτησία είναι μια διακριτική και εσωτερική περιοχή του νόμου που αναπτύσσεται σε απόκριση των τεχνολογικών αλλαγών. Η επιβολή των νόμων ωστόσο δεν είναι αποδοτική αν δεν συνοδεύεται από την ελεύθερη βούληση των ανθρώπων. Για να υπακούουν οι άνθρωποι σε ηθικές αξίες και κατ' επέκταση σε νόμους, επιβάλλεται κατάλληλη ενημέρωση και διαπαιδαγώγηση από μικρή ηλικία.

Σύμφωνα με τον Παγκόσμιο Οργανισμό Πνευματικών Δικαιωμάτων η πνευματική ιδιοκτησία μπορεί να χαρακτηριστεί σαν καρπός της ανθρώπινης δημιουργίας και επινόησης. Η προστασία των πνευματικών δικαιωμάτων είναι πολύ δύσκολη και η τεχνολογία προσπαθεί να συμβάλλει προς αυτήν την κατεύθυνση με την υδατογράφιση. Ο έλεγχος για υδατογραφημένα ψηφιακά αντικείμενα δε θα μπορούσε να είναι καθολικός, αλλά μια εξουσιοδοτημένη ομάδα θα μπορούσε σε τακτά χρονικά διαστήματα να πραγματοποιεί ελέγχους και να πιστοποιεί την αυθεντικότητα των ψηφιακών αντικειμένων ή τη νόμιμη κυριότητα των κατόχων τους, τιμωρώντας τους παραβάτες.

Στο τέταρτο κεφάλαιο προτείνεται μια μέθοδος απόκρυψης πληροφορίας που μπορεί να χρησιμοποιηθεί για να αποδειχθεί η κατοχή πνευματικής ιδιοκτησίας, εισάγοντας την έννοια μιας κρυπτογραφικά ασφαλούς υπογραφής κατ' αναλογία με τις γεννήτριες κρυπτογραφικά ασφαλών ψευδοτυχαίων αριθμών [Arm2003, ACK2002, ArC2001]. Αυτή η μέθοδος βασίζεται στην ένθεση μιας υπογραφής στα

αρχικά δεδομένα, αλλά αντί να χρησιμοποιηθεί η υπογραφή η ίδια, χρησιμοποιείται ένα συγκεκριμένο μετα-χαρακτηριστικό της υπογραφής για να αποδειχθεί η κυριότητα των ψηφιακών αντικειμένων.

Όλες οι παρόμοιες τεχνικές καλούνται να επιλύσουν τα εξής δύο προβλήματα: α) το γεγονός ότι οποιοσδήποτε μπορεί να χρησιμοποιήσει την ψηφιακή υπογραφή για να ισχυριστεί το νόμιμο κάτοχο των δεδομένων (που παρέχονται και από τα οποία έχει κλαπεί η υπογραφή), και (β) το γεγονός ότι η αύξηση του μεγέθους της υπογραφής είτε κάνει τη μέθοδο λιγότερο ανθεκτική σε επιθέσεις (όπως στην περίπτωση μεγάλου μη επαναλαμβανόμενου όγκου δεδομένων υπογραφών), είτε κάνει το μη εξουσιοδοτημένο εντοπισμό και άρα και την εξαγωγή της υπογραφής ευκολότερη.

Η προτεινόμενη τεχνική εστιάζει (α) στη μετατόπιση του ενδιαφέροντος από *το πώς φαίνονται οι υπογραφές των χρηστών*, σαν ακολουθία δυαδικών ψηφίων, στο *τι αναπαριστούν οι υπογραφές των χρηστών*, και (β) τη χρήση του *μετασχηματισμού wavelet* με σκοπό την ένθεση υπογραφών, ώστε να εισάγεται η μικρότερη παραμόρφωση, να γίνεται ανθεκτικότερη η υπογραφή και να διατηρείται η ποιότητα του ψηφιακού αντικειμένου.

Η κατασκευή των υπογραφών που προτείνονται είναι άρρηκτα συνδεδεμένες με τις γνωστές *Διαντιδραστικές Αποδείξεις Μηδενικής Γνώσης (Zero Knowledge Interactive Proof protocol)* για δύσκολα υπολογιστικά προβλήματα (*computationally intractable problems*) ή μη ντετερμινιστικού χρόνου επίλυσης (*NP - complete*), και ιδιαίτερα στα προβλήματα χρωματισμού γράφων με τρία χρώματα. Εκμεταλλευόμενοι την υπολογιστική πολυπλοκότητα αυτού του προβλήματος, προτείνεται η κατασκευή μεγάλων υπογραφών που αναπαριστούν τους πίνακες γειτνίασης τυχαίων 3-χρωματίσιμων γράφων. Το κύριο πλεονέκτημα της προτεινόμενης μεθόδου βασίζεται στην ιδέα ότι ο γράφος μαζί με τον 3-χρωματισμό των κορυφών του παίζει το ρόλο της υπογραφής και η αναγνώρισή της δεν επηρεάζεται από την επίδειξη του ίδιου του γράφου. Αντίθετα η αναγνώριση της υπογραφής επηρεάζεται από την επίδειξη της γνώσης του 3-χρωματισμού, το οποίο βάσει της θεωρίας πολυπλοκότητας δεν είναι εύκολο να βρεθεί. Έτσι, ακόμα και αν κάποιος κλέψει την υπογραφή, δε θα είναι δυνατόν να υποδυθεί τον νόμιμο κάτοχο των δεδομένων, εφόσον απαιτείται ο 3-χρωματισμός για να προσδιοριστεί η ταυτότητα του.

Θα πρέπει να δοθεί έμφαση ότι σε αυτή την περίπτωση η ανθεκτικότητα της υπογραφής έναντι των επιθέσεων δεν βρίσκεται μόνο στη διαδικασία ένθεσης, αλλά

επίσης και στα χαρακτηριστικά του γράφου, γι' αυτό το λόγο η κυριότητα των πνευματικών δικαιωμάτων μπορεί να καθοριστεί ακόμα και αν ένα μικρό τμήμα του γράφου επιζήσει από τις επιθέσεις (εφόσον όπως αναφέρθηκε ο 3-χρωματισμός του ακόμα αποτελεί ένα δύσκολο συνδυαστικά πρόβλημα).

Η πνευματική ιδιοκτησία των δεδομένων προστατεύεται από ένα πρωτόκολλο (τις Διαντιδραστικές Αποδείξεις Μηδενικής Γνώσης) που αποδεικνύει τη νόμιμη κατοχή και συγχρόνως αποφεύγει την αποκάλυψη της υπογραφής. Οπότε στο κεφάλαιο αυτό παρουσιάζεται το συγκεκριμένο πρωτόκολλο προσαρμοσμένο στην περίπτωση της αποκάλυψης του 3-χρωματισμού των γράφων, καθώς γίνεται και μια σύντομη περιγραφή στην NP-Complete θεωρία για την παραγωγή τυχαίων και δύσκολων στιγμιότυπων που θα παίξουν τον ρόλο της υπογραφής. Τέλος, δίνεται η διαδικασία απόκρυψης δεδομένων με χρήση των wavelets και τα πειραματικά αποτελέσματα που αναδεικνύουν την ανθεκτικότητα της μεθόδου, καθώς και την καλή ποιότητα των παραγόμενων εικόνων.

Στο πέμπτο κεφάλαιο προτείνεται μια μέθοδος υδατογράφησης που πραγματοποιείται στο χωρικό πεδίο [Arm2000, Arm1999]. Το υδατογράφημα εντίθεται στο μπλε κανάλι των εικόνων σε συγκεκριμένες θέσεις που εγγυώνται την ελαχιστοποίηση των δυαδικών ψηφίων που τροποποιούνται. Η διαδικασία ένθεσης εφαρμόζεται και στα 8 επίπεδα του μπλε καναλιού, διαμοιράζοντας τα υδατογραφήματα ανομοιόμορφα και ενθέτοντας λιγότερα υδατογραφήματα στα περισσότερα σημαντικά επίπεδα και περισσότερα στα λιγότερα σημαντικά επίπεδα.

Αποδεικνύεται πειραματικά και θεωρητικά ότι η ύπαρξη προϋπάρχοντων υδατογραφημάτων είναι αμελητέα, ενώ η πιστοποίηση των υδατογραφημένων εικόνων ακόμα και μετά από πιθανές πολλαπλές επιθέσεις συνιστά την επιτυχία της μεθόδου. Αυτή η πιστοποίηση γίνεται με βάση τρία κριτήρια, το λόγο PSNR, το κριτήριο της ομοιότητας καθώς και το ανθρώπινο οπτικό σύστημα.

Στο έκτο κεφάλαιο προτείνεται μια ασφαλής μέθοδος υδατογράφησης στο πεδίο των συχνοτήτων [Arm2001]. Η μέθοδος αυτή εφαρμόζεται σε κείμενα που έχουν περάσει από το σαρωτή και τα μεταχειριζόμαστε πλέον σαν εικόνες. Το υδατογράφημα ύστερα από μια προεπεξεργασία στην οποία υπόκειται, εντίθεται στους συντελεστές που αντιπροσωπεύουν τις λεπτομέρειες σε μια εικόνα. Μια τέτοια τεχνική θα μπορούσε να φανεί χρήσιμη σε βάσεις δεδομένων των μουσείων που αποθηκεύουν και σαρώνουν πολύτιμα έγγραφα.

Πειραματικά αποτελέσματα αποδεικνύουν ότι αυτή η μέθοδος δεν επηρεάζει οπτικά μια εικόνα και επιπλέον το υδατογράφημα αποδεικνύεται ότι είναι ανθεκτικό,

εφόσον μπορεί να ανιχνευτεί ακόμα και μετά από τροποποιήσεις της εικόνας. Χρησιμοποιήθηκε η μετρική της ομοιότητας ως κριτήριο για την ανίχνευση του υδατογραφήματος. Τα πειράματα έδειξαν ότι η προτεινόμενη μέθοδος έχει αρκετά καλή συμπεριφορά σε συμπίεση JPEG και το υδατογράφημα παραμένει ανιχνεύσιμο ακόμα και σε υψηλούς ρυθμούς συμπίεσης. Αλλά και μετά από άλλες τροποποιήσεις της υδατογραφημένης εικόνας αποδεικνύεται ότι η προτεινόμενη μέθοδος μπορεί να χαρακτηριστεί ανθεκτική, διατηρώντας ένα από τα κύρια πλεονεκτήματα της μεθόδου, ότι δηλαδή διατηρείται το υδατογράφημα εντελώς αόρατο αφήνοντας το αρχικό σαρωμένο κείμενο σχεδόν ανέπαφο.

Τέλος στο έβδομο και τελευταίο κεφάλαιο δίνονται πιθανές εξελίξεις των ζητημάτων που συζητήθηκαν σε προηγούμενα κεφάλαια και πώς θα μπορούσε να αντιμετωπιστεί συλλογικά το θέμα της προστασίας των πνευματικών δικαιωμάτων και της πιστοποίησης της αυθεντικότητας.

Κεφάλαιο 2

Φιλοσοφική υπόσταση των συστημάτων ασφαλείας στα πληροφοριακά συστήματα

2.1. Εισαγωγή

Η ηθική ως κώδικας δεοντολογίας προβάλλει κανόνες στο γενικό πλαίσιο των μηχανισμών ασφαλείας στα πληροφοριακά συστήματα. Οι μηχανισμοί ασφαλείας στον ηλεκτρονικό κόσμο, ιδιαίτερα δε στο Διαδίκτυο, παίζουν έναν παρόμοιο ρόλο με το ρόλο των νόμων στην οργανωμένη κοινωνία. Ο κύριος στόχος τους είναι να παρέχουν προστασία στους κατόχους των ηλεκτρονικών περιουσιών, όπως είναι οι τίτλοι πολυμέσων, τα αρχεία ήχου, εικόνων, βίντεο, είτε ακόμα και απλών κειμένων. Στον πραγματικό κόσμο υπάρχουν πολλοί κώδικες δεοντολογίας αναφορικά με την έννοια της ιδιοκτησίας. Το ίδιο φαινόμενο παρατηρείται και στον ηλεκτρονικό κόσμο. Σε αυτό το κεφάλαιο διαπραγματεύονται θέματα που δείχνουν πως πολλά ζητήματα μεταφέρονται από τον πραγματικό στον ηλεκτρονικό κόσμο. Και πιο συγκεκριμένα ερευνώνται εδώ κώδικες δεοντολογίας που είναι κρυμμένοι πίσω από διαφορετικούς τύπους μηχανισμών ασφαλείας. Θα μελετηθεί καθένας μηχανισμός ασφαλείας ξεχωριστά και στη συνέχεια θα υπάρξει σύγκριση μεταξύ τους

ερευνώντας πώς οι κανόνες δεοντολογίας διαφοροποιούνται σε σχέση με τη φύση καθενός μηχανισμού ασφαλείας.

Στις μέρες μας η ανάπτυξη και η διανομή ψηφιακών προϊόντων πληροφορίας είναι γρήγορη και ανέξοδη, εξαιτίας της ραγδαίας ανάπτυξης των νέων τεχνολογιών, όπως το Διαδίκτυο. Θα μπορούσε να δει κανείς το διαδίκτυο σαν ένα σύνολο αυτόνομων υποδικτύων που επικοινωνούν μέσω του IP πρωτοκόλλου (*Internet Protocol*) [Ste1994]. Αυτό το πρωτόκολλο παρέχει ομοιόμορφη σύνδεση, παρόλη την ποικιλία του Διαδικτύου, αλλά φυσικά δεν παρέχει ομοιόμορφη συμπεριφορά. Έτσι λοιπόν εξαιτίας της φύσης του, το Διαδίκτυο δεν μπορεί να ελεγχθεί με κεντρικό τρόπο. Από την άλλη μεριά στην οργανωμένη κοινωνία ασφάλεια σημαίνει και επιβολή κάποιων κανόνων στην ηλεκτρονική κοινότητα που έχουν σχέση με το Διαδίκτυο. Σε ένα τέτοιο περιβάλλον ανακύπτει ένα πολύ σοβαρό πρόβλημα: *τα ψηφιακά αντικείμενα είναι εκτεθειμένα σε πολλές τροποποιήσεις (ηθελημένες ή όχι)*. Κάτω από αυτές τις συνθήκες είναι αδιαμφισβήτητη η ανάγκη για την εισαγωγή νέων εργαλείων και μηχανισμών που διασφαλίζουν την προστασία των ψηφιακών αντικειμένων, όπως είναι η προστασία των πνευματικών δικαιωμάτων ή η απόδειξη γνησιότητας των αντικειμένων.

Η προστασία των ψηφιακών αντικειμένων σκοπεύει στη διατήρηση των πνευματικών δικαιωμάτων ιδιοκτησίας (*Intellectual Property Rights - IPRs*) σχετικά με την κυριότητα ή τη χρήση τους. Η προστασία των IPRs επηρεάζει κυρίως τις ανθρώπινες συναλλαγές και συνεπώς τις ανθρώπινες σχέσεις. Οι ανθρώπινες σχέσεις βασίζονται κυρίως σε κώδικες δεοντολογίας (*ethics*). Έτσι η προστασία των πνευματικών αντικειμένων είναι ένας νέος τομέας στον οποίο οι κώδικες δεοντολογίας θα είναι πολύ σημαντικοί, όπως συμβαίνει και με όλες τις πλευρές των ανθρώπινων παρεμβάσεων. Ο ρόλος του κώδικα δεοντολογίας θα πρέπει να είναι συμβουλευτικός και όχι επιβλητικός. Η επιβολή θα πρέπει να αφεθεί στους νόμους, ενώ οι κώδικες δεοντολογίας θα πρέπει να έχουν το προβάδισμα έναντι των νόμων, αφήνοντας τους ανθρώπους να θέσουν τα όριά τους. Σύμφωνα με αυτόν το συλλογισμό θα μπορούμε να μιλάμε για *κώδικα δεοντολογίας* υπολογιστών (*computer ethics*), εφόσον η κοινωνία των υπολογιστών κατ' ουσία «αντιγράφει» την πραγματική κοινωνία (το εμπόριο εξελίσσεται σε ηλεκτρονικό εμπόριο, το ταχυδρομείο σε ηλεκτρονικό ταχυδρομείο κ.ά.).

Τα ψηφιακά αντικείμενα από τη φύση τους έχουν διαφορετικές και πολλές φορές αντικρουόμενες απαιτήσεις για ασφάλεια. Για παράδειγμα τα αρχεία ήχου χρειάζονται την ένθεση διαφανών υπογραφών για την εγγύηση των IPRs των

κατόχων, ενώ το περιεχόμενο των εικόνων θα πρέπει να παραμείνει ανέπαφο για τη διατήρηση της γνησιότητάς του. Υπάρχουν τρεις κύριες κατευθύνσεις για την ασφάλεια των ψηφιακών αντικειμένων. Η μια κατεύθυνση στην ψηφιακή ασφάλεια είναι η κρυπτογραφία. Ο κύριος στόχος της κρυπτογραφίας είναι η μεταφορά των ψηφιακών αντικειμένων σε μια μορφή η οποία να μην είναι προσιτή, αλλά μη αναγνωρίσιμη από μη εξουσιοδοτημένους χρήστες. Η δεύτερη κατεύθυνση αφορά ψηφιακές υπογραφές, οι οποίες εστιάζουν στην ακεραιότητα των δεδομένων εξασφαλίζοντας ότι ο χρήστης έχει πρόσβαση στο πρωταρχικό αρχείο. Τέλος, οι τεχνικές υδατογράφησης έρχονται να ενισχύσουν τις ψηφιακές υπογραφές, προσθέτοντας μια επιπλέον πληροφορία στα δεδομένα, χωρίς όμως να επηρεάζουν την ποιότητα του προϊόντος, παρέχοντας έτσι προστασία των πνευματικών δικαιωμάτων και απόδειξη γνησιότητας του περιεχομένου.

Σε αυτό το κεφάλαιο συζητιούνται θέματα που προκύπτουν από την έννοια της ιδιοκτησίας, έτσι όπως εμφανίζεται στον πραγματικό κόσμο και πώς αυτά τα θέματα μεταφέρονται στον ηλεκτρονικό κόσμο. Γίνεται μια ανάλυση της δεοντολογίας και των κωδίκων ηθικής που υπάρχουν πίσω από κάθε είδος μηχανισμού ασφαλείας και παρέχεται μια σύγκριση μεταξύ τους. Ιδιαίτερα δε δεικνύεται πώς οι κανόνες δεοντολογίας διαφοροποιούνται ανάλογα με τη φύση του κάθε μηχανισμού ασφαλείας.

2.2. Κρυπτογραφία

Καθώς το Διαδίκτυο και γενικότερα ο τρόπος της ηλεκτρονικής επικοινωνίας γίνεται επικρατέστερο, η ηλεκτρονική ασφάλεια γίνεται όλο και περισσότερο σημαντική. Η κρυπτογραφία (*cryptography*) χρησιμοποιείται σε διάφορες εφαρμογές επιβάλλοντας προστασία σε πληροφορίες των πιστωτικών καρτών, σε μηνύματα του ηλεκτρονικού ταχυδρομείου, και γενικά σε μεταδιδόμενα δεδομένα. Η ορολογία *κρυπτογραφία* αναφέρεται στην τέχνη της επιστήμης που αφορά τις αρχές, τα μέσα και τις μεθόδους για τη μετάφραση απλής πληροφορίας σε ακατανόητη και για την επαναφορά της σε κατανοητή [INF2004].

Έτσι η κρυπτογραφία αντιπροσωπεύει την τέχνη της προστασίας της πληροφορίας με τη μετατροπή της (με την κωδικοποίησή της – π.χ. μεταφράζοντάς την σε κάποιον μυστικό κώδικα) σε μη αναγνώσιμη μορφή, που ονομάζεται κρυπτογράφημα (*cipher text*). Μόνο αυτοί που κατέχουν το μυστικό κλειδί (*secret*

key) μπορούν να αποκρυπτογραφήσουν τα κωδικοποιημένα δεδομένα στην αρχική τους μορφή. Τα κωδικοποιημένα μηνύματα μπορούν μερικές φορές να σπάσουν με την κρυπτανάλυση (*cryptanalysis* ή *code-breaking*), παρόλο που οι μοντέρνες τεχνικές κρυπτογραφίας είναι θεωρητικά άτρωτες [Web2004]. Τα συστήματα κρυπτογραφίας μπορούν γενικά να διαχωριστούν σε συστήματα συμμετρικού κλειδιού (*symmetric-key systems*), που χρησιμοποιούν ένα και μοναδικό κλειδί, που είναι γνωστό σε αποστολέα και αποδέκτη, και σε συστήματα δημόσιου κλειδιού (*public-key systems*), που χρησιμοποιούν δύο κλειδιά: ένα δημόσιο κλειδί (*public key*) γνωστό σε όλους και ένα εμπιστευτικό κλειδί (*private key*) που χρησιμοποιεί μόνο ο αποδέκτης των κρυπτογραφημένων δεδομένων.

Εικόνα 2.1: Διάγραμμα συμμετρικής κρυπτογραφίας

Η συμμετρική κρυπτογραφία είναι εμπιστευτική, επειδή κωδικοποιεί το κάθε μήνυμα με ένα μυστικό κλειδί και με χρήση ενός αλγορίθμου (Εικόνα 2.1). Τα απροστάτευτα δεδομένα, για παράδειγμα το κείμενο, στην αρχική τους μορφή θεωρούνται άθικτα. Η χρήση του αλγορίθμου ωστόσο παράγει μια ανακατωμένη απόδοση του μηνύματος, η οποία μπορεί να μεταδοθεί ασφαλώς πλέον μέσω του δικτύου/διαδικτύου. Ο αποδέκτης μπορεί να αποκρυπτογραφήσει το μήνυμα χρησιμοποιώντας το αρχικό κλειδί για να αναπαράγει το κείμενο. Το κλειδί που χρησιμοποιείται τόσο από τον αποστολέα όσο και από τον αποδέκτη θα πρέπει να παραμένει μυστικό. Το βασικό πρόβλημα σε αυτές τις κρυπτογραφικές εφαρμογές είναι πώς θα γίνει η διαχείριση των κλειδιών και πώς αυτά θα κρατηθούν μυστικά.

Τα κρυπτογραφικά συστήματα δημόσιου κλειδιού λύνουν αυτό το πρόβλημα, αντικαθιστώντας το μυστικό κλειδί με ένα ζευγάρι κλειδιών, ένα ιδιωτικής χρήσης και ένα δημόσιο (Εικόνα 2.2). Η πληροφορία που κρυπτογραφείται με ένα δημόσιο

κλειδί μπορεί να ανακτηθεί μόνο με το συμπληρωματικό κλειδί ιδιωτικής χρήσης. Με αυτό το σύστημα μπορούν να δημοσιεύονται όλα τα δημόσια κλειδιά σε έναν ανοικτό κατάλογο, διευκολύνοντας έτσι την επικοινωνία μεταξύ διαφόρων ομάδων. Επιπλέον της κρυπτογράφησης, τα δημόσια και τα ιδιωτικής χρήσης κλειδιά θα μπορούσαν να χρησιμοποιηθούν για τη δημιουργία και την επαλήθευση ηλεκτρονικών υπογραφών, αν και στην πράξη είναι ενδεδειγμένο να υπάρχουν ξεχωριστά κλειδιά για την κρυπτογράφηση (*encryption*) και την υπογραφή (*signing*) [Hew2004].

Εικόνα 2.2: Κρυπτογραφικό σύστημα δημόσιου κλειδιού (*public key*)

Το βασικό θέμα στα κρυπτογραφικά συστήματα είναι ότι η εμφάνιση των αρχικών δεδομένων αλλάζει. Ένας μη εξουσιοδοτημένος χρήστης δεν μπορεί να *διαβάσει* τα δεδομένα που διακινούνται στο δίκτυο, εκτός και αν έχει το κλειδί. Εκείνο που εντυπωσιάζει είναι ότι η ποιότητα των δεδομένων δεν επηρεάζεται καθόλου. Ο σκοπός των κρυπτογραφικών δεδομένων είναι μόνο η απόκρυψη του περιεχομένου των ψηφιακών προϊόντων και η αποκάλυψή τους μόνο στον κάτοχο του κλειδιού. Συνεπώς ο κάτοχος του κλειδιού θα πρέπει να είναι και ο μόνος εξουσιοδοτημένος χρήστης ή ο δημιουργός τους, διατηρώντας έτσι και τα πνευματικά δικαιώματα. Είναι αξιοπρόσεκτο ότι οι κρυπτογραφικές τεχνικές εισάγουν δύο κύριες καταστάσεις: είτε κάποιος έχει τα κλειδιά, αποκρυπτογραφεί τα μηνύματα και τα διαβάζει, είτε κάποιος δεν μπορεί να τα διαβάσει καθόλου, ακόμα και αν τα κλέψει από το δίκτυο. Οι δύο διαφορετικές καταστάσεις των κρυπτογραφικών συστημάτων ερμηνεύουν τις δύο ξεκάθαρα διαχωρισμένες καταστάσεις της αλήθειας (*truth*) και του ψεύδους (*fault*), δίχως να αφήνουν περιθώρια για αμφιβολίες. Ένας ζωγράφος θα μπορούσε να απεικονίσει τις δύο

αυτές καταστάσεις με δύο μόνο χρώματα: το λευκό, που δεικνύει την πληρότητα όλων, και το μαύρο, που δεικνύει την απουσία τους.

Το μειονέκτημα των κρυπτογραφικών συστημάτων ίσως είναι ότι παρεμποδίζουν την ευρεία διάδοση των ψηφιακών αντικειμένων, εφόσον ερμηνεύονται μόνο από εξουσιοδοτημένους χρήστες. Γι' αυτόν το λόγο τα κρυπτογραφικά συστήματα χρησιμοποιούνται μόνο για συγκεκριμένες εφαρμογές, κυρίως δε για τη μεταφορά εμπιστευτικών μηνυμάτων, όπου ο δημιουργός πράγματι επιθυμεί την απόκρυψη του περιεχομένου των μηνυμάτων.

2.3. Ψηφιακές υπογραφές

Μια ψηφιακή υπογραφή (*digital signature*) είναι ένας ψηφιακός κώδικας που επισυνάπτεται σε μια ηλεκτρονική μεταφορά του μηνύματος, που όμως εξακριβώνει μοναδικά την ταυτότητα του αποστολέα. Όπως στις γραπτές υπογραφές, ο σκοπός των ψηφιακών υπογραφών είναι η εγγύηση ότι ο αποστολέας που στέλνει το μήνυμα είναι πράγματι αυτός που ισχυρίζεται πως είναι. Οι ψηφιακές υπογραφές είναι ιδιαίτερα σημαντικές στο ηλεκτρονικό εμπόριο και στα περισσότερα συστήματα απόδειξης γνησιότητας [Web2004].

Η εισαγωγή των ψηφιακών υπογραφών στα δεδομένα διαφέρει κατά πολύ από τις προηγούμενες κρυπτογραφικές μεθόδους. Οι ψηφιακές υπογραφές εισάγονται στα δεδομένα ή στην επικεφαλίδα (*header*) είτε ακόμα και σε συνοδευτικό αρχείο, ενώ στην κρυπτογραφία όλο το αρχείο κωδικοποιείται. Αυτό συμβαίνει διότι ο σκοπός των ψηφιακών υπογραφών είναι η διασφάλιση κυρίως της ακεραιότητας των αρχικών δεδομένων με το να υπογράφονται τα δεδομένα από τον κάτοχο, έτσι ώστε να είναι δυνατή η επικύρωση του κατόχου. Έτσι, τα πρωτογενή δεδομένα που ταξιδεύουν συνοδευόμενα με μια ψηφιακή υπογραφή είναι μεν προσιτά στους χρήστες, αλλά οι τυχόν τροποποιήσεις τους δεν είναι επιτρεπτές. Αν τα προϊόντα αυτά τροποποιηθούν τότε δε θα δίνεται εγγύηση για την επιβεβαίωση του κατόχου και άρα και της ακεραιότητας των δεδομένων. Συνεπώς, η έννοια της ανθεκτικότητας δεν είναι καθοριστική στις τεχνικές των ψηφιακών υπογραφών.

Υπάρχουν δύο κύριες τεχνικές ψηφιακών υπογραφών. Στην πρώτη και απλούστερη γίνεται ένθεση της ψηφιακής υπογραφής κατευθείαν στην επικεφαλίδα του αρχείου, περιγράφοντας τον κάτοχο των δεδομένων. Στη δεύτερη τεχνική γίνεται συσχέτιση ενός κλειδιού με τα αρχικά δεδομένα με χρήση μιας συνάρτησης

(π.χ. μιας *hash function*) για την παραγωγή μιας ψηφιακής υπογραφής. Η παραγόμενη ψηφιακή υπογραφή εισάγεται στη συνέχεια στο ψηφιακό προϊόν. Κάτι τέτοιο έχει ως αποτέλεσμα τον υποβιβασμό της ποιότητας των δεδομένων του μαρκαρισμένου αρχείου.

Οι τεχνικές των ψηφιακών υπογραφών είναι πιο ευέλικτες σε σχέση με τις κρυπτογραφικές τεχνικές σχετικά με την ελευθερία που δίνεται στους χρήστες. Στις κρυπτογραφικές τεχνικές οι χρήστες δεν μπορούν να κατανοήσουν ένα κρυπτογραφημένο αρχείο, εκτός και αν είναι εξουσιοδοτημένοι (δηλαδή κατέχουν κάποιο κλειδί). Αντίθετα, στις τεχνικές των ψηφιακών υπογραφών κάθε χρήστης μπορεί να διαβάσει το αρχείο και επιπλέον μπορεί και να καταστρέψει τις ψηφιακές υπογραφές. Η φιλοσοφία πίσω από τις ψηφιακές υπογραφές είναι ότι ο χρήστης είναι εντελώς ελεύθερος να διαβάσει το αρχείο και να το επεξεργαστεί όπως επιθυμεί, και εξαρτάται από τη δική του καλή θέληση να μην καταστρέψει τις αποδείξεις γνησιότητας του αρχείου. Υπό αυτή την άποψη, η *ολοκληρωτική* κρυπτογραφία και η *απόλυτη ελευθερία* των τεχνικών των ψηφιακών υπογραφών περιλαμβάνουν τις δύο ακραίες καταστάσεις, οι οποίες είναι φανερές όχι μόνο σε συστήματα ασφαλείας, αλλά επίσης και σε μοντέλα ανθρώπινων συμπεριφορών.

2.4. Ψηφιακές τεχνικές υδατογράφησης

Οι τεχνικές ψηφιακής υδατογράφησης (*digital watermarking techniques*) ενθέτουν μοναδικά σημάδια (υδατογραφήματα) σε πολυμέσα, ήχους, βίντεο, εικόνες, ή ακόμα και σε κείμενο, με σκοπό να επιβεβαιώσει τη γνησιότητα του περιεχομένου και να παρέχει προστασία των πνευματικών δικαιωμάτων, δίχως τον υποβιβασμό της ποιότητάς τους. Αυτή είναι η βασική διαφορά ανάμεσα στις τεχνικές υδατογράφησης και στις τεχνικές των ψηφιακών υπογραφών. Οι τελευταίες ενδιαφέρονται για τη διατήρηση της ακεραιότητας των δεδομένων και όχι τόσο για τη διατήρηση της ποιότητας των δεδομένων. Επιπλέον, όπως ήδη αναφέρθηκε, η ανθεκτικότητα δεν αποτελεί κύριο θέμα των τεχνικών των ψηφιακών υπογραφών, ενώ στις τεχνικές υδατογράφησης η επιβίωση του υδατογραφήματος είναι ζωτικής σημασίας και σκοπεύει στη επιβεβαίωση των πνευματικών δικαιωμάτων. Από την άλλη μεριά οι τεχνικές υδατογράφησης διαφέρουν ριζικά από τις κρυπτογραφικές τεχνικές, μια και στις πρώτες γίνεται ένθεση ενός σημαδιού μέσα στα δεδομένα που μεταδίδονται,

ενώ στις τελευταίες αλλάζουν εντελώς τα δεδομένα από την αρχική τους μορφή πριν την μετάδοσή τους.

Οι τεχνικές υδατογράφησης για να είναι αποδοτικές έχουν κάποια χαρακτηριστικά. Πολλά από αυτά τα χαρακτηριστικά είναι αντικρουόμενα και μια καλή εξισορρόπηση μεταξύ τους είναι καθοριστική για την επιλογή των χαρακτηριστικών. Η κατάλληλη επιλογή των χαρακτηριστικών σχετίζεται άμεσα με τα χαρακτηριστικά της εφαρμογής στην οποία θα χρησιμοποιηθεί. Η ικανοποίηση όλων των απαιτήσεων δεν είναι εύκολο καθήκον, αλλά υπάρχουν αρκετές εταιρίες που προφέρουν ανταγωνιστικές τεχνολογίες. Όλες αυτές κάνουν το υδατογράφημα να εμφανίζεται σαν θόρυβος, δηλαδή σαν τυχαία δεδομένα που υπάρχουν στα ψηφιακά αρχεία ούτως ή άλλως. Μερικά από τα γενικά χαρακτηριστικά των συστημάτων υδατογράφησης παραθέτονται στη συνέχεια [Κου1999, Kat2000]:

1. Μη αντιληπτικότητα (*Imperceptibility, Invisibility/Inaudibility*): Μια από τις πιο σημαντικές απαιτήσεις είναι ότι το υδατογράφημα θα πρέπει να είναι ορατά μη ανιχνεύσιμο, ανεξάρτητα από την εφαρμογή και τον σκοπό του συστήματος υδατογράφησης. Τεχνουργήματα που εισάγονται μέσω μιας διαδικασίας υδατογράφησης είναι όχι μόνο ενοχλητικά και ανεπιθύμητα, αλλά μπορεί επίσης να ελαττώσουν ή να καταστρέψουν την εμπορική αξία των υδατογραφημένων δεδομένων. Γι' αυτό είναι σημαντικό να σχεδιαστούν μέθοδοι υδατογράφησης που να εκμεταλλεύονται τις επιδράσεις του ανθρώπινου οπτικού ή ακουστικού συστήματος. Οι μεταβολές που προκαλούνται από την ένθεση του υδατογραφήματος θα πρέπει να είναι κάτω από ένα κατώφλι αντιληπτικότητας, το οποίο σημαίνει ότι κάποιο είδος κριτηρίου αντιληπτικότητας θα πρέπει να χρησιμοποιείται όχι μόνο στο σχεδιασμό του υδατογραφήματος, αλλά επίσης και στον ποσοτικό προσδιορισμό της παραποίησης. Δύο προβλήματα προκύπτουν εδώ. Το πρώτο πρόβλημα είναι η αξιόπιστη εκτίμηση της εισαγόμενης παραμόρφωσης. Το δεύτερο πρόβλημα εμφανίζεται κατά την επεξεργασία των υδατογραφημένων δεδομένων. Για παράδειγμα στην υδατογράφηση εικόνων η ορατότητα του υδατογραφήματος μπορεί να αυξηθεί αν η εικόνα αλλάξει διαστάσεις. Από την παραπάνω απαίτηση εξαιρούνται τα ορατά υδατογραφήματα.
2. Ανθεκτικότητα (*Robustness*): Οι βασικές μέθοδοι υδατογράφησης θα πρέπει να είναι ανθεκτικές σε οποιοδήποτε είδος παραμόρφωσης που εισάγεται από κοινή ή κακόβουλη (*malicious*) επεξεργασία των δεδομένων. Μέχρι στιγμής

δεν έχει προταθεί καμιά τέτοια τέλεια μέθοδος και δεν είναι σίγουρο αν υπάρχει καν μια απόλυτα ασφαλής μέθοδος υδατογράφησης. Έτσι, τα εφαρμοσμένα συστήματα θα πρέπει να κάνουν ένα συμβιβασμό ανάμεσα στην ανθεκτικότητα και στις ανταγωνιστικές απαιτήσεις, όπως είναι η μη αντιληπτικότητα. Ανάλογα με τους σκοπούς της εφαρμογής των μεθόδων υδατογράφησης και άρα την επιθυμητή ανθεκτικότητα, επηρεάζεται η διαδικασία σχεδιασμού. Για παράδειγμα στην υδατογράφηση εικόνας, αν απαιτείται μια μέθοδος που να είναι ανθεκτική σε JPEG συμπίεση με υψηλούς συντελεστές συμπίεσης, πιθανότατα είναι πιο αποτελεσματικό να χρησιμοποιήσουμε μια μέθοδο που να λειτουργεί σε ένα πεδίο μετασχηματισμού από το να χρησιμοποιήσουμε μια μέθοδο που να λειτουργεί στο χωρικό πεδίο. Παρόμοια, αν κάποια μέθοδος θα πρέπει να προσαρμοστεί σε γενικευμένους γεωμετρικούς μετασχηματισμούς, όπως η περιστροφή, η μη ομοιόμορφη αλλαγή διαστάσεων και η διάτμηση, μια προσέγγιση στο χωρικό πεδίο είναι πιθανότατα πιο κατάλληλη.

3. Πλεονασμός (*Redundancy*): Για να εξασφαλιστεί η ανθεκτικότητα παρόλες τις μικρές επιτρεπόμενες αλλαγές, η πληροφορία του υδατογραφήματος είναι συνήθως πολλές φορές διασκορπισμένη σε πολλά δείγματα των αρχικών δεδομένων (*cover data*), παρέχοντας έτσι μια συνολική ανθεκτικότητα, γεγονός που σημαίνει ότι το υδατογράφημα μπορεί συνήθως να ανακτηθεί από ένα μικρό μέρος των υδατογραφημένων δεδομένων. Είναι ευνόητο ότι η ανάκτηση του υδατογραφήματος είναι περισσότερο ανθεκτική αν περισσότερα υδατογραφημένα δεδομένα είναι διαθέσιμα στη διαδικασία ανάκτησης. Παρόλα ταύτα, ο πλεονασμός που εισάγεται στα αρχικά δεδομένα δε θα πρέπει να ξεπερνά ένα όριο, αλλιώς τα πλεονάζοντα υδατογραφήματα είναι τελείως άχρηστα.
4. Ασφάλεια υδατογραφήματος και Κλειδιά (*Watermark security and Keys*): Στις περισσότερες εφαρμογές, όπως είναι η προστασία των πνευματικών δικαιωμάτων, η απόκρυψη της εισαγόμενης πληροφορίας χρειάζεται να επιβεβαιωθεί. Αυτό και σχετικά θέματα συχνά αναφέρονται σαν *ασφάλεια υδατογραφήματος*. Εφαρμογές στις οποίες η ασφάλεια δεν αποτελεί θέμα είναι και η σύνταξη ευρετηρίου βάσεων δεδομένων εικόνων. Αν όμως η απόκρυψη της πληροφορίας απαιτείται, ένα μυστικό κλειδί θα πρέπει να χρησιμοποιηθεί για τη διαδικασία εισαγωγής και εξαγωγής. Στη γενική τους λοιπόν μορφή, τα συστήματα υδατογράφησης χρησιμοποιούν ένα ή

περισσότερα κρυπτογραφικά ασφαλή κλειδιά. Αν το υδατογράφημα μπορεί να διαβαστεί από κάποιον, το ίδιο πρόσωπο μπορεί εύκολα και να το καταστρέψει, διότι όχι μόνο η στρατηγική ένθεσης, αλλά και οι θέσεις του υδατογραφήματος θα είναι γνωστές σε αυτή την περίπτωση.

5. Ανάκτηση υδατογραφήματος με ή χωρίς τα αρχικά δεδομένα (*Watermark extraction with or without the original data*): Στις μεθόδους υδατογράφησης η χρήση των αρχικών δεδομένων στη διαδικασία ανάκτησης συνήθως αυξάνει την ανθεκτικότητα όχι μόνο ως προς τις παραμορφώσεις θορύβου, αλλά και ως προς τις γεωμετρικές παραμορφώσεις. Σε πολλές εφαρμογές η πρόσβαση στα αρχικά δεδομένα δεν είναι δυνατή. Σε άλλες εφαρμογές επίσης, όπως σε εφαρμογές υδατογράφησης βίντεο, η χρήση των αρχικών δεδομένων μπορεί να είναι μη πρακτική, εξαιτίας του μεγάλου όγκου των δεδομένων που θα πρέπει να επεξεργαστούν. Εφόσον οι πρόσφατες τεχνικές υδατογράφησης απαιτούν και τα αρχικά δεδομένα για την ανάκτηση και δεδομένου του κινδύνου της χρήσης των αρχικών δεδομένων από κακόβουλους χρήστες, υπάρχει μια καθαρή τάση για την επινοήση τεχνικών που δεν απαιτούν τα αρχικά δεδομένα.
6. Εξαγωγή υδατογραφήματος ή επιβεβαίωση της παρουσίας ενός δεδομένου υδατογραφήματος (*Watermark extraction or verification of the existence of a watermark*): Όπως είναι γνωστό υπάρχουν δύο τύποι συστημάτων υδατογράφησης. Στον έναν τύπο υπάγονται τα συστήματα που εισάγουν μια συγκεκριμένη πληροφορία και αργότερα στη διαδικασία ανάκτησης γίνεται έλεγχος της ύπαρξης αυτής της πληροφορίας, και στον δεύτερο τύπο τα συστήματα που εισάγουν αυθαίρετα πληροφορία στα δεδομένα. Για παράδειγμα, η προστασία των πνευματικών δικαιωμάτων μπορεί να επιτευχθεί με συστήματα επιβεβαίωσης της παρουσίας του γνωστού υδατογραφήματος. Τα συστήματα υδατογράφησης που εισάγουν αυθαίρετα πληροφορία χρησιμοποιούνται για παράδειγμα για τον εντοπισμό της εικόνας (*image tracking*) στο Διαδίκτυο. Ένας τύπος συστημάτων που επιτρέπει την επιβεβαίωση υδατογραφήματος μπορεί να θεωρηθεί σαν σύστημα ανάκτησης υδατογραφήματος ενός δυαδικού ψηφίου (*one-bit watermark recovery scheme*).
7. Στατιστική αφάνεια (*Statistical invisibility*): Ο αλγόριθμος θα πρέπει να εμποδίζει τον εντοπισμό μη εξουσιοδοτημένων υδατογραφημάτων ή την αφαίρεσή τους, αν αυτά είναι γνωστά.

8. Παρόμοια συμπεριφορά στη συμπίεση (*Similar compression characteristics with the original signal*): Τα ψηφιακά προϊόντα θα πρέπει να ενσωματώσουν το υδατογράφημα με τέτοιο τρόπο έτσι ώστε το υδατογράφημα και το προϊόν να συμπεριφέρονται σαν μια οντότητα, έχοντας παρόμοια χαρακτηριστικά συμπίεσης.
9. Άμεση εισαγωγή του υδατογραφήματος στα δεδομένα (*The watermark should be embedded directly in the data*): Τα πραγματικά bits που αναπαριστούν το υδατογράφημα θα πρέπει να ανακατευτούν με τέτοιο τρόπο μέσα στο αρχείο έτσι ώστε να μην αναγνωρίζονται.
10. Υποστήριξη πολλαπλών υδατογραφημάτων (*Support multiple watermarks*): Μερικές εφαρμογές απαιτούν για μεγαλύτερη ασφάλεια την εισαγωγή πολλαπλών υδατογραφημάτων στο αρχικό προϊόν.
11. Αυτο-ρύθμιση (*Self-clocking*): Αυτό το χαρακτηριστικό εμφανίζεται ξεκάθαρα σε τεχνικές υδατογράφησης ήχων και βίντεο. Ο αλγόριθμος σε τέτοιες εφαρμογές θα πρέπει να εντοπίζει την αρχή και το τέλος της πλεονάζουσας πληροφορίας, που στην ουσία σχετίζεται με το υδατογράφημα.

Οι τεχνικές ψηφιακής υδατογράφησης είναι παρόμοιες με τις τεχνικές των ψηφιακών υπογραφών, ενώ είναι πιο ευέλικτες από τις κρυπτογραφικές τεχνικές, έχοντας ως κριτήριο την ελευθερία που δίνεται στους χρήστες. Στις τεχνικές υδατογράφησης κάθε χρήστης μπορεί να διαβάσει το αρχείο, χωρίς ωστόσο να μπορεί να αφαιρέσει το υδατογράφημα, εφόσον τα υδατογραφήματα που σχεδιάστηκαν για απόδειξη κυριότητας είναι ανθεκτικά. Αντίθετα με τις τεχνικές υδατογράφησης, στις τεχνικές των ψηφιακών υπογραφών οι υπογραφές δεν έχουν σχεδιαστεί να είναι ανθεκτικές. Η φιλοσοφία πίσω από τις τεχνικές υδατογράφησης είναι ότι οι χρήστες είναι εντελώς ελεύθεροι να διαβάσουν και να επεξεργαστούν το αρχείο, χωρίς όμως να μπορούν να καταστρέψουν τις αποδείξεις κυριότητας και γνησιότητας των αντικειμένων. Συνεπώς, υπάρχει μια ισορροπία που παρέχει πολλές ελευθερίες στο χρήστη και ταυτόχρονα προστατεύει και τα νομικά δικαιώματα των κατόχων.

2.5. Ηθικοί αντίκτυποι

Ο ρόλος της ηθικής και του κώδικα δεοντολογίας γενικότερα (*ethics*), καθώς υιοθετείται από τους μηχανισμούς ασφαλείας, είναι πολύ σημαντικός, εφόσον καθορίζει σε μεγάλο βαθμό και την ανθρώπινη συμπεριφορά. Ο κώδικας δεοντολογίας υπολογιστών (*computer ethics*), που βασίζεται σε δέκα κύριες εντολές [Ten2004], διαρθρώνει έναν κώδικα δεοντολογίας που καλούνται να τον ακολουθήσουν οι άνθρωποι με ελεύθερη βούληση. Οι περισσότερες από αυτές τις εντολές εφαρμόζονται μέσα από τους μηχανισμούς ασφαλείας. Οι επικρατούντες μηχανισμοί ασφαλείας είναι αυτοί που βασίζονται στην κρυπτογραφία, στις ψηφιακές υπογραφές και στις τεχνικές υδατογράφησης.

Μια από τις σημαντικές απόψεις δεοντολογίας είναι η μη χρήση των υπολογιστών προς βλάβη άλλων ανθρώπων. Οι μηχανισμοί ασφαλείας έρχονται να ισχυροποιήσουν αυτόν τον κανόνα διατηρώντας τα πνευματικά δικαιώματα και συνεπώς το οικονομικό ενδιαφέρον των κατόχων. Οι τεχνικές κρυπτογραφίας και οι τεχνικές των ψηφιακών υπογραφών εμποδίζουν ή εντοπίζουν αντίστοιχα, μη εξουσιοδοτημένους χρήστες, από την παραβίαση της ακεραιότητας των δεδομένων. Ιδιαίτερα δε η κρυπτογραφία δεν επιτρέπει καν σε μη εξουσιοδοτημένους χρήστες την πρόσβαση στο περιεχόμενο των αρχείων. Οι τεχνικές υδατογράφησης από την άλλη μεριά έχουν σχεδιαστεί για τη διατήρηση των δικαιωμάτων των κατόχων. Οι υπογραφές στις τεχνικές των ψηφιακών υπογραφών είναι ευαίσθητες στις επιθέσεις καθώς ο κύριος στόχος τους είναι η ακεραιότητα των δεδομένων (*data integrity*). Όσο για τις διαφορές μεταξύ υδατογράφησης και κρυπτογραφίας, στις κρυπτογραφικές τεχνικές θα μπορούσε να πει κανείς ότι τα αποκρυπτογραφημένα αρχεία είναι ευάλωτα σε όλες τις υπολειπόμενες επιδράσεις εκτός της κωδικοποίησης, ενώ τα ψηφιακά υδατογραφήματα είναι σχεδιασμένα να διατηρούνται κατά την εμφάνιση, την εκτύπωση καθώς και σε επαναδιανομή.

Η υιοθέτηση μιας εκ των τριών τεχνικών που εξετάστηκαν αφορά καθαρά την εφαρμογή και την πρόθεση αυτών που θα κάνουν την επιλογή. Η τεχνική ωστόσο που είναι πιο κοντά στην ιδέα της ελευθερίας, και η οποία βρίσκεται διάχυτη στην ψηφιακή κοινωνία (όπως είναι το διαδίκτυο) – βλέπε [ArL2002], είναι η υδατογράφηση: ο καθένας μπορεί να διαβάζει και να επεξεργάζεται τα προστατευμένα αρχεία. Με τη μόνη διαφορά ότι υπάρχουν προσεκτικά κρυμμένα κομμάτια δεδομένων που συνοδεύουν πάντα τα αρχεία και είναι πάντα εκεί έτοιμα

να αποδείξουν (και να προστατεύσουν) τον πραγματικό κάτοχο, αν προκύψει ζήτημα πνευματικής ιδιοκτησίας.

2.6. Συμπεράσματα

Η ψηφιακή κοινωνία των υπολογιστών είναι μια μινιατούρα του πραγματικού φυσικού κόσμου. Τα συστήματα ασφαλείας στον κόσμο των υπολογιστών αντανakλούν τους μηχανισμούς ασφαλείας του πραγματικού κόσμου [ArC2002]. Με αυτό το σκεπτικό τα κρυπτογραφικά συστήματα αντανakλούν την απόλυτη και αυστηρή επιβολή των νόμων. Οι τεχνικές των ψηφιακών υπογραφών καθρεπτίζουν την ελευθερία εκείνη στην οποία ο καθένας μπορεί ελεύθερα να δράσει σύμφωνα με τη θέλησή του, χωρίς όμως να υπάρχει έλεγχος αν η ελευθερία του ενός περιορίζει την ελευθερία των άλλων. Οι τεχνικές υδατογράφησης παρέχουν πολλές ελευθερίες στους χρήστες, ενώ ταυτόχρονα τους διδάσκουν να σέβονται τους νόμους και να μην τους αγνοούν. Η επιλογή του κατάλληλου μηχανισμού ασφαλείας που θα πρέπει να εφαρμοστεί εξαρτάται από την εφαρμογή, και θα πρέπει να γίνει κατανοητό ότι δεν υπάρχει πανάκεια και μοναδική υπερ-λύση για όλα τα προβλήματα ασφαλείας.

Σε αυτό το κεφάλαιο παρουσιάστηκαν κάποιοι κανόνες δεοντολογίας που προκύπτουν σε σχέση με τους μηχανισμούς της ηλεκτρονικής ασφάλειας και συζητήθηκε πώς αυτοί αναπαράγονται στον ηλεκτρονικό κόσμο. Μελετήθηκε κάθε μηχανισμός ασφαλείας ξεχωριστά και έγινε μια σύγκριση μεταξύ τους ερευνώντας κυρίως πώς οι κανόνες δεοντολογίας διαφοροποιούνται σύμφωνα με τη φύση του κάθε μηχανισμού ασφαλείας.

Κεφάλαιο 3

Υδατογράφηση: από τη δεοντολογία στην πράξη

3.1. Εισαγωγή

Η ευρεία χρήση του Διαδικτύου οδήγησε στη μεταφορά ενός απίστευτα μεγάλου αριθμού ψηφιακών αντικειμένων μέσω του δικτύου. Αντίγραφα ψηφιακών αντικειμένων (όπως για παράδειγμα μουσικής, εικόνων και βίντεο) διανέμονται μέσω του Διαδικτύου. Τα ψηφιακά αντικείμενα έχουν μια διαφορετική αίσθηση από τα άλλα είδους αντικείμενα, όπως τα αντίγραφα χαρτιού. Ένα ψηφιακό αντίγραφο είναι πανομοιότυπο με το αρχικό αντικείμενο και δεν υπάρχει κανένας εμφανής τρόπος που να διαχωρίζει το αντίγραφο από το πρωτότυπο, με απλή παρατήρηση. Σύμφωνα με τον Καντ «ένα αντίγραφο είναι εργασία της δουλειάς του συγγραφέα» (*«a copy is a work of the author's (opus)»*) [Kan1785]. Ο κάτοχος του αντιγράφου δε θα πρέπει να το δημοσιεύει χωρίς τη συγκατάθεση του συγγραφέα και γενικότερα του δημιουργού.

Οι νέες τεχνολογίες παρέχουν στους χρήστες *εύκολη πρόσβαση* στα ψηφιακά αντικείμενα. Η απαγόρευση της πρόσβασης σε αυτά δε θα αποτελούσε πανάκεια. Η φιλοσοφία του Διαδικτύου βασίζεται σε *τεχνικά έργα ανοιχτής προέλευσης* (*open*

source projects), όπου καθένας μπορεί να χρησιμοποιήσει το έργο ή τον κώδικα, αρκεί βεβαίως να κάνει σαφή αναφορά στους δημιουργούς (βλέπε GNU [GNU2004]). Από αυτήν τη σκοπιά η πρόσβαση στα ψηφιακά αντικείμενα δεν μπορεί και δεν πρέπει να απαγορευτεί. Ωστόσο θα πρέπει να υπάρχει ένας τρόπος που να παρέχει την πιστοποίηση κυριότητας των αντικειμένων. Οι τεχνικές υδατογράφησης αναπτύχθηκαν με σκοπό την προστασία των πνευματικών δικαιωμάτων.

Ο όρος *ηθική* (*ethics*) αναφέρεται, σύμφωνα με την αρχαία ελληνική φιλοσοφία, στον τρόπο ύπαρξης ενός ανθρώπου. Έτσι η ηθική ως φιλοσοφική επιστήμη ενδιαφέρεται κυρίως να ορίσει ποιο είναι το ηθικό νόημα της ζωής του ανθρώπου και ποια είναι τα κριτήρια εκείνα τα οποία καθιστούν μια πράξη ηθική. Στο σημείο αυτό αναφέρουμε το εξής ερώτημα του Καντ: «*τι οφείλω να πράττω;*» [Kan1781].

Η ηθική, ως επιστήμη, ορίζει τους κανόνες και τις αρχές, με τους οποίους ρυθμίζονται οι πράξεις των ανθρώπων. Παράλληλα όμως προσπαθεί να βρει τις αιτίες τους καθώς και τη σχέση μεταξύ πράξης και αιτίας. Στόχος λοιπόν της ηθικής φιλοσοφίας είναι η *πράξη* και οι ποικίλοι προσδιορισμοί της. Όταν μια πράξη χαρακτηρίζεται ηθική, διαμορφώνει ή τροποποιεί τις διανθρώπινες σχέσεις και για αυτό, ανάλογα, αποκτά ηθική αξία.

Καθετί που δημιουργεί ο άνθρωπος, «το πράττει», επομένως η πράξη από μια απλή λέξη αποκτά κοινωνική διάσταση. Και αυτό γιατί γίνεται από τον άνθρωπο, ο οποίος είναι μέλος ενός ευρύτερου κοινωνικού συνόλου. Επομένως το αποτέλεσμα μιας πράξης επηρεάζει όλα τα μέλη μιας κοινωνίας. Βασικό, θα αναφέρουμε στο σημείο αυτό, είναι η πράξη ενός ατόμου να υπακούει στους άγραφους ηθικούς κανόνες. Παρόλο που είναι πολλοί εκείνοι οι οποίοι ισχυρίζονται ότι οι άνθρωποι δεν ενεργούν με αυτόν τον τρόπο, είναι όμως γεγονός ότι όλοι οι άνθρωποι τείνουν να υπακούουν στις δικές τους εσωτερικές ηθικές αξίες, αν όχι στις γενικές ηθικές αξίες.

Από τα αρχαία χρόνια, εκτός των άγραφων ηθικών κανόνων υπήρχε και η ανάγκη νόμων. Οι νόμοι είναι εκείνοι οι οποίοι θα οδηγήσουν στην τιμωρία μιας πράξης και όχι οι άγραφοι ηθικοί κανόνες. Οι τελευταίοι μπορούν να επηρεάσουν μόνο τη συνείδησή μας. Συνεπώς μια πράξη μη αποδεκτή τιμωρείται από το νόμο, αλλά και είναι κατακριτέα με βάση τους ηθικούς κανόνες. Γενικότερα θα μπορούσαμε να αναφέρουμε πως η ηθικότητα του αποτελέσματος μια πράξης ανάγεται στην αρχική σκέψη και προαίρεση εκείνου που την έπραξε [Kat1982].

Περνώντας στο σημείο αυτό στον ευρύτερο επιστημονικό χώρο, θα λέγαμε πως είναι αρκετοί σήμερα οι επιστήμονες-ερευνητές, οι οποίοι δε θέλουν να συνδέσουν το αντικείμενο έρευνάς τους με τη φιλοσοφία. Όμως η θεώρηση της φιλοσοφίας συνδέεται αδιάσπαστα με τη θεώρηση της επιστήμης. Η φιλοσοφία δίνει στον επιστήμονα τη δυνατότητα να αναπτύξει μέσα από την απορία, τη μεθοδολογία της έρευνάς του.

Συνδεδειγμένος κρίκος μεταξύ φιλοσοφίας και επιστήμης είναι η παρατήρηση και το πείραμα, που χρησιμοποιούνται ως μέσο έκφρασης και καταγραφής του προϊόντος συνεργασίας των δύο αυτών δομών. Η παρατήρηση και το πείραμα λοιπόν, συνδέουν τη φιλοσοφία με την επιστήμη για να οικοδομήσουν το λειτουργικό μέρος της δράσης μέσα στο μοντέλο της έρευνας.

Θεωρώντας την έρευνα ως εναρκτήριο σημείο παράγουμε διάφορες μεθόδους προσδιορισμού της αυθεντικότητας των ψηφιακών αντικειμένων καθώς και των δημιουργών ή των νόμιμων κατόχων. Μοντέλα έρευνας που βασίζονται στη *δοκιμή* και στην *προσπάθεια* οδηγούν στην ανάπτυξη μιας πληθώρας μεθόδων υδατογράφησης. Η υδατογράφηση αναφέρεται σε τεχνικές που διασφαλίζουν τα πνευματικά δικαιώματα των κατόχων.

Η ανάγκη για μια τέτοια αναγνώριση δεν είναι καινούργια. Αρχικά υπήρχαν μέθοδοι υδατογράφησης, όταν το υλικό ήταν το χαρτί, ενώ στις μέρες μας επεκτείνεται σε πληροφορία που διανέμεται στο Διαδίκτυο, μετατρέποντας τις παλαιού τύπου τεχνικές υδατογράφησης σε υδατογράφηση ψηφιακών αντικειμένων.

Εν κατακλείδι, η γνώση που παράγεται από τη φιλοσοφία και την επιστήμη, ανθεί μέσα στον πολιτισμό, με αποτέλεσμα την εξέλιξή της. Έτσι λοιπόν και ο άνθρωπος εξελίσσεται σαν μια ολότητα, η οποία καθορίζεται από προσωπικές, τοπικές, εθνικές, ηθικές, θρησκευτικές και παγκόσμιες αξίες.

3.2. Δικαιώματα πνευματικής ιδιοκτησίας

Το Διαδίκτυο και γενικά οι νέες τεχνολογίες συνάντησαν μια απρόσμενη ανάπτυξη. Αυτή η ανάπτυξη άλλαξε απροσδόκητα και την καθημερινή μας συμπεριφορά. Με το Διαδίκτυο έρχονται στα σπίτια μας οι γενικές κατευθύνσεις τις μόδας και οι νέες τάσεις σε πολλά διαφορετικά πεδία που κυκλοφορούν στον κόσμο μέσω του δικτύου. Εμφανίζονται χωρίς τέλος διάφορα εικονικά περιβάλλοντα και θεάματα, που υπόσχονται απροσδόκητες εμπειρίες.

Σε μια προσπάθεια διάχυσης της πληροφορίας, κατασκευάζεται νέο προγραμματιστικό υλικό, μεταφέρονται καθημερινά εικόνες παντού στον κόσμο, εικονίδια ξεπερνούν τη στερεότυπη σημασία τους παρέχοντας κατανοητές μεταφορές (*metaphors*) στο εικονικό περιβάλλον. Επιπλέον δημιουργούνται λέξεις που δεν υπήρχαν πριν, τέτοιες όπως κυβερνο-χώρος, κυβερνο-έγκλημα (*cyber-crime*), κυβερνο-ναύτες (*cyber-nauts*) και πολλές άλλες. Σε αυτό το τεράστιο συνονθύλευμα ορθώνονται οι απαιτήσεις για Πνευματική Ιδιοκτησία (*Intellectual Property*) καθώς και για Πνευματικά Δικαιώματα (*Intellectual Property Rights - IPRs*). Σύμφωνα με τους Lehman και Brown [Leh1995]:

"Intellectual property is a subtle and esoteric area of the law that evolves in response to technological change."

Δηλαδή

«Πνευματική ιδιοκτησία είναι μια διακριτική και εσωτερική περιοχή του νόμου που αναπτύσσεται σε απόκριση των τεχνολογικών αλλαγών. »

Τα θέματα της πνευματικής ιδιοκτησίας πηγάζουν από το φυσικό κόσμο, όπου τα φυσικά αντικείμενα συμπεριλαμβάνουν την ιδέα της ιδιοκτησίας. Έτσι, θέματα δικαιωμάτων πνευματικής ιδιοκτησίας (*copyright*) είναι περισσότερο από ποτέ απαραίτητα για τέτοιου είδους προστασία. Ανάλογα, πνευματική εργασία όπως είναι η λογοτεχνία, ο προγραμματισμός των υπολογιστών, η καλλιτεχνική εργασία και τόσα άλλα θα πρέπει να έχουν το δικαίωμα της προστασίας, διασφαλίζοντας έτσι τα πνευματικά δικαιώματα των δημιουργών τους.

Ο Παγκόσμιος Οργανισμός Πνευματικών Δικαιωμάτων (*World Intellectual Property Organization - WIPO*) είναι υπεύθυνος για τη διοίκηση διεθνών θεμάτων πνευματικής ιδιοκτησίας. Σύμφωνα λοιπόν με τον WIPO [WIPO2004]:

"Copyright is the legal protection extended to the owner of the rights in an original work that he has created. It comprises two main sets of rights: the economic rights and the moral rights."

Δηλαδή

«Τα Δικαιώματα Πνευματικής Ιδιοκτησίας (Copyright) είναι η νόμιμη προστασία που εκτείνεται στον κάτοχο των δικαιωμάτων για την πρωτότυπη δουλειά που δημιουργήσε. Συμβιβάζει δύο κύριες ομάδες δικαιωμάτων: τα οικονομικά δικαιώματα και τα ηθικά δικαιώματα.»

Η πνευματική ιδιοκτησία, η οποία μπορεί να χαρακτηριστεί καρπός της ανθρώπινης δημιουργίας και επινόησης, διακρίνεται σε δύο κατηγορίες [WIPO2004]. Η πρώτη είναι η βιομηχανική ιδιοκτησία, η οποία περιλαμβάνει τις εφευρέσεις, τα ορόσημα, τον εργοστασιακό σχεδιασμό και οι γεωγραφικοί δείκτες των πηγών. Η δεύτερη κατηγορία είναι τα δικαιώματα πνευματικής ιδιοκτησίας και τα συσχετιζόμενα δικαιώματα, τα οποία περιλαμβάνουν ένα ευρύ φάσμα λογοτεχνικών και καλλιτεχνικών εργασιών.

Παρόλο που έχουν θεσπιστεί νόμοι για την προστασία των πνευματικών δικαιωμάτων είναι πολύ δύσκολο για τους σχετικούς νόμους να *συμβαδίζουν* με την τεχνολογία. Η νέα τεχνολογία έχει εκμηδενίσει τις αποστάσεις. Ο καθένας μπορεί να αντιγράψει ψηφιακά αντικείμενα από τη μια χώρα στην άλλη σε ελάχιστο χρόνο. Αν ο καταπατητής του νόμου και η παρατυπία πραγματοποιούνται στην ίδια χώρα τότε οι νόμοι είναι ξεκάθαροι. Αλλά αν ο καταπατητής του νόμου είναι σε μια χώρα, όπου μια συγκεκριμένη πράξη δεν είναι ή θεωρείται αδίκημα πνευματικής ιδιοκτησίας και η πνευματική εργασία είναι αποθηκευμένη σε ένα εξυπηρετητή (*server*) σε μια άλλη χώρα, όπου όμως η ίδια πράξη είναι παράνομη, τότε η σύγκρουση των νόμων σίγουρα δεν είναι μια εύκολα επιλύσιμη κατάσταση.

Είναι πολύπλοκο να αποφασιστεί ποιας χώρας οι νόμοι θα πρέπει να εφαρμοστούν στις νέες τεχνολογίες. Ένα παράδειγμα σύγκρουσης νόμων είναι η περίπτωση του Joe Gutnick ("Diamond") που δίωξε νομικά το περιοδικό "Barron's" του Dow Jones σε *Αυστραλέζικο* δικαστήριο, επειδή πίστευε ότι είχε δυσφημιστεί σε ένα άρθρο του. Συγκεκριμένα όμως το περιοδικό είχε δημοσιευτεί στις Ηνωμένες Πολιτείες, *αλλά* ήταν διαθέσιμο μέσω του δικτύου και ο Gutnick ισχυριζόταν ότι είχε δυσφημιστεί στην Αυστραλία και επιδίωκε μέσα από μια δίκη την επανόρθωση πιθανών ζημιών. Οι εκδότες ωστόσο επιθυμούσαν την εκδίκαση της υπόθεσης στην Αμερική, όπου οι νόμοι περί δυσφήμισης ήταν πολύ πιο χαλαροί [All2004].

Η γενική σύγχυση είναι προφανής. Δεν είναι λίγοι εκείνοι που υποστηρίζουν την περίπτωση Παγκόσμιων Νόμων για τις Νέες Τεχνολογίες, ανεξάρτητα από γεωγραφικούς περιορισμούς. Η σύσταση γενικών νόμων θα έλυνε πολλές διαφωνίες και προβλήματα. Όμως κάτι τέτοιο θα είχε πολλές δυσκολίες στην πραγμάτωσή του και γι' αυτό θα έπαιρνε πολύ χρόνο. Στο μεταξύ η κατάσταση παραμένει η ίδια, αν όχι χειρότερη.

3.3. Το Διαδίκτυο

Από το ξεκίνημά του, το πρωταρχικό χαρακτηριστικό του Διαδικτύου ήταν η ελεύθερη ανταλλαγή ιδεών, μηνυμάτων, εικόνων και γενικά ψηφιακών αντικειμένων. Στην αρχή δεν ήταν καθόλου εύκολο να προβλεφτούν οι μεγάλες του δυνατότητες, καθώς και η ραγδαία εξέλιξή του με τον εκπληκτικό αριθμό χρηστών του. Όμως αυτή η εξέλιξη είναι πραγματικότητα και υπάρχουν σοβαρές ενδείξεις ότι θα συνεχίσει να εξελίσσεται και τα επόμενα χρόνια. Πέρα όμως από την αρχική ιδέα, παράνομες πράξεις που πραγματοποιούνται στα όρια του διαδικτύου δημιουργούν πολλά προβλήματα. Ως ενοχλητική και διασπαστική συμπεριφορά μπορεί να χαρακτηριστεί η μη εξουσιοδοτημένη πρόσβαση, η κλοπή ηλεκτρονικής ιδιοκτησίας, η εξαπόλυση καταστρεπτικών ιών, ο ρατσισμός, η δυσφήμιση, η παρενόχληση σε ένα γεγονός [Joh1997]. Έτσι, από τη μια πλευρά είναι οι νέες τεχνολογίες και το Διαδίκτυο με το πρωταρχικό χαρακτηριστικό της ελεύθερης ανταλλαγής, που επιτρέπει όμως και παραβιάσεις, και από την άλλη είναι οι παράνομες πράξεις, ο νόμος και οι συνέπειές του.

Είναι χαρακτηριστικό ότι υπάρχουν δύο βασικές τάσεις στο Διαδίκτυο: 1) κάποιος θα πρέπει να πληρώσει για να πάρει και να χρησιμοποιήσει αυτό που ψάχνει και, 2) μπορεί κανείς να πάρει ό,τι ψάχνει δωρεάν. Η πρώτη περίπτωση είναι και πιο συνηθισμένη και είναι ακριβώς ό,τι γίνεται στον πραγματικό κόσμο. Στη περίπτωση του Διαδικτύου αυτό το ύφος χρησιμοποιείται στο διαφημιστικό χώρο, όπου προωθούνται προϊόντα με σκοπό να αυξηθεί ο αριθμός των καταναλωτών ή πελατών. Από την άλλη μεριά η δεύτερη και τελευταία περίπτωση βασίζεται σε άλλη φιλοσοφία, βλέποντας το διαδίκτυο σαν ένα νέο χώρο όπου δεν υπάρχουν διαφορές ανάμεσα στους ανθρώπους και όλοι συνεισφέρουν στην ανάπτυξή του. Όπως είπε και ο Rapaport «κανένας δεν είναι μικρός στο διαδίκτυο» ("*nobody is small on the web*") [Rap1997]. Αυτή η φιλοσοφία είναι περισσότερο έκδηλη στη βιομηχανία

προγραμματιστικού υλικού. Υπάρχει προγραμματιστικό υλικό που μπορεί κάποιος να αγοράσει και συνήθως πωλείται από μεγάλες εταιρίες και υπάρχει και προγραμματιστικό υλικό που δίνεται δωρεάν στο διαδίκτυο. Το τελευταίο σκεπτικό υποστηρίζεται ακράδαντα από το GNU. GNU είναι η επαναληπτική συντομογραφία των λέξεων "GNU's Not Unix". Το GNU λανσαρίστηκε το 1984 με την ανάπτυξη ενός λειτουργικού συστήματος που έμοιαζε κατά πολύ στο λειτουργικό σύστημα Unix, αλλά όμως θα ήταν δωρεάν προγραμματιστικό υλικό: το GNU σύστημα [GNU2004]. *Δωρεάν προγραμματιστικό υλικό* δε σημαίνει απλά ότι ο χρήστης έχει την άδεια να *τρέξει* ένα εκτελέσιμο πρόγραμμα. Σημαίνει επίσης ότι ο χρήστης είναι απόλυτα ελεύθερος να αντιγράψει, να διανείμει, να μελετήσει να αλλάξει και να βελτιώσει το προγραμματιστικό υλικό. Είναι θέμα ελευθερίας.

Ένα πρόγραμμα θεωρείται δωρεάν ή ελεύθερο προγραμματιστικό υλικό, και αναφέρεται ως πρόγραμμα ανοικτής πηγής (*open source project*) αν οι χρήστες έχουν όλες τις προαναφερθείσες ελευθερίες. Έτσι οι χρήστες θα πρέπει να είναι ελεύθεροι να επανακατανείμουν τα αντίγραφα, με ή χωρίς τροποποιήσεις, δωρεάν ή χρεώνοντας τη διανομή, σε οποιονδήποτε οπουδήποτε, χωρίς να πρέπει να ρωτήσουν ή να πληρώσουν για την άδεια [GNU2004]. Και αν κάποιος χρήστης έχει δημοσιεύσει τις αλλαγές του, δεν υποχρεούται να ειδοποιήσει κανέναν ιδιαίτερα ή με κάποιον ιδιαίτερο τρόπο. Η ελευθερία της χρήσης ενός προγράμματος σημαίνει ελευθερία χρήσης αυτού από οποιονδήποτε τύπο ανθρώπου ή οργανισμού σε οποιοδήποτε τύπο υπολογιστή, για οποιαδήποτε εργασία και χωρίς να απαιτείται επικοινωνία με αυτόν που ανέπτυξε το πρόγραμμα ή με κάποιον ιδιαίτερο πράκτορα.

Παρόλ' αυτά, η παραπομπή ή η αναφορά, ότι δηλαδή ένα νέο πρόγραμμα βασίζεται σε GNU προγραμματιστικό υλικό, μπορεί να θεωρηθεί χωρίς αμφιβολία ως περιοριστικό στοιχείο. Αν κάποιος χρησιμοποιεί GNU προγραμματιστικό υλικό σαν δομικό κομμάτι για ένα νέο προγραμματιστικό υλικό, τότε και το νέο πρόγραμμα θα χαρακτηριστεί ως GNU. Η φιλοσοφία είναι να βοηθιέται κανείς, αλλά και να βοηθά άλλους. Αυτή η κυρίαρχη έννοια για δωρεάν προγραμματιστικό υλικό μπορεί να επεκταθεί και σε άλλου είδους ψηφιακά αντικείμενα, όπως είναι οι εικόνες και η μουσική, ερχόμενη σε σύγκρουση με την έννοια προστασίας της πνευματικής ιδιοκτησίας (*copyright*).

Με σκοπό να αποφευχθούν παραβιάσεις απλές ή νομικές, θα μπορούσε να υπάρξει πρόταση για εξονυχιστικό έλεγχο του Διαδικτύου έναντι απαράδεκτων πράξεων ή λειτουργιών. Μια τέτοια πρόταση ωστόσο θα μπορούσε να χαρακτηριστεί σχέση ουτοπία. Είναι αρκετό να δει κανείς τι έγινε στην Αυστραλία για να καταλάβει

πόσο μη πρακτικό κάτι τέτοιο θα ήταν. Όταν η Αυστραλιανή κυβέρνηση αποφάσισε ότι ήθελε να περιορίσει τη σύμβαση ονομασιών για την Αυστραλία, ο πρακτικός αριθμός των εργαζομένων που χρειάστηκε ήταν εξαιρετικά μεγάλος [Bla2000]. Για παράδειγμα κάθε λέξη που θα θεωρείτο προσβλητική δε θα έπρεπε να έχει την κατάληξη ".au" στο *βασικό όνομα (domain name)*. Αυτή η προσέγγιση ναυάγησε παταγωδώς, μια και πολλοί είναι εκείνοι που χρησιμοποίησαν τις πιστωτικές τους κάρτες και μίσθωσαν βασικά ονόματα οπουδήποτε αλλού εκτός από Αυστραλία, χρησιμοποιώντας την κατάληξη ".com".

Αν ένα τόσο απλό θέμα όπως είναι η ονομασία των URLs είναι δύσκολο να ελεγχθεί, τότε ο έλεγχος της μεταφοράς κάθε ψηφιακού αντικειμένου, όπως των εικόνων, βίντεο ή προγραμματιστικού υλικού είναι καθόλα αδύνατος. Κάτω από αυτή τη σκοπιά θα πίστευε κανείς ότι μια και είναι αδύνατον να ελεγχθεί το Διαδίκτυο, θα πρέπει να παραμείνει έτσι όπως είναι. Αλλά είναι αυτό σωστό; Τι γίνεται με τα θέματα προστασίας πνευματικών δικαιωμάτων των ψηφιακών αντικειμένων; Είναι η προστασία πνευματικών δικαιωμάτων και η ελεύθερη διακίνηση πράγματι δύο συγκρουόμενα θέματα;

Το γεγονός είναι ότι το Διαδίκτυο δεν είναι απαλλαγμένο από τα πνευματικά δικαιώματα των ψηφιακών αντικειμένων, ανεξάρτητα από το τι αρέσει σε πολλούς να πιστεύουν [All2004]. Και εφόσον η λύση δεν είναι η απαγόρευση οποιουδήποτε ψηφιακού αντικειμένου, η ύπαρξη ενός τρόπου για την πιστοποίηση της αυθεντικότητας ενός υδατογραφημένου αντικειμένου ή του νόμιμου κατόχου θα έδινε νέο ύψος στη φιλοσοφία που διαπνέει το Διαδίκτυο.

Κάτι τέτοιο θα μπορούσε να πραγματοποιηθεί, όπως γίνεται σε πολλές περιπτώσεις, με κατάλληλη *εκπαίδευση* των ανθρώπων και διαμορφώνοντας την κοινωνική τους συμπεριφορά έτσι ώστε να αντιδρούν με σεβασμό σε θέματα προστασίας πνευματικών δικαιωμάτων. Είναι γνωστό εξάλλου ότι η κοινωνική διαπαιδαγώγηση στο διαδίκτυο (*online*) σημαίνει πολλά περισσότερα από ό,τι νέοι νόμοι και προσαρμοσμένα διατάγματα [Joh1997]. Και όπως ισχυρίστηκε και ο Εμμανουέλ Καντ στην εργασία του "Grundlegung der Metaphysik der Sitten" [Koe2004]:

"Then, that the moral is good, it is not enough; for the ethical laws worth observing, they should also be driven by esoteric will." ("Denn bei dem, was moralisch gut sein soll, ist es nicht

genug, daß es dem sittlichen Gesetze gemäß sei, sondern es muß auch um desselben willen geschehen.")

Δηλαδή

«Ότι το ηθικό είναι καλό δεν είναι αρκετό, η τήρηση των ηθικών νόμων θα πρέπει να συνοδεύεται και από εσωτερική θέληση.»

Είναι επίσης γνωστό ότι αν οι χρήστες είναι ενημερωμένοι για τις συνέπειες, τότε διαμορφώνουν ανάλογα και τις πράξεις τους. Σύμφωνα με τους Kreie και Cronan ίσως το πιο χρήσιμο συμπέρασμα μιας από των ερευνών τους είναι ότι τόσο οι άνδρες όσο και οι γυναίκες, αν γνωρίζουν τις συνέπειες μιας δεδομένης συμπεριφοράς τους, τότε είναι πολύ πιθανόν να την αλλάξουν [Kre1998]. Γι' αυτόν το λόγο οι χρήστες των υπολογιστών θα πρέπει εξ αρχής να είναι γνώστες των συνεπειών των πράξεών τους [Joh1997].

Μια πιθανή λύση θα μπορούσε να είναι η ακόλουθη: να υπάρχουν όλα τα ψηφιακά αντικείμενα στο Διαδίκτυο, αλλά εκείνα που είναι κατοχυρωμένα θα μπορούσε να είναι υδατογραφημένα. Ο έλεγχος για υδατογραφημένα ψηφιακά αντικείμενα δε θα μπορούσε να είναι καθολικός, αλλά μια εξουσιοδοτημένη ομάδα θα μπορούσε σε τακτά χρονικά διαστήματα να πραγματοποιεί ελέγχους και να πιστοποιεί την αυθεντικότητα των ψηφιακών αντικειμένων ή τη νόμιμη κυριότητα των κατόχων τους, τιμωρώντας τους παραβάτες. Έγκειται στους χρήστες αν επιθυμούν να εκθέσουν την προσωπική τους δουλειά στο Διαδίκτυο σαν υδατογραφημένη ή όχι. Το να εκθέσει κάποιος τη δουλειά του μη υδατογραφημένη δεν εμπίπτει σε πειθαρχική επίπληξη. Αλλά είναι αυτοί οι ίδιοι οι χρήστες που μπορεί να επιθυμούν τη χρήση κατοχυρωμένων ψηφιακών αντικειμένων. Σε κάθε περίπτωση η κατοχύρωση πνευματικών δικαιωμάτων θα πρέπει να γίνεται σεβαστή. Αν αφήσουμε το σύστημα του διαδικτύου να λειτουργήσει με κανόνες σαν αυτούς, τότε το ίδιο το σύστημα θα βρει ποιος είναι ο πιο αποδοτικός τρόπος για να εξελιχθεί.

3.4. Θέματα υδατογράφησης

Οι τεχνικές υδατογράφησης δεν είναι καινούργιες. Ένα από τα αρχαιότερα υδατογραφήματα βρέθηκε στην περιοχή του Cambridge (c. 1550) και απεικόνιζε το μονόγραμμα TGE RG, που ήταν η συντομογραφία του ονόματος του παραγωγού χαρτιού και του τόπου (Thomas Goodrich Eliensis – Remy/Remigius Guedon) [Pet1999]. Εκείνη την εποχή τα υδατογραφήματα υπήρχαν κυρίως για την εξακρίβωση του πολτού που θα παρήγαγε το χαρτί, ως μια βεβαίωση της ποιότητάς του. Τα υδατογραφήματα είναι επίσης γνωστά και από τα χαρτονομίσματα.

Στην εποχή της πληροφορίας, η διεισδυτική φύση των ψηφιακών αντικειμένων έχει εισχωρήσει και στις πιο κλασσικές μεθόδους. Συνεπώς, από τις μεθόδους υδατογράφησης περάσαμε στις ψηφιακές μεθόδους υδατογράφησης. Η ψηφιακή υδατογράφηση θα μπορούσε να χαρακτηριστεί ως η τεχνική που μεταφέρει πληροφορία ανεπαίσθητα ή όχι, πρώτα με την ένθεσή της μέσα στα αρχικά δεδομένα και έπειτα με την ανάκτησή της. Διαφορετικοί τύποι τεχνικών υδατογράφησης έχουν αναπτυχθεί για διαφορετικούς τύπους ψηφιακών αντικειμένων, όπως το κείμενο, ο ήχος, η εικόνα και το βίντεο.

3.4.1 Υδατογράφηση κειμένου

Οι τεχνικές υδατογράφησης που εφαρμόζονται σε κείμενα αποτελούν και τις πιο δύσκολες τεχνικές. Η υδατογράφηση του προγραμματιστικού υλικού θα μπορούσε επίσης να χαρακτηριστεί σαν ένας τύπος υδατογράφησης κειμένου.

Θα αναφερθούμε με συντομία στις διαφορετικές τεχνικές που χρησιμοποιούνται για υδατογράφηση κειμένου. Κατά πρώτον, οι τεχνικές ανοικτού διαστήματος εισάγουν κενά διαστήματα. Τα κενά ανάμεσα στις προτάσεις ή στις λέξεις αποτελούν το κλειδί για την απόδειξη της γνησιότητας των κειμένων. Παρόμοιες με αυτές τις τεχνικές είναι οι τεχνικές μορφοποίησης του κειμένου, όπου η εμφάνιση και μόνο του κειμένου αναδεικνύει τη γνησιότητά του. Παράδειγμα τέτοιων μορφοποιήσεων θα μπορούσε να είναι η μετατόπιση των λέξεων ή των γραμμών σε ένα κείμενο. Στην κατηγορία των τεχνικών υδατογράφησης κειμένων ανήκουν και οι συντακτικές και σημασιολογικές μέθοδοι, όπου η γνησιότητα των κειμένων πιστοποιείται με τη συντακτική και τη σημασιολογική του ανάλυση αντίστοιχα. Τέλος, υπάρχουν και κάποιες τεχνικές όπου τα κείμενα τα

μεταχειρίζονται σαν εικόνες και εκεί εφαρμόζονται τεχνικές υδατογράφησης εικόνων.

Δυστυχώς είναι πολύ εύκολο να αφαιρεθούν εντελώς τα υδατογραφήματα από τα κείμενα, όταν αυτά έχουν εντεθεί με τεχνικές όπως η μετατόπιση γραμμών, η μετατόπιση λέξεων, η μορφοποίηση γραμματοσειρών και γενικά με τεχνικές που αλλάζουν ελάχιστα την εμφάνιση του κειμένου. Αντιθέτως, οι τεχνικές υδατογραφήματος που στηρίζονται σε συντακτική και σημασιολογική ανάλυση των κειμένων είναι περισσότερο ανθεκτικές.

3.4.2 Υδατογράφηση ήχου

Οι τεχνικές υδατογράφησης ήχου παρουσιάζουν μεγάλο εμπορικό ενδιαφέρον, εφόσον πολλά κομμάτια μουσικής και ήχων διακινούνται στο Διαδίκτυο. Υδατογράφηση ήχου είναι η τεχνική κατά την οποία έχουμε ένθεση δεδομένων στην πλευρική ζώνη δεδομένων. Η χρησιμότητά της είναι δικαιολογημένη αν κάποιος σκεφτεί τη διένεξη αναφορικά με την πειρατεία ποιοτικών μουσικών CD στο Διαδίκτυο σε μορφή MPEG Layer III (MP3). Οι τεχνικές υδατογράφησης ήχων που έχουν προταθεί σκοπεύουν στην ανάπτυξη ικανοποιητικού μηχανισμού υδατογράφησης και κάποιες από αυτές μπορεί επίσης να προσφέρουν ένα σύστημα παρακολούθησης για τον εντοπισμό μουσικών κομματιών στην τηλεόραση, στο ραδιόφωνο, καθώς και στο Διαδίκτυο.

3.4.3 Υδατογράφηση εικόνας

Οι τεχνικές υδατογράφησης εικόνων είναι εξίσου πολύ σημαντικές, εφόσον οι ψηφιακές εικόνες μπορούν να παραχθούν από πολλές πηγές, όπως από σαρωτές (*scanner*), ψηφιακές φωτογραφικές μηχανές, υπολογιστές, ψηφιακές βιντεοσκοπικές μηχανές και ακόμα από δορυφόρο. Αυτές μπορούν να διαχωριστούν σε ορατές τεχνικές υδατογράφησης και σε αόρατες. Στις ορατές τεχνικές υδατογράφησης το υδατογράφημα υπερθέτεται στην αρχική εικόνα με αποτέλεσμα να γίνεται ορατό. Αντίθετα στις αόρατες τεχνικές υδατογράφησης το υδατογράφημα δε φαίνεται. Στην ουσία οι πρώτες τεχνικές σκοπεύουν στο να ενημερώσουν το χρήστη για τα δικαιώματα πνευματικής ιδιοκτησίας κατά την εμφάνιση των εικόνων, ενώ στις τελευταίες τεχνικές το υδατογράφημα παρέχει προστασία χωρίς ορατή αλλαγή της εικόνας. Τέτοιες τεχνικές συνήθως μεταβάλλουν την ένταση των εικονοστοιχείων (*pixel*) και αναφέρονται στο χωρικό πεδίο (*spatial domain*

techniques) ή μεταβάλλουν τους συντελεστές της εικόνας μετά από κάποιο μετασχηματισμό και αναφέρονται στο πεδίο συχνοτήτων (*frequency domain techniques*).

3.4.4 Υδατογράφιση βίντεο

Όπως οι τεχνικές υδατογράφισης εικόνων διακρίνονται σε ορατές και αόρατες, έτσι και οι τεχνικές υδατογράφισης βίντεο έχουν κατ' αναλογία τον ίδιο διαχωρισμό. Το λογότυπο κάθε τηλεοπτικού σταθμού που μεταδίδεται μαζί με κάθε βίντεο αποτελεί χαρακτηριστικό παράδειγμα της υδατογράφισης βίντεο. Αλλά και οι αόρατες τεχνικές υδατογράφισης είναι επίσης πολύ δημοφιλείς, εφόσον υδατογραφούν το βίντεο χωρίς να το επηρεάζουν ορατά.

3.5. Γιατί υδατογράφιση;

Είναι προφανές ότι δεν υπάρχει μια γενική μεθοδολογία υδατογράφισης. Υπάρχουν διαφορετικά ψηφιακά αντικείμενα και για καθέναν τύπο τους υπάρχει μια πληθώρα ψηφιακών τεχνικών. Επιπροσθέτως, οι τεχνικές υδατογράφισης είναι εξαρτημένες και από το σκοπό για τον οποίο θα χρησιμοποιηθούν. Υπάρχουν αρκετοί λόγοι για τους οποίους θα εφαρμόζαμε τεχνικές υδατογράφισης, και σε κάθε περίπτωση αλλάζουν οι απαιτήσεις των συστημάτων υδατογράφισης.

Ο ρόλος του υδατογραφήματος είναι πολύμορφος. Μπορεί να χρησιμοποιηθεί για πιστοποίηση αυθεντικότητας των ψηφιακών αντικειμένων, για αναγνώριση του δημιουργού, για προστασία έναντι παραβιάσεων πνευματικής ιδιοκτησίας, για πιστοποίηση των νόμιμων κατόχων και για την παρεμπόδιση κάποιων από την ιδιοποίηση ξένης πνευματικής ιδιοκτησίας.

3.5.1 Απόδειξη γνησιότητας

Μια πολύ κοινή εφαρμογή των τεχνικών υδατογράφισης είναι εκείνη κατά την οποία υπάρχει η απαίτηση για την απόδειξη γνησιότητας (*authentication*) των ψηφιακών αντικειμένων. Στις εφαρμογές της απόδειξης γνησιότητας οποιαδήποτε αλλαγή των αρχικών δεδομένων θα πρέπει να εντοπίζεται. Για αυτόν το σκοπό χρησιμοποιούνται *ευπρόσβλητα* (*fragile*) υδατογραφήματα. Αυτά δεν απαιτείται να είναι ανθεκτικά σε διάφορες τροποποιήσεις, όπως είναι οι γεωμετρικοί

μετασχηματισμοί και η συμπίεση. Εκμεταλλευόμενοι τα διάφορα χαρακτηριστικά των ψηφιακών αντικειμένων, όπως τα χαρακτηριστικά των ακμών των εικόνων, μπορεί να γίνει έλεγχος της ακεραιότητας των αρχικών δεδομένων και να ανιχνευθούν πιθανές τροποποιήσεις. Φυσικά μπορούν να χρησιμοποιηθούν και υδατογραφήματα που δεν είναι ευπρόσβλητα, για την απόδειξη γνησιότητας των ψηφιακών αντικειμένων. Όταν τα υδατογραφήματα είναι ευπρόσβλητα τότε η απουσία τους είναι εκείνη που αποτελεί ισχυρή ένδειξη ότι το συγκεκριμένο ψηφιακό αντικείμενο έχει τροποποιηθεί, ενώ όταν χρησιμοποιούνται ανθεκτικά υδατογραφήματα η σύγκριση μεταξύ του ανακτημένου υδατογραφήματος και του αρχικού μάς δίνει την ακεραιότητα της εικόνας.

3.5.2 Προστασία πνευματικών δικαιωμάτων

Η προστασία των πνευματικών δικαιωμάτων (*copyright protection*) είναι η πιο σημαντική εφαρμογή της υδατογράφησης σήμερα. Η δημοσίευση των ψηφιακών αντικειμένων στον Παγκόσμιο Ιστό (*WWW*) συνεισφέρει στην ευρεία διάδοσή τους, αφήνοντας συχνά τους δημιουργούς απροστάτευτους από μη εξουσιοδοτημένη χρήση των δημιουργημάτων τους. Τα *δικαιώματα πνευματικής ιδιοκτησίας (IPRs)* των δημιουργών μπορούν να διασφαλιστούν με την ένθεση πληροφορίας σχετικής με τα αρχικά δεδομένα ή τον νόμιμο κάτοχο των δεδομένων, παρεμποδίζοντας έτσι άλλους να ισχυριστούν την κυριότητα.

Για μια τέτοια χρήση τα υδατογραφήματα θα πρέπει να είναι ανθεκτικά σε οποιαδήποτε τροποποίηση των δεδομένων. Επιπλέον, το εξαγόμενο υδατογράφημα θα πρέπει να είναι ευκρινές και να μπορεί να αποδεικνύει τη νόμιμη κατοχή.

3.5.3 Δακτυλικό αποτύπωμα

Η τεχνική των δακτυλικών αποτυπωμάτων (*fingerprinting*) χρησιμοποιείται για την επιβεβαίωση των νόμιμων αποδεκτών [Kut2000]. Με την τεχνική αυτή ένα διαφορετικό υδατογράφημα εντίθεται σε καθένα ξεχωριστό ψηφιακό αντικείμενο που διανέμεται. Οι τεχνικές των δακτυλικών αποτυπωμάτων χρησιμοποιούνται για την εξακρίβωση της ταυτότητας του τελευταίου διανομέα των ψηφιακών αντικειμένων. Έτσι όταν εντοπίζονται παράνομα αντίγραφα, μπορεί πολύ εύκολα να εντοπιστεί ο τελευταίος διανομέας.

Η ύπαρξη του υδατογραφήματος στις τεχνικές των δακτυλικών αποτυπωμάτων είναι *ζωτικής* σημασίας. Συνεπώς και εδώ, όπως και στις τεχνικές για

την προστασία των πνευματικών δικαιωμάτων, τα υδατογραφήματα θα πρέπει να είναι ανθεκτικά σε επιθέσεις και ευκρινή κατά τη διαδικασία ανάκτησης.

3.5.4 Προστασία αντιγραφής

Οι τεχνικές για την προστασία των αντιγραφών (*copy protection*) ακολουθούν μια *πιο αυστηρή πολιτική* σε σύγκριση με τις προηγούμενες τεχνικές. Ο ρόλος του υδατογραφήματος εδώ δεν είναι να εξακριβώνει την ταυτότητα των κατόχων ή των νόμιμων αποδεκτών, αλλά να ενεργοποιήσει μηχανισμούς προστασίας, έτσι ώστε να απαγορεύσει την αντιγραφή των ψηφιακών αντικειμένων σε μη εξουσιοδοτημένους χρήστες.

Η υδατογράφιση μπορεί επίσης να χρησιμοποιηθεί για την κωδικοποίηση πληροφορίας αντιγραφής, η οποία όμως να μπορεί να ανακτηθεί τόσο από ψηφιακά, όσο και από αναλογικά συστήματα. Συνήθως, τα συστήματα προστασίας αντιγράφων επιτρέπουν τη δυνατότητα μόνο *μιας* αντιγραφής.

Η προστασία από τις αντιγραφές εφαρμόστηκε στα συστήματα DVD, όπου ένα υδατογράφημα, που περιέχει την πληροφορία της αντιγραφής, έχει ενθεθεί στα δεδομένα. Οι τεχνικές για την προστασία από τις αντιγραφές εφαρμόζονται κυρίως σε κλειστά συστήματα και λιγότερο σε ανοιχτά όπως το Διαδίκτυο.

3.6. Συμπεράσματα

Το Διαδίκτυο κυβερνείται από δύο κύριες τάσεις: στην πρώτη έχουμε την ελεύθερη διακίνηση όλων των ψηφιακών αντικειμένων, ενώ στη δεύτερη έχουμε τις συναλλαγές που βασίζονται στα χρήματα και αποτελούν την εξέλιξη του παραδοσιακού εμπορίου. Και οι δύο τάσεις είναι σεβαστές, και η απόφαση για το αν τα ψηφιακά αντικείμενα θα πρέπει να είναι κατοχυρωμένα, είναι αποκλειστική των δημιουργών τους.

Η απότομη ανάπτυξη του Διαδικτύου παρέχει άφθονες ευκαιρίες σε απатеώνες για να εξασκήσουν τις δεξιότητές τους. Υπάρχουν πολλά που πρέπει να γίνουν για να εμποδιστεί η μη εξουσιοδοτημένη χρήση των ψηφιακών αντικειμένων. Κατά πρώτον θα πρέπει να διαφοροποιηθεί η συμπεριφορά των χρηστών, έτσι ώστε αυτοί να συμμορφώνονται με τα δικαιώματα πνευματικής ιδιοκτησίας (*IPRs*). Το πιο φυσιολογικό θα ήταν οι πράξεις των χρηστών να ήταν νόμιμες, επειδή έτσι τους υπαγόρευε η συνείδησή τους. Εκπαιδεύοντας τους ανθρώπους και διαμορφώνοντας

την κοινωνική τους συμπεριφορά, θα μπορούσαν να τους κάνουν να αντιδρούν με σεβασμό στην πνευματική ιδιοκτησία. Ο νόμος θα πρέπει και αυτός να βοηθήσει προς αυτήν την κατεύθυνση. Όταν υπάρχει ενημέρωση για τις συνέπειες, τότε οι άνθρωποι διαμορφώνουν αντίστοιχα τις πράξεις τους. Η ιδιοκτησία των ψηφιακών αντικειμένων θα μπορούσε να βεβαιώνεται με την ύπαρξη ενός υδατογραφήματος μέσα σε αυτά.

Παρόλ' αυτά ανακύπτουν πολλά προβλήματα. Κατά πρώτον δεν υπάρχει διεθνής νομοθεσία που να καλύπτει την *περιοχή του διαδικτύου* και κάτι τέτοιο είναι εξαιρετικά δύσκολο, καθώς υπάρχουν διαφορετικοί νόμοι και ποινές σε κάθε χώρα. Επιπλέον, δεν υπάρχει κοινά αποδεκτό πρότυπο στις τεχνικές υδατογράφησης, με αποτέλεσμα να μην υπάρχει επίσημη τεχνική υδατογράφησης, που να είναι *νομικά* κατοχυρωμένη και αποδεκτή από όλους. Συνεπώς, ίσως το πιο πολύπλοκο ζήτημα είναι το θέμα της συνεργασίας διαφορετικών επιστημονικών αρχών και όλων των χωρών σε ένα κοινό σημείο αναφοράς.

Σε αυτό το κεφάλαιο επιχειρήθηκε η παρουσίαση του προβλήματος των δικαιωμάτων της πνευματικής ιδιοκτησίας. Συζητήθηκαν πιθανές λύσεις και τα προβλήματα τους. Για την επίλυση σύνθετων προβλημάτων απαιτείται η κριτική σκέψη αντί της επίκρισης, η αναγνώριση των προβλημάτων, η θέληση για την επίλυσή τους, η εφαρμογή των θεωριών, πρακτικά και εύχρηστα εργαλεία και φυσικά θάρρος και υπευθυνότητα για την αντιμετώπιση των συνεπειών.

Κεφάλαιο 4

Τεχνική απόκρυψης βασιζόμενη σε υπολογιστικά δύσκολα προβλήματα

4.1. Εισαγωγή

Σε αυτό το κεφάλαιο παρουσιάζεται μια μέθοδος απόκρυψης πληροφορίας που μπορεί να χρησιμοποιηθεί για να αποδειχθεί η κατοχή πνευματικής ιδιοκτησίας [Arm2003]. Όταν ο όγκος της πληροφορίας που εντίθεται σε ένα μέσο είναι μεγάλος, όπως είναι μια εικόνα, τότε μιλάμε για τεχνικές απόκρυψης πληροφορίας γενικά, δίχως να εξετάζεται ο σκοπός για τον οποίο γίνεται. Στις τεχνικές υδατογράφησης ο όγκος της πληροφορίας που εντίθεται είναι σχετικά μικρός, αλλά ο σκοπός είναι ξεκάθαρος. Βασική επιδίωξη στις μεθόδους υδατογράφησης είναι η προστασία των πνευματικών δικαιωμάτων των κατόχων των αντικειμένων και η πιστοποίηση της αυθεντικότητά τους. Στο συγκεκριμένο κεφάλαιο παρουσιάζεται μια μέθοδος απόκρυψης της πληροφορίας με σκοπό ίδιο με αυτόν των τεχνικών υδατογράφησης. Για αυτόν ακριβώς το λόγο στην συνέχεια θα χρησιμοποιείται ο όρος *υπογραφή*, με την έννοια του *υδατογραφήματος*, ενώ καμιά σχέση δε θα έχει με τις ψηφιακές υπογραφές που περιγράφηκαν σε προηγούμενο κεφάλαιο. Οι ψηφιακές υπογραφές που βασίζονται στα συστήματα κρυπτογράφησης δημοσίου

κλειδιού έχουν το μειονέκτημα ότι είναι πολύ ευάλωτες σε αλλαγές μερικών bits (έτσι ώστε να καθίσταται αδύνατη η χρήση τους για υδατογράφιση/απόκρυψη πληροφορίας), ενώ οι συγκεκριμένες υπογραφές που περιγράφονται σε αυτό το κεφάλαιο μπορούν να ικανοποιήσουν το σκοπό για τον οποίο εισήχθηκαν, ακόμα και αν καταστραφεί ένα μέρος τους. Αυτή η μέθοδος βασίζεται στην ένθεση μιας υπογραφής στα αρχικά δεδομένα, αλλά αντί να χρησιμοποιηθεί η υπογραφή η ίδια για να αποδειχθεί η κυριότητα των ψηφιακών αντικειμένων, χρησιμοποιείται ένα συγκεκριμένο «μετα-χαρακτηριστικό» της υπογραφής.

4.2. Προστασία με χρήση συμβολοσειρών - υπογραφών

Είναι γεγονός στις μέρες μας ότι τα ψηφιακά αντικείμενα είναι εκτεθειμένα όλο και περισσότερο σε διάφορες πράξεις, όπως είναι η μη εξουσιοδοτημένη τροποποίηση, η αναπαραγωγή και η επαναδιανομή, όχι μόνο εξαιτίας της ευρείας διάδοσης της χρήσης του Διαδικτύου, αλλά επίσης εξαιτίας της επινόησης μέσων για ανέξοδη αναπαραγωγή δεδομένων. Αυτό έχει καθορίσει και την εμφάνιση μιας ποικιλίας μεθόδων προστασίας ([Ben1996, Fab1999]) βασιζόμενων σε υπογραφές για την προστασία των κατοχυρωμένων ψηφιακών αντικειμένων, όπως είναι ο ήχος, οι εικόνες και το βίντεο, εξασφαλίζοντας ότι ο κάτοχος των αντικειμένων θα μπορεί να αναγνωρισθεί.

Η πλειοψηφία αυτών των μεθόδων αντιμετωπίζουν δύο βασικές δυσκολίες: (α) το γεγονός ότι οποιοσδήποτε μπορεί να χρησιμοποιήσει την ψηφιακή υπογραφή για να ισχυριστεί το νόμιμο κάτοχο των δεδομένων (που παρέχονται και από τα οποία έχει κλαπεί η υπογραφή), και (β) το γεγονός ότι η αύξηση του μεγέθους της υπογραφής είτε κάνει τη μέθοδο λιγότερο ανθεκτική σε επιθέσεις (όπως στην περίπτωση μεγάλου μη επαναλαμβανόμενου όγκου δεδομένων υπογραφών), είτε κάνει τον μη εξουσιοδοτημένο εντοπισμό και άρα και την εξαγωγή της υπογραφής ευκολότερη (όπως στην περίπτωση μεγάλου αριθμού επαναλαμβανόμενων υπογραφών). Οι περισσότερες μέθοδοι ενθέτουν μια εξειδικευμένη ανά χρήστη ακολουθία δυαδικών ψηφίων στο υλικό που θέλουν να προστατέψουν, και όταν αυτή εντοπίζεται εξακριβώνεται μοναδικά ο νόμιμος κάτοχος σε περιπτώσεις αμφισβήτησης των πνευματικών δικαιωμάτων. Ωστόσο, δεδομένου του γεγονότος ότι η αναγνώριση του νόμιμου κατόχου επηρεάζεται από την απλή παρουσίαση της υπογραφής έχει το μειονέκτημα ότι αν κλαπεί η υπογραφή, μπορεί επομένως να

χρησιμοποιηθεί από οποιονδήποτε για να ισχυριστεί ιδιοκτησία των δεδομένων (επιθέσεις αντιστροφής). Επιπλέον, οι περισσότερες μέθοδοι χρησιμοποιούν είτε πολύ μεγάλη υπογραφή, είτε επαναλήψεις μιας καθορισμένης μικρής ψηφιακής ακολουθίας αποτελούμενης από διαφορετικά δυαδικά ψηφία που συνήθως παράγονται τυχαία. Στην πρώτη περίπτωση, η μοναδική μεγάλη υπογραφή είναι πολύ ευαίσθητη μιας και ασήμαντες τροποποιήσεις στα δεδομένα-φορέα (*cover data*) μπορεί να καταστήσουν την υπογραφή άχρηστη. Στη τελευταία περίπτωση, εξαιτίας της επανάληψης, η υπογραφή είναι ευκολότερο να εντοπιστεί στατιστικά. Και στις δύο περιπτώσεις η χωρητικότητα των δεδομένων φορέα είναι πάντα ένα εμπόδιο [Sol2002], εφόσον η πρόσθεση μεγάλου όγκου δεδομένων σαν υπογραφή μπορεί να μειώσει σημαντικά την ποιότητα της εικόνας.

4.3. Γενική περιγραφή της προτεινόμενης μεθόδου

Η προτεινόμενη μέθοδος μπορεί να δώσει λύση και στα δύο προβλήματα που αναφέρθηκαν παραπάνω. Βασίζεται στις γνωστές *Διαντιδραστικές Αποδείξεις Μηδενικής Γνώσης (Zero Knowledge Interactive Proof protocol - ZKIP)* [Pap1994] για δύσκολα υπολογιστικά προβλήματα (*computationally intractable problems* ή *NP - complete*) [Gar1979], και ιδιαίτερα στα προβλήματα χρωματισμού γράφων με τρία χρώματα. Αυτό το πρόβλημα έγκειται στην ανάθεση τριών διαθέσιμων χρωμάτων στις κορυφές ενός γράφου έτσι ώστε κανένα ζεύγος γειτονικών κορυφών να μην έχει το ίδιο χρώμα. Το κύριο πλεονέκτημα της προτεινόμενης μεθόδου βασίζεται στην ιδέα ότι ο γράφος μαζί με τον 3-χρωματισμό των κορυφών του παίζει το ρόλο της υπογραφής και η αναγνώρισή της δεν πραγματοποιείται απλά από την επίδειξη του ίδιου του γράφου (όπως θα γινόταν με μια κατάλληλα κωδικοποιημένη υπογραφή, που θα αποτελείτο από μια ακολουθία δυαδικών ψηφίων). Αντίθετα, η αναγνώριση της υπογραφής συντελείται από την επίδειξη της γνώσης του 3-χρωματισμού, ο οποίος βάση της θεωρίας πολυπλοκότητας δεν είναι εύκολο να βρεθεί. Με άλλα λόγια, η ικανότητα μιας ακολουθίας δυαδικών ψηφίων να εξακριβώσει την ταυτότητα ενός προσώπου πηγάζει από την ερμηνεία της σαν ένα στιγμιότυπο ενός υπολογιστικά δύσκολου προβλήματος. Αυτό έχει την εξής επίδραση: ακόμα και αν κάποιος κλέψει την ακολουθία των δυαδικών ψηφίων (δηλαδή τον γράφο), δε θα είναι δυνατόν να υποδυθεί το νόμιμο κάτοχο των

δεδομένων, εφόσον απαιτείται η γνώση του 3-χρωματισμού για να προσδιοριστεί η ταυτότητα του.

Πιο συγκεκριμένα, η υπογραφή ενός χρήστη αναπαριστάται από τον πίνακα γειτνίασης ενός τυχαία 3-χρωματίσιμου γράφου με λόγο ακμών προς κορυφών μέσα σε μια περιοχή, η οποία πειραματικά είναι γνωστό ότι παράγει στιγμιότυπα τα οποία είναι τα πιο δύσκολα για να χρωματιστούν. Σε μια διαμάχη για τα δικαιώματα πνευματικής ιδιοκτησίας, ο νόμιμος κάτοχος θα είναι ο μόνος που θα μπορεί να παρουσιάσει γρήγορα τον 3-χρωματισμό του γράφου ως υπογραφή του, ενώ η υπολογιστική δυσκολία ενός 3-χρωματισμού για τέτοια στιγμιότυπα μπορεί να θεωρηθεί ως ισχυρή απόδειξη υπέρ του. Γι' αυτόν το λόγο, η μέθοδος που περιγράφεται εδώ αποτελεί επίσης μια εναλλακτική πρόταση για ισχυρή ηλεκτρονική υπογραφή. Αντίθετα με τις άλλες μεθόδους, η προτεινόμενη μέθοδος δεν εστιάζει σε στατιστικά χαρακτηριστικά υπογραφών (π.χ. τυχαιότητα), ή σε υπογραφές που αναπαριστούν το λογότυπο μιας εταιρίας, αλλά στην κατάλληλη αναπαράσταση συνδυαστικών αντικειμένων (γράφος) με χαρακτηριστικά που είναι δύσκολο να υπολογιστούν (3-χρωματισμός). Με αυτόν τον τρόπο ενισχύεται η προστασία των πνευματικών δικαιωμάτων των ψηφιακών αντικειμένων, εφόσον η αποκάλυψη της ψηφιακής υπογραφής ενός προσώπου δεν είναι αρκετή για την προσωποποίηση του νόμιμου κατόχου, και μόνο ο τελευταίος θα μπορεί αμέσως να παρουσιάσει τον 3-χρωματισμό, ο οποίος είναι δύσκολο να υπολογιστεί αν δεν είναι ήδη γνωστός. Μια τέτοια υπογραφή, της οποίας ο χαρακτηρισμός και η μοναδικότητα βασίζεται σε υπολογιστικά δύσκολα (*intractable*) προβλήματα, παρέχει ένα παράδειγμα μιας κρυπτογραφικά ασφαλούς υπογραφής κατά αναλογία με τις γεννήτριες κρυπτογραφικά ασφαλών ψευδοτυχαίων αριθμών.

Εκμεταλλευόμενοι την υπολογιστική πολυπλοκότητα αυτού του προβλήματος, προτείνεται η κατασκευή μεγάλων υπογραφών που αναπαριστούν τους πίνακες γειτνίασης τυχαίων 3-χρωματίσιμων γράφων. Το παραπάνω σύστημα έχει το επιπλέον πλεονέκτημα ότι η αποκάλυψη μιας τέτοιας υπογραφής δεν έχει συνέπειες, εφόσον είναι ουσιαστική η γνώση της ιδιότητας της υπογραφής (ο χρωματισμός της δηλαδή), η οποία μπορεί να χρησιμοποιηθεί ως απόδειξη της κυριότητας των αρχικών δεδομένων.

Επιπλέον, δεδομένου του γεγονότος ότι η προτεινόμενη μέθοδος χρησιμοποιεί *wavelet* μετασχηματισμό [Mal1999], μπορεί να εισαχθεί στα δεδομένα φορέα ένας μεγάλος όγκος δεδομένων (3-χρωματίσιμος γράφος μεγάλων διαστάσεων) χωρίς να επηρεαστεί η ποιότητα της εικόνας. Αυτό γίνεται μέσω της *wavelet* αναπαράστασης,

όπου παρέχεται μια χρονοχωρική αναπαράσταση των δεδομένων, παρέχοντας έτσι τη δυνατότητα ένθεσης μεγάλου όγκου δεδομένων, χωρίς να επηρεάζεται η ποιότητα. Τα πειράματα που παρουσιάζονται σε αυτό το κεφάλαιο δείχνουν ότι οι μετρήσεις PSNR παραμένουν υψηλότερες από 39dB. Ένα άλλο σημαντικό θέμα που διευθετείται στην προτεινόμενη τεχνική είναι η ανθεκτικότητα της μεθόδου σε επιθέσεις, παρόλο που απαιτεί την ενσωμάτωση μεγάλου αριθμού δεδομένων (τον πίνακα γειτνίασης ενός τρία χρωματίσιμου γράφου), καθώς και η ασφάλεια του γράφου. Χρησιμοποιείται ο διακριτός μετασχηματισμός *wavelet* έτσι ώστε να συγκεντρώνει την ενέργεια της εικόνας στην *LL* ζώνη. Με την ένθεση του γράφου στην *LL* ζώνη, επιτυγχάνεται η ανθεκτικότητα της τελικής εικόνας σε διάφορες αλλαγές και τροποποιήσεις. Ο προτεινόμενος αλγόριθμος είναι πράγματι ανθεκτικός σε μερικές τροποποιήσεις των εικόνων, αλλά δεν είναι ανθεκτικός σε πολύ ισχυρά εργαλεία όπως είναι το *StirMark*. Κάτι τέτοιο ωστόσο δεν προκαλεί έκπληξη, εφόσον το μέγεθος της εισαγόμενης πληροφορίας είναι κατά πολύ μεγαλύτερο από ένα τυπικό υδατογράφημα. Εκτός όμως από τη χρήση του μετασχηματισμού *wavelet*, η ανθεκτικότητα της μεθόδου ισχυροποιείται από τον τρόπο λειτουργίας της. Ακόμα και αν παραμείνει δηλαδή μόνο ένα μικρό τμήμα αυτών των δεδομένων στα αρχικά δεδομένα, μπορεί να καθοριστεί ο νόμιμος κάτοχος (εφόσον το πρόβλημα του 3-χρωματισμού των υπό-γράφων είναι επίσης ένα δύσκολο πρόβλημα για να υπολογιστεί). Με αυτό το σκεπτικό η καταστροφή ενός μέρους της υπογραφής από διάφορες τροποποιήσεις δεν αποτελεί πρόβλημα, αφού η υπολειπόμενη υπογραφή δύναται να πιστοποιήσει το νόμιμο κάτοχο.

Με βάση την πιστοποίηση μηδενικής γνώσης, έχουν προταθεί στο παρελθόν διάφορα συστήματα υπογραφής. Συγκεκριμένα, στη [Cra1999] ο Craver επιχειρεί την προστασία των ψηφιακών αντικειμένων με την παραγωγή μιας υπογραφής που είναι δύσκολο να αναπαραχθεί. Η μέθοδος που ακολουθεί βασίζεται στο πρόβλημα της Χαμιλτόνιας πορείας (*Hamiltonian Path problem*), το οποίο είναι υπολογιστικά δύσκολο (*computationally intractable*). Η πνευματική ιδιοκτησία των δεδομένων προστατεύεται από ένα πρωτόκολλο που αποδεικνύει τη νόμιμη κατοχή και συγχρόνως αποφεύγει την αποκάλυψη της υπογραφής. Σε ένα άλλο σύστημα που προτάθηκε από τον Hirotsugu στο [Hir1996], η τοπολογία που τοποθετείται ο γράφος εξαρτάται από τα χαρακτηριστικά της εικόνας που θα χρησιμοποιηθεί. Ο Hirotsugu κατορθώνει την προστασία των πνευματικών δικαιωμάτων της εικόνας χωρίς την αποκάλυψη της υπογραφής, δηλαδή του γράφου, εκμεταλλευόμενος το γεγονός ότι ο ισομορφισμός του γράφου (*graph isomorphism*) είναι ένα δύσκολο

υπολογιστικά πρόβλημα και χρησιμοποιεί επίσης το πρωτόκολλο *Διαντιδραστικών Αποδείξεων Μηδενικής Γνώσης (ZKIP)* για αυτό.

Η μέθοδος που παρουσιάζεται εδώ διαφέρει σημαντικά και από τις δύο προαναφερόμενες μεθόδους: ακόμα και αν κάποιος καταφέρει να εντοπίσει την υπογραφή, δε θα μπορέσει να τη χρησιμοποιήσει, εκτός και αν γνωρίζει τον τρία χρωματισμό του γράφου εκ των προτέρων. Η προτεινόμενη εφαρμογή του πρωτοκόλλου Μηδενικής Γνώσης (*Zero Knowledge*) έρχεται σε δεύτερο επίπεδο, και βασίζεται στη γνώση του τρία-χρωματισμού μιας ακολουθίας δυαδικών ψηφίων που αναπαριστούν το γράφο, ερμηνεύοντας έτσι ένα στιγμιότυπο του προβλήματος του τρία χρωματισμού. Η δύναμη των στιγμιότυπων των υπολογιστικά δύσκολων προβλημάτων που ενθέτονται σαν υδατογραφήματα σε ψηφιακές εικόνες έγκειται στο γεγονός ότι ακόμα και αν ο επίδοξος *επιθετικός (attacker)* κλέψει την υπογραφή, δεν μπορεί να χρησιμοποιήσει το υδατογράφημα για να υποδυθεί το νόμιμο κάτοχο. Με άλλα λόγια, η αποκάλυψη της υπογραφής δεν έχει συνέπειες στο νόμιμο κάτοχο, καθώς ο πιθανός επιθετικός θα δυσκολευτεί να βρει τον τρία χρωματισμό των κορυφών του γράφου. Με αυτόν τον τρόπο έχουμε ταυτόχρονα προστασία των πνευματικών δικαιωμάτων (*copyright protection*) εξαιτίας της ένθεσης των δυαδικών ψηφίων (υδατογράφημα) και απόδειξη γνησιότητας του κατόχου (*authentication*) εξαιτίας της γνώσης του τρία χρωματισμού του γράφου, που αναπαριστούν τα δυαδικά ψηφία. Μια άλλη διαφορά αυτής της προσέγγισης με την προσέγγιση του Hirotsugu είναι ότι ο γράφος που εντίθεται δεν εξαρτάται από τα αρχικά δεδομένα, οπότε μας δίνεται η δυνατότητα να χρησιμοποιήσουμε τη θεωρία των φαινομένων κατωφλίου σε δύσκολα υπολογιστικά προβλήματα για την κατασκευή αρκετά *δύσκολων* υπογραφών.

Αυτή η μέθοδος εστιάζει στο σχεδιασμό της και επιπλέον παρουσιάζει πειράματα που εφαρμόστηκαν σε μεγάλες έγχρωμες εικόνες. Από τα πειράματα συνεπάγεται ότι είναι δυνατόν να προσθέσουμε ένα (τρία-χρωματισμο) γράφο σε έγχρωμες εικόνες χωρίς να επηρεαστεί η ποιότητα της εικόνας (παρουσιάζονται μετρήσεις PSNR και παραδείγματα HVS). Ιδιαίτερα σημαντικά είναι τα πειράματα που αποδεικνύουν την ανθεκτικότητα της υπογραφής μετά από διάφορες επιθέσεις ακόμα και μετά από επιθέσεις που μειώνουν αισθητά την ποιότητα της εικόνας.

Αυτή η μέθοδος μπορεί να εφαρμοστεί σε οποιαδήποτε δεδομένα φορέα, όπως εικόνα ή βίντεο, που χρειάζονται προστασία [ArC2001, ACK2002]. Τα πειράματά μας ωστόσο, επικεντρώθηκαν στην περιοχή των εικόνων. Εδώ παρουσιάζονται πειράματα που αποδεικνύουν την ικανότητα εφαρμογής της

προτεινόμενης μεθόδου σε μεγάλες έγχρωμες εικόνες, δηλαδή την ικανότητα να ενσωματώσουμε έναν μεγάλο γράφο με τη χρήση των *wavelets* χωρίς να επηρεαστεί η ποιότητα των δεδομένων φορέα και η ανθεκτικότητα της μεθόδου έναντι ποικίλων επιθέσεων. Θα πρέπει να δοθεί έμφαση ότι σε αυτήν την περίπτωση η ανθεκτικότητα της υπογραφής έναντι των επιθέσεων δε βρίσκεται μόνο στη διαδικασία ένθεσης, αλλά επίσης και στα χαρακτηριστικά του γράφου, γι' αυτόν το λόγο η κυριότητα των πνευματικών δικαιωμάτων μπορεί να καθοριστεί ακόμα και αν ένα μικρό τμήμα του γράφου επιζήσει από τις επιθέσεις (εφόσον όπως αναφέρθηκε ο 3-χρωματισμός του ακόμα αποτελεί ένα δύσκολο συνδυαστικά πρόβλημα).

4.4. Στοιχεία θεωρίας NP-Completeness

Ένα πρόβλημα είναι *πολυωνυμικού χρόνου επίλυσης* αν υπάρχει αλγόριθμος που το λύνει σε χρόνο $T(n) = O(n^c)$, όπου c είναι μια σταθερά. Αντίθετα, ένα πρόβλημα θεωρείται *εκθετικού χρόνου επίλυσης* αν δεν υπάρχει κανένας αλγόριθμος πολυωνυμικού χρόνου για την επίλυσή του. Χονδρικά, ο χώρος των υπολογιστικών προβλημάτων μπορεί να χωριστεί σε τρεις κατηγορίες:

1. Πολυωνυμικά προβλήματα (P) – με αποδεδειγμένη την ύπαρξη πολυωνυμικού αλγορίθμου
2. Εκθετικά προβλήματα (E) – με αποδεδειγμένη μη ύπαρξη πολυωνυμικού αλγορίθμου
3. Δύσκολα (*intractable* ή *non-computable*) προβλήματα (I) – με μια ιδιότητα αναγωγής που θα περιγράψουμε πιο κάτω. Για τα προβλήματα αυτά δεν γνωρίζουμε εάν υπάρχει ή όχι λύση πολυωνυμικού χρόνου, αν και υπάρχουν σημαντικοί λόγοι να πιστεύουμε ότι τέτοια λύση δεν υπάρχει.

4.4.1 Ορισμός κλάσης NP

Παρακάτω δίνονται ορισμοί [NPC2004] για τα NP προβλήματα.

Ορισμός 1:

Ένα πρόβλημα ονομάζεται πολυωνυμικού μη ντετερμινιστικού χρόνου επίλυσης (*Non-deterministically Polynomial - NP*) αν μπορεί να βρεθεί μια

μη ντετερμινιστικού χρόνου επίλυσης μηχανή Turing που μπορεί να λύσει το πρόβλημα σε ένα πολυωνυμικό αριθμό κινήσεων.

Εναλλακτικός ορισμός:

Ορισμός 2:

Ένα πρόβλημα χαρακτηρίζεται ως NP αν απαιτείται πολυωνυμικός (ντετερμινιστικός) χρόνος για την πιστοποίηση της ορθότητας μιας υποψήφιας λύσης.

Να σημειωθεί εδώ ότι είναι πολύ πιο εύκολο και γρήγορο να ελεγχθεί μια λύση, παρά να βρεθεί.

Ορισμός 3:

Ένα πρόβλημα χαρακτηρίζεται ως NP αν υπάρχει ένας NP αλγόριθμος για αυτό, δηλαδή αλγόριθμος μη πολυωνυμικού ντετερμινιστικού χρόνου που το επιλύει.

Για καλύτερη κατανόηση δίνεται ένα παράδειγμα NP προβλήματος: το πρόβλημα του Χαμιλτόνιου Κύκλου (*Hamiltonian Cycle (HC) problem*). Ως δεδομένα εισόδου έχουμε ένα γράφο G , και το ερώτημα είναι αν ο G έχει Χαμιλτόνιο Κύκλο. Για την επίλυση του προβλήματος εισάγεται μια φανταστική, μη πραγματοποιήσιμη εντολή, η οποία καλείται "choose()". Η συμπεριφορά της "choose()" έχει ως εξής:

1. αν το πρόβλημα έχει μια λύση από N στοιχεία, τότε η choose(i) επιστρέφει το i -στο στοιχείο της σωστής λύσης σε σταθερό χρόνο.
2. αν το πρόβλημα δεν έχει λύση, τότε η choose(i) επιστρέφει απλώς άχρηστα πράγματα, δηλαδή μια αβέβαιη τιμή.

Ένας NP αλγόριθμος έχει δύο στάδια:

1. Το πρώτο στάδιο είναι ένα στάδιο αναζήτησης που χρησιμοποιεί την "choose()" για να βρεθεί μια λύση του προβλήματος.

2. Το δεύτερο στάδιο ελέγχει την ορθότητα της λύσης που παράγεται από το πρώτο στάδιο. Ο χρόνος σε αυτό το στάδιο είναι πολυωνυμικός στο μέγεθος των δεδομένων εισόδου n .

Δίνεται παρακάτω ένας NP αλγόριθμος για το HC πρόβλημα.

```
begin
  /* Πρώτο στάδιο */
  for i=1 to n do
    X[i] := choose(i);
  endfor

  /* Δεύτερο στάδιο */
  for i=1 to n do
    for j=i+1 to n do
      if X[i] = X[j] then
        return(no);
      endif
    endfor
  endfor
  for i=1 to n-1 do
    if (X[i],X[i+1]) is not an edge then
      return(no);
    endif
  endfor
  if (X[n],X[1]) is not an edge then
    return(no);
  endif

  return(yes);
end
```

Η λύση του HC προβλήματος είναι $O(n)$, και ο χρόνος του δεύτερου σταδίου είναι $O(n^2)$. Γι' αυτόν το λόγο το πρόβλημα HC είναι NP.

4.4.2 NP-πληρότητα

Μετά τους ορισμούς των NP προβλημάτων θα δοθεί και ο ορισμός του NP-πλήρες προβλήματος.

Ορισμός

Ένα πρόβλημα R είναι NP πλήρες αν κατά πρώτον το R είναι NP και κατά δεύτερον αν κάθε NP πρόβλημα P μετασχηματίζεται σε πολυωνυμικό χρόνο στο R.

Με απλά λόγια θα μπορούσε να πει κανείς ότι ένα πρόβλημα R είναι NP πλήρες αν το R είναι το πιο δύσκολο από όλα τα NP προβλήματα. Δίνονται στη συνέχεια τρία γνωστά θεωρήματα και τα συμπεράσματά τους:

Θεώρημα 1

Έστω P και R να είναι δύο προβλήματα. Αν το P μετασχηματίζεται στο R και το R είναι πολυωνυμικού χρόνου επίλυσης, τότε και το P είναι πολυωνυμικού χρόνου επίλυσης.

Το συμπέρασμα που εξάγεται είναι ότι αν ένα πρόβλημα P καταλήγει σε ένα πρόβλημα R , τότε το R είναι τουλάχιστον τόσο δύσκολο όσο και το P .

Θεώρημα 2

Ένα πρόβλημα R είναι NP πλήρες, αν το R είναι NP και αν υπάρχει ένα NP πλήρες πρόβλημα R_0 που καταλήγει στο R .

Αυτό το θεώρημα δηλώνει κατά βάση τη στρατηγική που ακολουθείται για να αποδειχθεί ότι ένα πρόβλημα είναι NP πλήρες. Δηλαδή τα βήματα που ακολουθούνται για να αποδειχθεί ότι ένα πρόβλημα R είναι NP πλήρες είναι:

1. Αποδεικνύεται ότι το R είναι NP
2. Βρίσκεται ένα ήδη γνωστό NP πλήρες πρόβλημα R_0 το οποίο με κάποιον πολυωνυμικό μετασχηματισμό καταλήγει στο R .

Για να είναι αποτελεσματική αυτή η στρατηγική απαιτείται τουλάχιστον ένα ήδη γνωστό NP πλήρες πρόβλημα. Αυτό παρέχεται από το θεώρημα του Cook [Pap1994].

Θεώρημα 3 (Cook)

Το SAT είναι ένα NP πλήρες πρόβλημα.

Στην προτεινόμενη μέθοδο εκμεταλλευόμαστε το NP-πλήρες πρόβλημα του χρωματισμού ενός ήδη δημιουργημένου γράφου με τρία χρώματα γράφου. Για αύξηση της πολυπλοκότητας του προβλήματος επιλέγεται γράφος με λόγο ακμών

προς κορυφών κοντά στην τιμή 2.3, όπου είναι η περιοχή των φαινομένων κατωφλίου των συνδυαστικών προβλημάτων.

4.5. Παραγωγή τυχαίων στιγμιότυπων του προβλήματος 3-χρωματισμού γράφων

Ένας γράφος $G=(V,E)$, όπου V είναι το σύνολο των κορυφών και E είναι το σύνολο των ακμών του γράφου G , είναι τρία χρωματίσιμος αν οι κορυφές του μπορούν να χρωματιστούν το πολύ με τρία χρώματα έτσι ώστε δύο γειτονικές κορυφές να μην έχουν χρωματιστεί με το ίδιο χρώμα. Η ανάθεση χρωμάτων που γίνεται σεβόμενη αυτόν τον περιορισμό ονομάζεται τρία-χρωματισμός του G .

Ενώ ο χρωματισμός με τρία χρώματα ενός ήδη δημιουργημένου γράφου ανάγεται στα υπολογιστικά δύσκολα επιλύσιμα προβλήματα (*computationally intractable problems*) ή στα προβλήματα μη ντετερμινιστικού χρόνου επίλυσης (*NP - complete problems*) ([Pap1994, Gar1979]), αντίθετα η κατασκευή των γράφων μαζί με το χρωματισμό τους είναι ιδιαίτερα απλή. Ο αλγόριθμος που ακολουθεί περιγράφει την κατασκευή τους:

1. Έστω p_1, p_2 , και p_3 τρεις πραγματικοί αριθμοί, τέτοιοι ώστε $p_1 + p_2 + p_3 = 1$ και $p_1 \cdot p_2 \cdot p_3 \neq 0$.
2. Δημιουργούμε μια τυχαία μετάθεση (*permutation*) $i_1, i_2, \dots, i_n$ των αριθμών $1, 2, \dots, n$.
3. Για κάθε $j=1, \dots, n$, μια κορυφή v_j γίνεται ανάθεση στην κλάση χρώματος C_k με πιθανότητα p_k , όπου $k=1, 2, 3$.
4. Για κάθε ζεύγος των u, v των κορυφών που δεν ανήκουν στην ίδια κλάση χρώματος εισάγεται μια μη κατευθυνόμενη (*undirected*) ακμή (u, v) με πιθανότητα p .

Για κάθε τιμή της πιθανότητας p , ο παραπάνω αλγόριθμος παράγει εγγυημένα ένα επιλύσιμο στιγμιότυπο του προβλήματος των τριών χρωμάτων με αναμενόμενο μέγεθος των κλάσεων χρωμάτων $|C_1|=p_1 \cdot n$, $|C_2|=p_2 \cdot n$ και

$|C_3| = p_3 \cdot n$. Ο παραπάνω αλγόριθμος παρέχει και τον τρία χρωματίσιμο γράφο και το χρωματισμό των κορυφών του. Ωστόσο, κάτι τέτοιο δεν είναι αρκετό. Στην πραγματικότητα εκείνο που χρειάζεται είναι ένας γράφος του οποίου όμως ο χρωματισμός είναι δύσκολο να βρεθεί. Με άλλα λόγια απαιτείται ένα δύσκολο στιγμιότυπο που προβλήματος του χρωματισμού με τρία χρώματα. Γενικά, το πρόβλημα του χαρακτηρισμού των δύσκολων στιγμιότυπων των υπολογιστικά δύσκολων (*intractable*) προβλημάτων οδήγησε στην ανάπτυξη μιας πλούσιας θεωρίας, της θεωρίας πολυπλοκότητας στιγμιότυπων (*instance complexity*), η οποία συνδέεται με τη θεωρία της *descriptive* ή *Kolmogorov complexity*.

Παρόλο που οι μέχρι στιγμής θεωρίες δεν προσφέρουν έναν αποδοτικό τρόπο για τη δημιουργία ή ακόμα και για την αναγνώριση δύσκολων στιγμιότυπων των υπολογιστικά δύσκολων προβλημάτων, ωστόσο υπάρχει ένας αριθμός ευριστικών προσεγγίσεων, που θα μπορούσε κανείς να ακολουθήσει για να παράγει τέτοια στιγμιότυπα με υψηλή πιθανότητα να είναι δύσκολα. Μια ενδιαφέρουσα πιθανότητα για τη δημιουργία τέτοιων στιγμιότυπων προέρχεται από την ερευνητική περιοχή των φαινομένων κατωφλίου (*threshold phenomena*) των συνδυαστικών προβλημάτων (*combinatorial problems*) [Coo1997, Hay1997, Kir1994].

Αν G είναι ένας τυχαίος γράφος με m ακμές και n κορυφές τότε ως r ορίζεται ο λόγος m/n . Στις δουλειές των Cheeseman, Kanefsky και Taylor [Che1991] αποδεικνύεται πειραματικά ότι για τιμές του r κοντά στην τιμή 2.3, οι γράφοι που έχουν δημιουργηθεί τυχαία είναι είτε σχεδόν όλοι τρία χρωματίσιμοι, είτε σχεδόν κανένας τρία χρωματίσιμος, εξαρτώμενοι από αν το r είναι λίγο μικρότερο, είτε λίγο μεγαλύτερο από την τιμή 2.3 αντίστοιχα ($r < 2.3$ ή $r > 2.3$). Αυτό σημαίνει ότι υπάρχει μια συγκεκριμένη τιμή r_0 της μεταβλητής r στην οποία μπορεί να παρατηρηθεί απότομη μεταβολή από την κατάσταση της απόλυτης βεβαιότητας για την ύπαρξη ενός τρία χρωματίσιμου γράφου στην κατάσταση της απόλυτης βεβαιότητας για τη μη ύπαρξη του χρωματισμού ενός τυχαίου γράφου. Από την άποψη της θεωρίας της πολυπλοκότητας η ύπαρξη ενός γράφου με λόγο ακμών προς κορυφών ίσο προς r_0 είναι μια κρίσιμη παρατήρηση και παρέχει τη μεγαλύτερη δυσκολία ως προς το χρωματισμό του.

Επιστρέφοντας στον αλγόριθμο που παράγει τρία χρωματίσιμα στιγμιότυπα, η επιλογή της πιθανότητας p θα μπορούσε να στηριχθεί στο γεγονός ότι μέση τιμή

(expected ratio) $E[r]$, η οποία ισούται με $E[m]/n$, να είναι ίση προς r_o . Έτσι, θεωρώντας ότι $|C_k| = p_i \cdot n$, με $k=1,2,3$, η πιθανότητα p εξάγεται ως εξής:

$$r_o = E[r] = \frac{E[m]}{n} = p \cdot (p_1 \cdot p_2 + p_1 \cdot p_3 + p_2 \cdot p_3) \cdot n.$$

Από όπου προκύπτει ότι $p = \frac{r_o}{(p_1 \cdot p_2 + p_1 \cdot p_3 + p_2 \cdot p_3) \cdot n}$. Είναι πειραματικά παρατηρημένο ότι τα στιγμιότυπα είναι πιο δύσκολα να επιλυθούν όταν όλες οι κλάσεις χρωμάτων είναι περίπου ίσες $p_1 = p_2 = p_3 = 1/3$ γεγονός που συνεπάγεται ότι $p = 3 \cdot r_o / n$. Με αυτόν τον τρόπο είναι αντιπροσωπευτική η περιοχή δύσκολων στιγμιότυπων (*hard instances*).

Δεν είναι ωστόσο ξεκάθαρο αν ένα τέτοιο αντιπροσωπευτικό δείγμα περιέχει πολλούς χρωματισμούς εκτός από αυτόν που παράγεται από τον προτεινόμενο αλγόριθμο. Κάτι τέτοιο θα είχε μια μεγάλη ανεπιθύμητη συνέπεια, θα έδινε δηλαδή στον ανταγωνιστή που θα έκλεβε τον γράφο, το πλεονέκτημα να ανακαλύψει έναν από αυτούς τους χρωματισμούς και έτσι να χρησιμοποιεί το γράφο σαν δική του υπογραφή. Παρόμοιοι συλλογισμοί για το πρόβλημα ικανοποιησιμότητας λογικών τύπων με τρία λεκτικά ανά όρο (*satisfiability problem with clauses of 3 literals, 3-SAT*) εκφράζονται στο [Ach2000]. Το πρόβλημα που παρουσιάζεται εκεί είναι η δημιουργία τυχαίων υποδειγμάτων με λόγο όρων προς μεταβλητές (*clauses to variables*) γύρω στην τιμή κατωφλίου, που κατασκευάζονται έτσι ώστε να ικανοποιούν μια δεδομένη αληθή ανάθεση (*assignment*) (παρόμοια με την κατασκευή ενός τρία-χρωματίσιμου γράφου). Το πρόβλημα είναι ότι η προφανής μέθοδος για να επιτύχει την παραγωγή υποδειγμάτων, εκτός από την επιθυμητή ανάθεση (*assignment*) ικανοποιεί ταυτόχρονα και πολλές άλλες αναθέσεις. Κάτι τέτοιο θα μπορούσε να έχει την αντίθετη επίδραση, τέτοια ώστε να έχουμε παραγωγή υποδειγμάτων όπως του αλγόριθμου επίλυσης Walksat, που είναι πολύ πιο εύκολα να λυθούν από τα προκείμενα υποδείγματα (*satisfiable*) που έχουν ξεχωριστεί από όλα τα υποδείγματα που παράγονται ομοιόμορφα (*uniformly*) στις τιμές κατωφλίων από τη 3-SAT γεννήτρια υποδειγμάτων.

Μια άλλη ευρετική προσέγγιση που μπορεί να υιοθετηθεί για να ενισχύσει τα στιγμιότυπα έναντι αυτής της ανεπάρκειας είναι η διαβεβαίωση ότι εκτός της λύσης που επιβάλλεται στα στιγμιότυπα, δεν υπάρχει άλλη λύση (ή υπάρχουν πολύ λίγες).

Τέτοια προσέγγιση ακολουθείται στο [Mot1999] για το πρόβλημα 3-SAT, όπου δεικνύεται ότι αν επιλεγόντουσαν ικανοποιητικά πολλοί όροι (*clauses*) τυχαία από τους όρους που ικανοποιούν την αληθή ανάθεση (*assignment*), τότε ο λογικός τύπος που θα παράγεται κατέχει μια μοναδική λύση με πιθανότητα $1 - O(1)$ (βλέπε [Mot1999]). Εξαιτίας του αυξανόμενου αριθμού των πιθανών τιμών ανά μεταβλητή για τρία χρωματισμό (3 τιμές έναντι 2 στο 2-SAT), η τεχνική των [Mot1999] δεν μπορεί να γενικευτεί κατευθείαν και στην τωρινή περίπτωση. Είναι δυνατόν ωστόσο να ισχυριστεί κανείς ότι ένας αριθμός ειδικών χρωματισμών εξαιρούνται από τους νόμιμους χρωματισμούς μετά από την κατασκευή τους με βάση τον προηγούμενο αλγόριθμο: οι χρωματισμοί που εξαιρούνται είναι αυτοί που παράγονται από προηγούμενο χρωματισμό με αλλαγή ενός χρώματος σε άλλο χρώμα υψηλότερου δείκτη. Έτσι, υποθέτοντας ότι τα χρώματα έχουν αριθμηθεί ως 0, 1 και 2, οι χρωματισμοί που εξαιρούνται είναι αυτοί που παράγονται από άλλους χρωματισμούς με αλλαγή του χρώματος των κορυφών σε ένα «μεγαλύτερου δείκτη» χρώμα. Σαφώς, ένας χρωματισμός P είναι ένας διαμερισμός του συνόλου κορυφών V σε τρία σύνολα κορυφών V_0 , V_1 και V_2 έτσι ώστε να μην υπάρχει ακμή που να ενώνει δύο κορυφές του ίδιου υποσυνόλου. Μια κορυφή u χρώματος i είναι σταθερή (*unmovable*) σε κάθε αλλαγή χρώματος j (όπου $j \neq i$) που ακυρώνει τον χρωματισμό P . Έτσι, η u του χρώματος i είναι *αμετακίνητη* αν είναι παρακείμενη (*adjacent*) με τουλάχιστον μια κορυφή ενός συνόλου V_j , έτσι ώστε $j \neq i$. Ένας χρωματισμός P είναι *αυστηρός* και *δύσκαμπτος* (*rigid*) αν όλες οι κορυφές είναι αμετακίνητες. Μια καλή σκέψη θα ήταν να αρχίσει κανείς το χρωματισμό έτσι ώστε να υπάρχει μεγάλη πιθανότητα αυτός να είναι *αυστηρός* και *δύσκαμπτος*. Στο [Kar2000] η πιθανότητα να είναι ο χρωματισμός P *αυστηρός* και *δύσκαμπτος* υπολογίζεται δεδομένων (i) των κλασμάτων x , y , z των δεδομένων ακμών που ενώνουν κορυφές από V_0V_1 , V_0V_2 και V_1V_2 αντίστοιχα, και (ii) των κλασμάτων α , β , γ των κορυφών που αποδίδουν τα χρώματα 0, 1, και 2 αντίστοιχα.

$$P[P \text{ είναι δύσκαμπτος δεδομένων } x, y, z, \alpha, \beta, \gamma] \sim$$

$$\left[e^{-\alpha \left(\int_0^1 \ln \left(\frac{u_{12}-x}{1-x} \right) dx - c_{12} \ln u_{12} \right) - \alpha \left(\int_0^1 \ln \left(\frac{u_{13}-x}{1-x} \right) dx - c_{13} \ln u_{13} \right) - \beta \left(\int_0^1 \ln \left(\frac{u_{23}-x}{1-x} \right) dx - c_{23} \ln u_{23} \right)} \right]^n$$

με

$$u_{12} = \frac{1}{1 - e^{-c_{12}} \phi_2(c_{12} e^{-c_{12}})}, \quad c_{12} = \frac{xr}{\alpha}$$

$$u_{13} = \frac{1}{1 - e^{-c_{13}} \phi_2(c_{13} e^{-c_{13}})}, \quad c_{13} = \frac{yr}{\alpha}$$

$$u_{23} = \frac{1}{1 - e^{-c_{23}} \phi_2(c_{23} e^{-c_{23}})}, \quad c_{23} = \frac{(1-x-y)r}{\beta}$$

όπου $\phi_2(t)$ είναι η μικρότερη ρίζα της εξίσωσης $\phi_2(t) = e^{t\phi_2(t)}$. Αυτή η ρίζα μπορεί να εκφραστεί χρησιμοποιώντας τη συνάρτηση *Lambert W* (βλέπε [Cor1996]). Το σύμβολο " $\sim$ " σημαίνει ότι οι πολυωνυμικά μεγάλοι συντελεστές μπορούν να αγνοηθούν (όπως μπορεί εύκολα να υπολογιστεί από την προσέγγιση Stirling). Ευριστικά οι τιμές των $x, y, z, \alpha, \beta, \gamma$ μπορούν να ρυθμιστούν έτσι ώστε να αυξήσουν την προσέγγιση που δίνεται παραπάνω. Να σημειωθεί εδώ ότι οι παράγοντες α, β , και γ που εισάγονται στην εκτίμηση της πιθανότητας οδηγούν στο συμπέρασμα ότι ο τύπος του αρχικού χρωματισμού έχει επίδραση στην πιθανότητα να είναι *παράνομοι* άλλοι "γειτονικοί" χρωματισμοί.

Από την άλλη μεριά, υπάρχει ένας κοινότυπος τρόπος για να αποκλείονται πολλές πιθανές λύσεις απλά προσθέτοντας μεγάλο αριθμό ακμών στον παραγόμενο γράφο με τον αλγόριθμο που περιγράφηκε παραπάνω (ακόμα και φτιάχνοντας έναν πλήρη τριμερή (*3-partite*) γράφο). Το μειονέκτημα αυτής της προσέγγισης είναι ότι τα στιγμιότυπα με πάρα *πολύ λίγες* (δηλαδή $o(n)$) ή *πάρα πολλές* (δηλαδή $\omega(n)$) ακμές επιλύονται πολύ εύκολα. Χωρίς να διεξάγουμε εξαντλητική έρευνα με αυστηρά επιχειρήματα, η πρώτη απλή διαδικασία παρέχει πάρα πολλούς χρωματισμούς, ενώ στην τελευταία, υπάρχει ένας απλός αλγόριθμος τυχαιότητας που βασίζεται σε τυχαία δειγματοληψία και που χρωματίζει γράφους, οι οποίοι ονομάζονται *πυκνοί* (*dense*) γράφοι. Αυτοί οι γράφοι χαρακτηρίζονται από κάθε κορυφή έχοντας $\theta(n)$ γείτονες.

Μια άλλη, πιο αυστηρή και πιο ενδιαφέρουσα προσέγγιση είναι η κατασκευή μια βεβαίας (*certain*) τυχαίας κλάσης λυμένων 3-χρωματίσιμων στιγμιότυπων με την ακόλουθη ιδιότητα: αν βρεθεί αλγόριθμος ικανός να λύνει στιγμιότυπα των κλάσεων με θετική (οσοδήποτε μικρή) πιθανότητα, τότε υπάρχει επίσης και αλγόριθμος που επιλύει ένα από τα μη ντετερμινιστικού χρόνου προβλήματα (*NP - complete problems*) στη χειρότερή τους περίπτωση, πράγμα μη αναμενόμενο. Στο [Ajt1996], ο στόχος που επιτεύχθηκε ήταν ακριβώς αυτός, για την ιδιαίτερη κλάση των προβλημάτων πλέγματος (*lattice problems*).

Εκείνο που θα πρέπει να τονιστεί είναι ότι η περιοχή της δημιουργίας λυμένων δύσκολων στιγμιότυπων είναι ενεργή και διεξάγεται πολλή έρευνα που σκοπεύει στη δημιουργία στιγμιότυπων με *περιορισμένο* αριθμό λύσεων.

4.6. Διαντιδραστικές αποδείξεις μηδενικής γνώσης για 3-χρωματισμό

Αυτή η ενότητα περιγράφει τις γνωστές Διαντιδραστικές Αποδείξεις Μηδενικής Γνώσης (*Zero Knowledge Interactive Proof protocol - ZKIP*) για τη γνώση του τρία χρωματισμού ενός 3-χρωματίσιμου γράφου. Το ZKIP έχει την ιδιότητα του να μπορεί κανείς να παρέχει απόδειξη γνώσης της ιδιότητας ενός αντικειμένου (π.χ. ο 3-χρωματισμός ενός γράφου) χωρίς να χρειάζεται να αποκαλύψει καμιά πληροφορία γι' αυτό.

Ας θεωρήσουμε ότι A είναι το πρόσωπο εκείνο που γνωρίζει τον 3-χρωματισμό των κορυφών ενός γράφου $G=(V,E)$ και B είναι το πρόσωπο εκείνο που ισχυρίζεται ότι γνωρίζει τον 3-χρωματισμό όπως ο A . Για ευκολία συμβολίζουμε τα τρία χρώματα με τα ακόλουθα δυαδικά ψηφία 00, 11, και 01. Για κάποια κορυφή $v \in V$, το χρώμα της θα συμβολίζεται με $C(v)=b_1b_0$, όπου b_1 και b_0 είναι είτε το 0 είτε το 1.

Το ZKIP πρωτόκολλο περιλαμβάνει έναν αριθμό από γύρους. Σε κάθε γύρο λαμβάνουν χώρα τα επόμενα βήματα (βλέπε για παράδειγμα [Pap1994]):

1. Ο A παράγει μια τυχαία μετάθεση (*permutation*) των τριών χρωμάτων. Έτσι το χρώμα κάθε κορυφής αλλάζει σύμφωνα με τη μετάθεση αυτή.
2. Μετά ο A παράγει το $|V|$ RSA κρυπτοσυστήματα, ένα για κάθε κορυφή v . Το i -στο κρυπτοσύστημα, για την κορυφή v_i , αποτελείται από τα

στοιχεία (p_i, q_i, d_i, e_i) όπου p_i, q_i είναι δύο μεγάλοι *πρώτοι* αριθμοί (οι οποίοι μπορούν να δημιουργηθούν εύκολα χρησιμοποιώντας έναν γρήγορο πιθανοτικό αλγόριθμο για έλεγχο πρώτων αριθμών, όπως αυτός των Miller-Rabin), d_i είναι εμπιστευτικό κλειδί αποκωδικοποίησης και e_i είναι το δημόσιο διαθέσιμο κλειδί κωδικοποίησης (το οποίο μπορεί να παραχθεί εύκολα από τον Ευκλείδειο αλγόριθμο για εύρεση του μεγαλύτερου κοινού διαιρέτη δύο αριθμών).

- Μετά, για κάθε κορυφή v_i ο A πιθανοτικά κωδικοποιεί ένα νέο χρώμα $C'(v_i)$ του v_i . Υποθέτοντας ότι $C'(v_i) = b'_1 b'_0$, υπάρχουν δύο δυαδικά ψηφία b'_1, b'_0 που αναπαριστούν το νέο χρώμα. Τότε ακολουθούν δύο λειτουργίες, όπου $n_i = p_i q_i$ και x_i, x'_i είναι δύο τυχαίοι ακέραιοι, όχι μεγαλύτεροι από $n_i/2$ (οι λειτουργίες που ακολουθούν πραγματοποιούνται εύκολα από την επαναλαμβανόμενη τεχνική τετραγώνου (*repeated squaring technique*)):

$$y_i = (2x_i + b_i)^{e_i} \bmod n_i$$

$$y'_i = (2x'_i + b'_i)^{e_i} \bmod n_i$$

- Τέλος, ο A αποκαλύπτει στον B όλο το σύνολο (y_i, y'_i, n_i, e_i) για την κορυφή v_i .
- Ο B επιλέγει τυχαία μια ακμή που συνδέει τις δύο κορυφές v_i, v_j . Στη συνέχεια ο A αποκαλύπτει τα μυστικά κλειδιά d_i και d'_i που χρησιμοποιήθηκαν κατά την κωδικοποίηση του RSA συστήματος για την κωδικοποίηση των χρωμάτων των αντίστοιχων κορυφών. Ο B αποκωδικοποιεί το κωδικοποιημένο χρώμα ως εξής

$$b_i = (y_i^{d_i} \bmod n_i) \bmod 2$$

και παρόμοια για τα b'_i, b_j, b'_j , και ελέγχει ότι τα χρώματα είναι διαφορετικά.

- Τα παραπάνω βήματα επαναλαμβάνονται $k|E|$ φορές όπου το k αναπαριστά την *αξιοπιστία* (*reliability*) του πρωτοκόλλου.

Θα πρέπει δηλαδή κάθε φορά μέσω του πρωτοκόλλου να εμφανίζονται πάντα δύο γειτονικές κορυφές με διαφορετικό χρώμα. Αν τώρα ο A δεν κατέχει πράγματι τον τρία χρωματισμό, τότε υπάρχει μια μη μηδενική πιθανότητα ο A να «πιαστεί» σε κάποιο βήμα. Μετά την εκτέλεση των ανεξάρτητων $k|E|$ γύρων αυτή η πιθανότητα είναι τουλάχιστον

$$1 - \left(1 - \frac{1}{|E|}\right)^{k|E|} \geq 1 - e^{-\frac{1}{|E|}k|E|} = 1 - e^{-k}$$

Η τελευταία έκφραση προσεγγίζει εκθετικά ως προς k τη μονάδα (1), βεβαιώνοντας έτσι ότι σίγουρα ο A θα φανερωθεί, αν ψεύδεται, ύστερα από έναν αριθμό γύρων του ZKIP πρωτοκόλλου. Το σημαντικό χαρακτηριστικό του ZKIP πρωτοκόλλου, όπως εμφανίζεται πιο πάνω, δεν είναι μόνο ότι παρέχει ισχυρές αποδείξεις για τη γνώση του χρωματισμού, αλλά με τη μετάθεση (*permuting*) και την κωδικοποίηση (*encrypting*) των χρωμάτων, εκμηδενίζει ουσιαστικά τη γνώση του B για το χρωματισμό. Σε κάθε γύρο, δίνεται στον B μόνο ό,τι είναι προφανές: στον τρία χρωματισμό του γράφου οι κορυφές σε κάθε ακμή είναι χρωματισμένες διαφορετικά (χωρίς ο B να μπορεί να βγάλει συμπέρασμα για τα χρώματα των κορυφών). Αυτό δίνει τη δυνατότητα στον A να χρησιμοποιήσει την υπογραφή του πολλές φορές εφόσον δεν αποκαλύπτει καμιά πληροφορία για αυτήν.

4.7. Αναγνώριση του νόμιμου κατόχου

Η εφαρμογή του πολύ γνωστού πρωτοκόλλου διαντιδραστικών αποδείξεων μηδενικής γνώσης (*zero-knowledge interactive protocol*) [Pap1994] για τον τρία χρωματισμό, με σκοπό την υπογραφή μιας δημιουργίας και την εξακρίβωση του κατόχου περιλαμβάνει τρία μέρη:

- Τον κάτοχο A της αρχικής εικόνας.
- Το άτομο B που επιχειρεί και ισχυρίζεται λανθασμένα ότι η εικόνα είναι δική του.
- Τον κριτή C .

Το πρωτόκολλο που περιγράφεται εδώ είναι μηδενικής γνώσης, αναφορικά με την αποκάλυψη της υπογραφής στον κριτή, και παρέχει απόδειξη της γνησιότητας του κατόχου. Ο κάτοχος, A , ενθέτει έναν αρκετά μεγάλο και δύσκολα επιλύσιμο τρία-χρωματίσιμο γράφο στην αρχική εικόνα I (όπου ο γράφος παράγεται όπως περιγράφεται στην προηγούμενη ενότητα και εντίθεται με τεχνική που θα περιγραφεί στην επόμενη ενότητα). Στην ουσία εκείνο που ενθέτει ο A είναι ο πίνακας γειτνίασης του γράφου, ο οποίος για έναν μη κατευθυνόμενο γράφο χωρίς βρόχους ακμών απαιτεί $n \cdot (n-1)/2$ bits. Συμβολίζοντας την παραγόμενη εικόνα με I' , τότε αυτή είναι η εικόνα που ο κάτοχος A θα δημοσιεύσει για παράδειγμα στο Διαδίκτυο. Ας υποθέσουμε τώρα ότι ο B κατεβάζει (*downloads*) την I' και ισχυρίζεται τη νόμιμη κατοχή. Τότε ο A πείθει τον κριτή C ότι αυτός είναι ο κάτοχος ως ακολούθως:

1. Ο A ισχυρίζεται στον C ότι υπάρχει ένα σετ δυαδικών ψηφίων στην εικόνα του B (δηλαδή στην I'), που αναπαριστούν τον πίνακα γειτνίασης ενός γράφου για τον οποίο γνωρίζει τον τρία χρωματισμό του.
2. Ο A δίνει στον C τη μέθοδο να εξαγάγει από τις θέσεις τους τα δυαδικά ψηφία του πίνακα γειτνίασης και ο A με τον C αρχίζουν να εκτελούν πρωτόκολλο μηδενικής γνώσης για τον τρία χρωματισμό του γράφου.

Αν τώρα ο B ισχυριστεί και αυτός ότι είναι ο νόμιμος κάτοχος της εικόνας, τότε ο A τον προκαλεί να του δείξει την υπογραφή του στην αρχική εικόνα I λέγοντας στον κριτή τις θέσεις των δυαδικών ψηφίων της δικής του υπογραφής (η I δεν έχει αποκαλυφθεί στον B). Η I είναι η αρχική εικόνα, την οποία μόνο ο A κατέχει, ενώ δημοσιεύει μόνο την υδατογραφημένη εικόνα I' . Κάτι τέτοιο όμως είναι απίθανο, να φανεί δηλαδή η υπογραφή του B στην I , και έτσι αυτός ισχυρίζεται ότι ο A έχει καταφέρει και έχει αφαιρέσει εντελώς τη δική του υπογραφή. Έτσι ο κριτής συμπεραίνει ένα από τα ακόλουθα:

1. Ο B λέει την αλήθεια και ο A , και εκτός από την υποθετική καταστροφή της υπογραφής του B στην εικόνα I , έχει επίσης καταφέρει να ανακαλύψει μια ακολουθία δυαδικών ψηφίων στην I' (την "αρχική" του B) που αντιπροσωπεύει τον πίνακα γειτνίασης ενός γράφου, για τον οποίο ο A γνωρίζει τον 3-χρωματισμό του, πριν την εκτέλεση του πρωτοκόλλου.

2. Ο A λέει την αλήθεια, έχοντας δείξει μια υπολογιστικά δύσκολη ιδιότητα μιας ακολουθίας δυαδικών ψηφίων που έχουν ενθεθεί I , και ο B δεν κατάφερε να καταστρέψει αυτή την υπογραφή.

Το πρώτο συμπέρασμα, αν ήταν αληθινό, θα οδηγούσε τον κριτή στο συμπέρασμα ότι η επίδειξη του τρία χρωματισμού ενός γράφου είναι ζήτημα απλής τύχης. Ωστόσο, εξαιτίας της δυσκολίας του προβλήματος του τρία χρωματισμού, τα ζητήματα καθαρής τύχης αποκλείονται με πολύ υψηλή πιθανότητα. Γι' αυτόν το λόγο το δεύτερο συμπέρασμα είναι πιο αξιόπιστο από το πρώτο.

4.8. Διαδικασία απόκρυψης δεδομένων

Υπάρχουν τρεις παράγοντες οι οποίοι λαμβάνονται υπόψη συχνά, όταν αναφερόμαστε σε συστήματα σχεδιασμού απόκρυψης δεδομένων:

1. η *χωρητικότητα* (*capacity*) μιας εικόνας ή γενικότερα ενός ψηφιακού αντικειμένου
2. η *ποιότητα* (*quality*) του παραγόμενου προϊόντος (π.χ. της εικόνας) μετά την εισαγωγή της υπογραφής ή του υδατογραφήματος, και
3. η *ανθεκτικότητα* (*robustness*) της μεθόδου.

Αυτοί οι τρεις παράγοντες σχετίζονται μεταξύ τους, όπως φαίνονται στο σχήμα 4.1 που αναφέρεται στο [Lin2000]. Με σταθερόν τον έναν από τους τρεις παράγοντες, φαίνεται η αλληλεξάρτηση που υπάρχει ανάμεσα στους άλλους δύο.

Γενικά, οποιαδήποτε τεχνική απόκρυψης πληροφορίας προκαλεί υποβάθμιση της ποιότητας του αντικειμένου. Αν οι τεχνικές αυτές εφαρμόζονται σε εικόνες, τότε έχουμε οπτική υποβάθμιση της εικόνας, εφόσον πρακτικά αλλάζουν οι τιμές της αρχικής εικόνας, αλλά σκοπός είναι οι αλλαγές αυτές να είναι όσο το δυνατόν μικρότερες, ώστε να μην είναι ορατές. Είναι επομένως σημαντικό να τεθεί μια ελάχιστη τιμή μέτρησης της ποιότητας της εικόνας, ώστε να χρησιμοποιηθεί για την αξιολόγηση της μεθόδου. Η προτεινόμενη μέθοδος σχεδιάστηκε έτσι ώστε να διατηρεί τη τιμή του PSNR (*Peak Signal to Noise Ratio*) μεταξύ της αρχικής και της υδατογραφημένης εικόνας μεγαλύτερη από 39dB. Αυτή η τιμή θεωρείται πολύ

υψηλή συγκριτικά με το μέγεθος της υπογραφής το οποίο στην περίπτωση μας πλησιάζει τα 500 Kbits.

Εικόνα 4.1: Παράγοντες που επιδρούν στην απόκρυψη πληροφορίας

Εφόσον η ποιότητα της υδατογραφημένης εικόνας απαιτείται να είναι σε υψηλά επίπεδα, η χωρητικότητα και η ανθεκτικότητα της μεθόδου είναι οι άλλοι δύο παράγοντες που πρέπει να ληφθούν υπόψη. Στην προτεινόμενη μέθοδο, επιλέχθηκαν κριτήρια σχετικά με την *οπτική αντίληψη*, με σκοπό την αποτίμηση της ποιότητας της τελικής εικόνας ύστερα από την ένθεση μεγάλου ποσοστού δεδομένων στην αρχική εικόνα, καθώς και σχετικά με την ανθεκτικότητα της μεθόδου έναντι συνηθισμένων επιθέσεων.

Ως αρχικές εικόνες στα παρόντα πειράματα επιλέχθηκαν έγχρωμες εικόνες υψηλής ανάλυσης με διαστάσεις 1024×1024 pixels. Αν το μέγεθος της αρχικής εικόνας είναι αρκετά μεγάλο, και μάλιστα της τάξεως που ήδη αναφέρθηκε, τότε το μέγεθος της υπογραφής είναι περίπου 500 Kbits, δηλαδή όσο είναι ένα επίπεδο δυαδικών ψηφίων μετά την πρώτη αποσύνθεση της εικόνας. Για την ένθεση της υπογραφής γίνεται χρήση του *διακριτού μετασχηματισμού wavelet (DWT)*. Ο διακριτός μετασχηματισμός wavelet έχει ένα πλεονέκτημα έναντι άλλων μετασχηματισμών, εξαιτίας της ικανότητας του να αναπαριστά το σήμα στο χρόνο

και τη συχνότητα ταυτόχρονα. Το σήμα περνά μέσα από μια σειρά υπερπερατών φίλτρων για να αναλύσουν τις υψηλές συχνότητες, καθώς και από μια σειρά υποπερατών φίλτρων για να αναλύσουν τις χαμηλές συχνότητες. Εδώ το ρόλο του σήματος έχει η εικόνα, η οποία μπορεί να θεωρηθεί σαν ένα δισδιάστατο σήμα. Εφαρμόζοντας το διακριτό μετασχηματισμό wavelet στην αρχική εικόνα, παράγεται το πρώτο επίπεδο αποσύνθεσης που αποτελείται από τέσσερες υπο-εικόνες. Για την παραγωγή αυτών των υπο-εικόνων εφαρμόζονται υποπερατά (L) και υπερπερατά (H) φίλτρα στις στήλες της εικόνας και μετά στις παραγόμενες γραμμές εφαρμόζονται και πάλι υποπερατά (L) και υπερπερατά (H) φίλτρα. Με αυτόν τον τρόπο οι τρεις υπο-εικόνες LH , HL και HH αντιστοιχούν στις υψηλές συχνότητες των συντελεστών wavelet, ενώ η LL υπο-εικόνα αποτελεί μια εξασθετισμένη έκδοση της αρχικής εικόνας μιας και εμπεριέχει τις χαμηλές συχνότητες. Αυτή η τελευταία υπο-εικόνα θα μπορούσε να αναλυθεί σε επιπλέον επίπεδα, αν κάτι τέτοιο ήταν επιθυμητό [Poi2000]. Θα πρέπει να σημειωθεί ότι το μέγεθος της υπογραφής συνδέεται άμεσα με το μέγεθος του γράφου, το οποίο με τη σειρά του επιλέγεται σύμφωνα με το μέγεθος της αρχικής εικόνας. Έτσι, για μικρές αρχικές εικόνες θα χρησιμοποιηθούν και μικρές υπογραφές, ενώ για μεγάλες εικόνες αναλογικά θα χρησιμοποιηθούν και μεγάλες υπογραφές.

Η κύρια απαίτηση της μεθόδου είναι *επιβίωση* της υπογραφής ακόμα και μετά από πιθανές επιθέσεις που πιθανώς να εφαρμόστηκαν στην υδατογραφημένη εικόνα. Συνεπώς ο τρόπος ένθεσης της υπογραφής θα πρέπει να γίνει έτσι ώστε η υπογραφή να διαφυλάσσεται μαζί με τη σημαντική πληροφορία της εικόνας. Αυτός ο περιορισμός συναντάται σε οποιοδήποτε ανθεκτικό σύστημα απόκρυψης πληροφορίας και μπορεί να πραγματοποιηθεί εφαρμόζοντας *μετασχηματισμό* από το χωρικό πεδίο στο πεδίο συχνοτήτων. Τέτοιοι μετασχηματισμοί είναι ο διακριτός μετασχηματισμός συνημιτόνου (DCT), ο γρήγορος μετασχηματισμός fourier (FFT), ο διακριτός μετασχηματισμός wavelet (DWT), καθώς και άλλοι.

Η πληροφορία της υπογραφής εντίθεται στην LL υπο-εικόνα μετά το πρώτο επίπεδο αποσύνθεσης του διακριτού μετασχηματισμού wavelet, η οποία αποτελεί και την πιο σημαντική ζώνη συχνοτήτων. Οι διαστάσεις αυτής της υπο-εικόνος αντιστοιχούν στο ένα τέταρτο των διαστάσεων της αρχικής εικόνας. Αν, για παράδειγμα, η αρχική εικόνα έχει διαστάσεις 1024×1024 , τότε η LL υπο-εικόνα θα έχει διαστάσεις 512×512 pixels. Η διαδικασία ένθεσης που περιγράφεται στην επόμενη ενότητα αποδεικνύει ότι η πληροφορία ενός δυαδικού ψηφίου σε κάθε

εικονοστοιχείο της LL υπο-εικόνας είναι αρκετά αποδοτικό για την ένθεση ενός μεγάλου 3-χρωματίσιμου γράφου στην ψηφιακή εικόνα.

4.9. Ένθεση τρία-χρωματίσιμου γράφου

Η τεχνική ένθεσης ενός τρία χρωματίσιμου γράφου εφαρμόστηκε σε εικόνες και μπορεί επίσης να εφαρμοστεί και σε άλλα είδη ψηφιακών αντικειμένων, όπως είναι το βίντεο.

Ο μετασχηματισμός wavelet μπορεί να παρέχει πληροφορίες τόσο για τις συχνότητες που έχει ένα σήμα, όσο και για τη χρονική τους διάρκεια, δίνοντας τη χρονο-συχνотική αναπαράσταση του σήματος. Αυτό το είδος μετασχηματισμού παρέχει τη δυνατότητα ένθεσης μεγάλου ποσού πληροφορίας στην υδατογραφημένη εικόνα και επιπλέον επιτυγχάνει την ανθεκτικότητα της μεθόδου σε διάφορους μετασχηματισμούς και εν γένει επιθέσεις.

Ένας τρία-χρωματίσιμος γράφος μπορεί να περιγραφεί από τον *πίνακα γειτνίασης*. Ένας τέτοιος πίνακας περιέχει μηδέν και άσσους, αναπαριστώντας έτσι τη μη ύπαρξη ή την ύπαρξη, αντίστοιχα, ακμών μεταξύ κορυφών του γράφου, και ακριβώς λόγω της δυαδικής του αναπαράστασης μπορεί να αναπαρασταθεί σαν μια ασπρόμαυρη εικόνα. Στην εικόνα 4.2 απεικονίζεται ο πίνακας γειτνίασης του γράφου που χρησιμοποιήθηκε με λόγο ακμών προς κορυφών 2.3, όπου είναι η περιοχή των φαινομένων κατωφλίου των συνδυαστικών προβλημάτων, προσπαθώντας να δημιουργήσουμε ένα δύσκολο επιλύσιμο πρόβλημα, αναφορικά με την εύρεση του χρωματισμού του.

Εικόνα 4.2: Ο γράφος που χρησιμοποιήθηκε (με μορφή εικόνας)

Η πληροφορία του γράφου εντίθεται σε έγχρωμες εικόνες και το μέγεθός του είναι το ένα τέταρτο της αρχικής εικόνας (βλ. σχήμα 4.3). Στο πρώτο στάδιο της διαδικασίας η αρχική εικόνα μετασχηματίζεται από το RGB μοντέλο στο YUV μοντέλο χρωμάτων. Η διαδικασία ένθεσης γίνεται μόνο στο Y επίπεδο, αλλά θα μπορούσε να επεκταθεί και στις άλλες δύο συνιστώσες της χρωμικότητας U και V. Οπότε το επόμενο στάδιο είναι να εφαρμοστεί το πρώτο επίπεδο wavelet ανάλυσης στη συνιστώσα της φωτεινότητας Y, παράγοντας έτσι τέσσερις υπο-εικόνες LL , HL , LH και HH της αρχικής εικόνας. Ο πίνακας γειτνίασης του τρία χρωματίσιμου γράφου απεικονίζεται με τη βοήθεια ενός απλού διπολικού μετασχηματισμού από $\{0,1\}$ σε $\{-1,1\}$. Έχοντας ως στόχο την ανθεκτικότητα του υδατογραφήματος, οι τιμές του πίνακα που παράγονται από τον παραπάνω μετασχηματισμό πολλαπλασιάζονται με ένα παράγοντα ίσο με 25, δίνοντας έτσι άλλη βαρύτητα στις τιμές του πίνακα γειτνίασης. Η τιμή αυτή επιλέχθηκε εμπειρικά, έτσι ώστε και το υδατογράφημα να είναι ανθεκτικό και η ποιότητα της υδατογραφημένης εικόνας να είναι ικανοποιητική. Ο γράφος εντίθεται στην LL υπο-εικόνα της αρχικής εικόνας με βάση τη μαθηματική έκφραση $I' = I + W$, όπου I είναι η αρχική εικόνα, W είναι ο γράφος και I' είναι η τελική, υδατογραφημένη εικόνα.

Εικόνα 4.3: Διαδικασία ένθεσης

Όταν ολοκληρωθεί η διαδικασία ένθεσης στην LL υπο-εικόνα, εφαρμόζεται ο αντίστροφος μετασχηματισμός wavelet ($IDWT$) για να παραχθεί η υδατογραφημένη εικόνα. Στο τέλος αυτή η εικόνα μετασχηματίζεται από το YUV στο RGB μοντέλο χρωμάτων.

4.10. Εξαγωγή του τρία-χρωματίσιμου γράφου

Για την εξαγωγή του γράφου απαιτούνται τόσο η αρχική εικόνα, όσο και η υδατογραφημένη, όπως φαίνεται στο σχήμα 4.4. Αυτές οι εικόνες αρχικά μετασχηματίζονται από το RGB στο YUV μοντέλο χρωμάτων. Όπως ήδη αναφέρθηκε η πληροφορία του γράφου ενυπάρχει στη Y συνιστώσα της υδατογραφημένης εικόνας.

Εικόνα 4.4: Διαδικασία εξαγωγής

Στη συνέχεια εφαρμόζεται ένα επίπεδο του DWT (διακριτού μετασχηματισμού wavelet) στη Υ συνιστώσα της αρχικής, αλλά και της υδατογραφημένης εικόνας. Παράγονται οκτώ υπο-εικόνες (τέσσερις από κάθε εικόνα), από τις οποίες ενδιαφέρον παρουσιάζουν μόνο οι LL υπο-εικόνες. Το επόμενο στάδιο είναι να αφαιρέσουμε τους LL' συντελεστές της υδατογραφημένης εικόνας από τους αντίστοιχους LL συντελεστές της αρχικής εικόνας με σκοπό την εξαγωγή του γράφου. Αν η διαφορά είναι θετική τότε η εξαγόμενη τιμή αντιστοιχίζεται στη μονάδα, ενώ αν το αποτέλεσμα είναι αρνητικό, τότε η εξαγόμενη τιμή αντιστοιχίζεται στο μηδέν.

4.11. Θέματα ποιότητας και αντοχής της μεθόδου

Οποιαδήποτε τεχνική απόκρυψης πληροφορίας εισάγει μια ποσότητα δεδομένων στα αρχικά δεδομένα (π.χ. στην εικόνα). Η ποιότητα της μεθόδου εξαρτάται από την έκταση στην οποία η αρχική εικόνα παραμένει ανέπαφη, και όπως συζητήθηκε σε προηγούμενη ενότητα, η ανθεκτικότητα της μεθόδου με την ποιότητα της υδατογραφημένης εικόνας έχουν μια σχέση ανταλλαγής, δηλαδή είναι πρακτικά αδύνατον να έχουμε και τη μέγιστη ποιότητα τη υδατογραφημένης εικόνας ταυτόχρονα με την καλύτερη ανθεκτικότητα της μεθόδου. Επιτυχημένη θεωρείται η μέθοδος εκείνη που συνεπάγεται τον ελάχιστο αριθμό πιθανών αλλαγών της αρχικής εικόνας. Η έκταση των αλλαγών της αρχικής εικόνας μπορεί να μετρηθεί χρησιμοποιώντας έναν αντικειμενικό τρόπο μέτρησης όπως είναι το PSNR, ή έναν υποκειμενικό τρόπο μέτρησης όπως είναι το Ανθρώπινο Οπτικό Σύστημα (*Human Visual System - HVS*). Ο τελευταίος τρόπος μέτρησης βασίζεται στην αρχή ότι η υδατογραφημένη εικόνα θα πρέπει να φαίνεται παρόμοια με την αρχική σε καθένα μέσο παρατηρητή. Είναι ολοφάνερο ότι η ένθεση μεγάλων γράφων στην αρχική εικόνα θα οδηγεί σε μικρές τιμές μέτρησης του PSNR, ενώ η ένθεση μικρών γράφων θα οδηγεί σε μεγάλες τιμές μέτρησης του PSNR. Στη μέθοδο που παρουσιάζεται εδώ στόχος είναι η επίτευξη υψηλών τιμών PSNR, και πιο συγκεκριμένα μας ενδιαφέρουν τιμές μεγαλύτερες από 39dB. Ένας τέτοιος στόχος είναι δύσκολος να επιτευχθεί, εφόσον ακόμα και μια μεσαίου τύπου συμπίεση JPEG οδηγεί συνήθως σε τιμές PSNR περίπου ίσες με 33dB. Συνεπώς, με σκοπό την επίτευξη των 39dB η διαδικασία ένθεσης σχεδιάστηκε έτσι ώστε να ελαχιστοποιεί τις αλλαγές στην αρχική

εικόνα και το μέγεθος του γράφου επιλέχθηκε έτσι ώστε να ταιριάζει με το μέγεθος της αρχικής εικόνας. Για μια εικόνα 1024×1024 εικονοστοιχείων, παρατηρήθηκε ότι η ένθεση ενός γράφου με πάνω από 500 κορυφές συνεπάγεται τιμές PSNR μεγαλύτερες από 39dB. Ο πίνακας 4.1 εμφανίζει τις μετρήσεις PSNR για έξι εικόνες που χρησιμοποιήθηκαν στα πειράματα.

<i>Εικόνα</i>	<i>PSNR μετρήσεις</i>
House	39.64
Train	39.75
Bridge	39.73
Rose	39.50
Swing	39.51
Saturn V	39.84

Πίνακας 4.1: Έλεγχος ποιότητας βασισμένος σε μετρήσεις PSNR

Αναφορικά με το κριτήριο HVS, δεν παρατηρήθηκαν αλλαγές μεταξύ της αρχικής και της υδατογραφημένης εικόνας από έναν κοινό παρατηρητή σε κανένα από τα πειράματα. Στο σχήμα 4.5, απεικονίζονται η αρχική εικόνα στα αριστερά και η υδατογραφημένη στα δεξιά.

Εικόνα 4.5: Αρχική (αριστερά) και υδατογραφημένη (δεξιά) εικόνα

Η απόδοση μιας μεθόδου απόκρυψης πληροφορίας σχετίζεται με την ανθεκτικότητα της μεθόδου έναντι πιθανών αλλαγών που εφαρμόζονται στην

υδατογραφημένη εικόνα. Τέτοιες αλλαγές, που ονομάζονται *επιθέσεις*, μπορεί να είναι σκόπιμες (με σκοπό την αφαίρεση του υδατογραφήματος) ή άσκοπες (π.χ. JPEG συμπίεση). Είναι φανερό ότι όσο πιο ισχυρές είναι οι επιθέσεις, τόσο λιγότερο ανθεκτικό παραμένει το υδατογράφημα. Συνήθως, μια υπογραφή αναμένεται να είναι ανθεκτική κυρίως σε επιθέσεις οι οποίες δεν επιδρούν στην ποιότητα της εικόνας. Ωστόσο, το αντικείμενο της προτεινόμενης μεθόδου ήταν η ανθεκτικότητα της μεθόδου ακόμα και όταν οι μετρήσεις PSNR είναι χαμηλότερες από 30dB. Με σκοπό τον έλεγχο της ανθεκτικότητας της μεθόδου εφαρμόσαμε τις ακόλουθες επιθέσεις: *θόλωμα εικόνας (blurring)* (για να ελεγχθεί η ανθεκτικότητα της μεθόδου σε επιθέσεις που ενισχύουν τις χαμηλές συχνότητες), *ενίσχυση ακμών εικόνας (sharpening)* (για να ελεγχθεί η ανθεκτικότητα της μεθόδου σε επιθέσεις που ενισχύουν τις υψηλές συχνότητες), συμπίεση JPEG με χρήση διαφορετικών ρυθμών συμπίεσης (50% και 80%) και θόρυβος (πρόσθεση 20% ομοιόμορφου θορύβου - *uniform noise* στην υδατογραφημένη εικόνα). Όπως φαίνεται και στα έξι πειράματα του πίνακα 4.2, οι μετρήσεις PSNR των υδατογραφημένων εικόνων μετά τις επιθέσεις είναι σχετικά χαμηλές. Οι μετρήσεις για το *blurring* είναι πάντα χαμηλότερες από 38dB, για το *sharpen* είναι χαμηλότερες από 33dB, για μεσαία συμπίεση JPEG είναι χαμηλότερες από 37dB, για πολύ μικρή συμπίεση Jpeg είναι χαμηλότερη από 39dB και για πρόσθεση θορύβου είναι χαμηλότερη από 27dB. Στον ομοιόμορφο θόρυβο κατά 20% παρατηρείται ότι επηρεάζεται σημαντικά η ποιότητα της εικόνας.

<i>Εικόνες</i>	<i>Blurring</i>	<i>Sharpen</i>	<i>JPEG medium</i>	<i>JPEG high</i>	<i>Uniform noise</i>
House	36.04	31.31	33.29	38.50	26.57
Train	37.25	32.24	34.47	38.18	26.46
Bridge	36.95	32.32	36.44	39.26	26.49
Rose	36.78	32.09	33.93	38.63	26.54
Swing	36.36	31.63	33.88	38.63	26.41
Saturn V	37.07	32.30	35.51	39.19	26.59

Πίνακας 4.2: Μετρήσεις PSNR (σε dB) μετά από διάφορες επιθέσεις

Μια μέθοδος χαρακτηρίζεται γενικά ανθεκτική απέναντι σε επιθέσεις αν η υπογραφή που εισάγεται μπορεί κατά πρώτον να εξαχθεί από την εικόνα, ακόμα και μετά από επιθέσεις που πιθανώς να έχει δεχθεί, και κατά δεύτερον αν

χρησιμοποιηθεί για να αποδειχθεί η κυριότητα των αρχικών δεδομένων. Ο πίνακας 4.3 παρουσιάζει το επί τοις εκατό ποσοστό του γράφου που έχει ανακτηθεί από κάθε εικόνα μετά από κάθε επίθεση.

<i>Εικόνες</i>	<i>Blurring</i>	<i>Sharpen</i>	<i>JPEG medium</i>	<i>JPEG high</i>	<i>Uniform noise</i>
House	84.12%	85.62%	71.46%	90.02%	65.71%
Train	85.11%	85.77%	79.64%	91.26%	62.92%
Bridge	92.12%	92.76%	78.04%	94.15%	65.26%
Rose	86.76%	88.10%	72.22%	90.20%	65.29%
Swing	85.67%	87.93%	74.60%	90.86%	66.39%
Saturn V	88.49%	90.03%	76.43%	91.42%	63.76%

Πίνακας 4.3: Το % ποσοστό του πίνακα γειτνίασης που επιζεί μετά από επιθέσεις

Θα πρέπει να σημειωθεί ότι στις περιπτώσεις όπως το *blurring*, το *sharpening* και η συμπίεση JPEG, ποσοστό περισσότερο από 70% του γράφου μπορεί να ανακτηθεί, ενώ στις περισσότερες περιπτώσεις το ποσοστό του γράφου που μπορεί να ανακτηθεί είναι περισσότερο από 80%, και μόνο στην περίπτωση της πρόσθεσης θορύβου το ποσοστό ανάκτησης του γράφου είναι πάνω από 60%. Όπως ήδη αναφέρθηκε, αυτή η μέθοδος δε βασίζεται στα δυαδικά ψηφία της υπογραφής για να αποδειχθεί η κυριότητα των αρχικών δεδομένων, αλλά στη γνώση του χρωματισμού του γράφου ή των υπο-γράφων που επιζούν. Να επισημανθεί εδώ ότι ο τρία-χρωματισμός του αρχικού γράφου αποτελεί και τον τρία-χρωματισμό για καθένα από τους υπο-γράφους.

4.12. Συμπεράσματα

Εξαιτίας της εμφάνισης τεχνολογικών μέσων που δύναται να αντιγράψουν και να μεταφέρουν πληροφορία γρήγορα και με πολύ χαμηλό κόστος, δημιουργήθηκε περισσότερο από κάθε άλλη φορά η ανάγκη αποδοτικών μεθόδων ικανών να προστατέψουν τα πνευματικά δικαιώματα ενός έργου που είναι αποθηκευμένο σε ψηφιακή μορφή. Η επιτακτική ανάγκη λύσεων, ικανών να αποδείξουν την νόμιμη κυριότητα των αντικειμένων, γίνεται ακόμα πιο φανερή σε περιπτώσεις φιλονικιών για τα πνευματικά δικαιώματα. Σε αυτό το κεφάλαιο παρουσιάστηκε μια μέθοδος

προστασίας των πνευματικών δικαιωμάτων των αντικειμένων εστιάζοντας (α) στη μετατόπιση του ενδιαφέροντος από *το πώς φαίνονται οι υπογραφές των χρηστών*, σαν ακολουθία δυαδικών ψηφίων, στο *τι αναπαριστούν οι υπογραφές των χρηστών*, και (β) τη χρήση του *μετασχηματισμού wavelet* με σκοπό την ένθεση υπογραφών ώστε να εισάγεται η μικρότερη παραμόρφωση και να διατηρείται η ποιότητα του ψηφιακού αντικειμένου.

Αναφορικά με το πρώτο χαρακτηριστικό, η ακολουθία των δυαδικών ψηφίων της υπογραφής κατασκευάστηκε έτσι ώστε να αναπαριστά στιγμιότυπα από δύσκολα συνδυαστικά προβλήματα. Το πρόβλημα που επιλέχθηκε για να αποδειχθεί η απόδοση της μεθόδου είναι το πρόβλημα του χρωματισμού ενός τρία-χρωματίσιμου γράφου, ενώ η υπογραφή δεν είναι άλλη από τον πίνακα γειτνίασης του γράφου, του οποίου ο χρωματισμός θα αποδείξει την ταυτότητα του νόμιμου κατόχου. Η κατασκευή ενός τυχαίου τρία-χρωματίσιμου γράφου μαζί με τον χρωματισμό των κορυφών του είναι εύκολο, ενώ αντίθετα η *ανακάλυψη* ενός τέτοιου χρωματισμού, όταν ο γράφος είναι ήδη έτοιμος, αποτελεί μια πολύ δύσκολη διαδικασία. Επιπλέον, αν οι γράφοι έχουν κατασκευαστεί μέσα σε μια συγκεκριμένη περιοχή που ορίζεται από μια παράμετρο ελέγχου (όπως είναι ο λόγος ακμών προς κορυφών), τα παραγόμενα στιγμιότυπα αναμένεται να είναι συγκριτικά πολύ δύσκολα στην επίλυση τους, από ότι θα ήταν ο χρωματισμός γράφων ίδιων διαστάσεων που έχουν παράμετρο ελέγχου εκτός της συγκεκριμένης περιοχής. Έτσι, η γνώση και μόνο του χρωματισμού θα μπορεί να χρησιμοποιηθεί σαν αποδεικτικό της νόμιμης κυριότητας.

Κεφάλαιο 5

Μέθοδος υδατογράφησης στο χωρικό πεδίο

5.1. Εισαγωγή

Σε αυτό το κεφάλαιο παρουσιάζεται μια ασφαλής μέθοδος υδατογράφησης, η οποία παρέχει ανθεκτικότητα σε μια ομάδα επιθέσεων. Το υδατογράφημα εντίθεται στο μπλε κανάλι των εικόνων σε συγκεκριμένες θέσεις που εγγυώνται την ελαχιστοποίηση των δυαδικών ψηφίων που τροποποιούνται. Αυτό γίνεται απλά όπου βρεθούν υπάρχουσες ομοιότητες μεταξύ του υδατογραφήματος και των αρχικών δεδομένων. Μετρήσεις ποιότητας και εμπειρικά πειράματα αποδεικνύουν ότι το υδατογράφημα παραμένει αόρατο. Έγιναν πάνω από 500 πειράματα σε αρκετές εικόνες, επιβεβαιώνοντας ότι το υδατογράφημα μπορεί να ανακτηθεί, ακόμα και μετά από πολλαπλές επιθέσεις. Η πιθανότητα για λάθος ανάκτηση του υδατογραφήματος σύμφωνα με αυτή τη μέθοδο είναι πάρα πολύ χαμηλή. Αυτή η χαμηλή πιθανότητα αποδεικνύεται και πειραματικά.

Οι μέθοδοι της ψηφιακής υδατογράφησης εκμεταλλεύονται το γεγονός ότι τα αρχικά δεδομένα εμπεριέχουν ένα ποσό πληροφορίας που δεν επηρεάζει απευθείας

το περιεχόμενο της εικόνας, όπως το αντιλαμβάνεται ένας παρατηρητής. Συνεπώς, τροποποιήσεις αυτής της πληροφορίας δε γίνονται αντιληπτές από έναν απλό παρατηρητή. Ακολουθούνται δύο βασικές κατευθύνσεις: (α) τροποποιήσεις των αρχικών δεδομένων στο συχνοτικό περιεχόμενο (για παράδειγμα [Cox1996]) και (β) τροποποιήσεις των αρχικών δεδομένων στο χωρικό περιεχόμενο ([Arm1999, Kut1997, Nik1996]). Επιπλέον αναφορές δίνονται στο Katzenbeisser et al. [Kat2000] και στο Voyatzis et al. [Voy1998].

Οι περισσότερες τεχνικές υδατογράφησης που εφαρμόζονται στο χωρικό πεδίο βασίζονται σε ιδιότητες του Ανθρώπινου Οπτικού Συστήματος (*Human Visual System - HVS*). Οι Kutter et al. [Kut1997] πρότειναν μια τεχνική που πραγματοποιεί διαμόρφωση πλάτους της μπλε συνιστώσας των εικόνων. Επιπλέον, εμπορικοί οργανισμοί όπως ο Digimarc και η Kodak χρησιμοποιούν τεχνικές υδατογράφησης για την ένθεση επιπλέον πληροφορίας στο μπλε κανάλι για να προστατέψουν τις εικόνες τους.

Σε αυτό το κεφάλαιο παρουσιάζεται μια νέα μέθοδος υδατογράφησης η οποία εκμεταλλεύεται και το HVS, αλλά και τη στατιστική φύση της εικόνας, για να πραγματοποιηθεί η υδατογράφηση. Η ανθεκτικότητα της μεθόδου δοκιμάστηκε με πάνω από 250 εικόνες σε διάφορες επιθέσεις. Αυτή η μέθοδος αξιολογήθηκε με χρήση του μοντέλου των Kutter – Petitcolas [Kut1999]. Έγινε χρήση του λόγου PSNR τόσο για τις αρχικές εικόνες, όσο και για τις υδατογραφημένες.

5.2. Μοντέλο υδατογράφησης

Αυτή η ενότητα περιγράφει το μοντέλο υδατογράφησης που προτείνεται και παρέχει τις θεωρητικές εκτιμήσεις για την ανθεκτικότητα της μεθόδου έναντι σε διάφορες επιθέσεις. Στις επόμενες υποενότητες περιγράφονται η τεχνική υδατογράφησης, η διαδικασία ανάκτησης, καθώς και οι αντίστοιχες πιθανότητες με τις στατιστικές ιδιότητες των ψηφιακών εικόνων.

5.2.1 Διαδικασία υδατογράφησης

Η διαδικασία υδατογράφησης αποτελείται από δύο κύρια βήματα: (α) το βήμα προεπεξεργασίας, για να βρεθούν τα πιο κατάλληλα μέρη μέσα στην εικόνα για την ένθεση των πολλαπλών υδατογραφημάτων και (β) το βήμα της ένθεσής τους στην εικόνα.

Το υδατογράφημα w έχει μήκος $l \in [32, 64]$ bits. Το υδατογράφημα w θα πρέπει να ικανοποιεί τους ακόλουθους περιορισμούς: (i) $|k_1 - k_0| \leq l/8$, όπου k_0 είναι ο αριθμός των εμφανίσεων των μηδενικών του υδατογραφήματος και k_1 είναι ο αριθμός των άσσων, και (ii) δεν επιτρέπεται η συνεχόμενη ακολουθία περισσότερων από 5 μηδενικών ή άσσων στο υδατογράφημα.

Το μπλε κανάλι αποτελείται από οκτώ (8) επίπεδα δυαδικών ψηφίων, αρχίζοντας από το περισσότερο σημαντικό ψηφίο (Επίπεδο 0) στο λιγότερο σημαντικό ψηφίο (Επίπεδο 7). Κάθε επίπεδο αποτελείται από έναν $m \times n$ δυαδικό πίνακα.

Για τις ανάγκες της μεθόδου μας εισάγεται η παράμετρος της *ομοιότητας* (*similarity*) S_m . Η κύρια ιδέα είναι η ένθεση της επιπλέον πληροφορίας στην εικόνα μειώνοντας όσο περισσότερο γίνεται τις πιθανές τροποποιήσεις που προκαλούνται στις τιμές των εικονοστοιχείων. Η παράμετρος S_m αναπαριστά τον αριθμό των δυαδικών ψηφίων που είναι πανομοιότυποι, ύστερα από σύγκριση του υδατογραφήματος w με την ακολουθία των δυαδικών ψηφίων στην αρχική εικόνα με μήκος l .

Παρόλη την απλότητα της μεθόδου είναι αναγκαίο να ορίσουμε ένα *κατώφλι* (*threshold*) t , το οποίο υπολογίζεται από το μήκος του υδατογραφήματος l και την *ομοιότητα* S_m . Το *κατώφλι* θα αναπαριστά τον αριθμό των δυαδικών ψηφίων που πρέπει να μεταβληθούν κάθε φορά που το υδατογράφημα θα εντίθεται σε μια ακολουθία δυαδικών ψηφίων μήκους l στα αρχικά δεδομένα.

Η προεργασία ξεκινάει από την *απόλυτη ομοιότητα*, όπου το *κατώφλι* είναι $t = 0$ και εμπλέκει την αναζήτηση του υδατογραφήματος και στα 8 επίπεδα του μπλε καναλιού της εικόνας για να βρει προϋπάρχοντα υδατογραφήματα. Δεδομένου ότι η εύρεση ενός υδατογραφήματος 64 δυαδικών ψηφίων σε ένα επίπεδο εικόνας ($640 \times 480 = 307.200$ εικονοστοιχεία), πριν από την διαδικασία της υδατογράφησης, είναι εξαιρετικά χαμηλή (όπως θα αποδειχθεί και παρακάτω αυτή η πιθανότητα είναι περίπου $1.7 \cdot 10^{-14}$), αυξάνεται το *κατώφλι* t κατά 1 και επαναλαμβάνεται όλη η διαδικασία αναζήτησης.

Αυτή διαδικασία επαναλαμβάνεται μέχρι να βρεθούν αρκετές θέσεις σε κάθε επίπεδο της εικόνας, όπου η υπογραφή s θα είναι παρόμοια με τις αντίστοιχες δυαδικές ακολουθίες μήκους l . Ο αριθμός των θέσεων ένθεσης είναι $(m \times n) - l + 1$ όπου m και n είναι οι διαστάσεις της εικόνας σε εικονοστοιχεία.

Η διαδικασία ένθεσης εφαρμόζεται και στα 8 επίπεδα του μπλε καναλιού, διαμοιράζοντας τα υδατογραφήματα ανομοιόμορφα και ενθέτοντας λιγότερα υδατογραφήματα στα περισσότερο σημαντικά επίπεδα και περισσότερα στα λιγότερα σημαντικά επίπεδα. Η ανομοιομορφία επιτυγχάνεται με την επιλογή διαφορετικού *κατωφλίου* t ανάμεσα στα επίπεδα. Μικρό t (εμπειρικά $t \leq 16$) επιτρέπει λίγες υποψήφιας θέσεις ένθεσης και μεγάλο t (εμπειρικά $t \geq 22$) επιτρέπει πολλές υποψήφιας θέσεις ένθεσης για το υδατογράφημα.

Αυτή η μέθοδος επιτυγχάνει την αόρατη τροποποίηση της αρχικής εικόνας, εφόσον για κάθε διαφορετικό υδατογράφημα ελέγχεται ο λόγος PSNR ανάμεσα στην αρχική και την υδατογραφημένη εικόνα. Η μέθοδός μας μπορεί να επαναληφθεί πολλές φορές μειώνοντας το *κατώφλι* t , όταν οι μετρήσεις PSNR είναι χαμηλότερες από 33dB. Το PSNR είναι μια παράμετρος μέτρησης του λάθους, και βασίζεται στο άθροισμα των διαφορών των τετραγώνων των αντίστοιχων εικονοστοιχείων των δύο εικόνων. Είναι βέβαια γνωστό ότι η ποιότητα της εικόνας με την ανθεκτικότητα της μεθόδου υδατογράφησης δεν συμβαδίζουν.

5.2.2 Ανάκτηση υδατογραφήματος

Η διαδικασία της ανάκτησης του υδατογραφήματος βασίζεται στον ίδιο συλλογισμό με τη διαδικασία ένθεσης. Ένα κλειδί k που περιλαμβάνει το υδατογράφημα w χρησιμοποιείται για σύγκριση σε κάθε υποψήφια ένθεση. Κάθε επίπεδο του μπλε καναλιού ανιχνεύεται χρησιμοποιώντας το υδατογράφημα w για να βρεθούν παρόμοια υδατογραφήματα με *κατώφλι* t . Η διαδικασία θεωρείται επιτυχής όταν η πιθανότητα για λανθασμένη ανάκτηση ενός αριθμού υδατογραφημάτων είναι μικρότερη από 10^{-6} . Αυτή η τιμή έχει υιοθετηθεί ως κριτήριο ανάκτησης. Πειραματικά αποτελέσματα απέδειξαν ότι τα καλύτερα αποτελέσματα επιτυγχάνονται για t κοντά στην περιοχή του 10.

Στην ιδανική περίπτωση όπου δεν έχουμε τροποποιήσεις στην εικόνα, ο αριθμός των υδατογραφημάτων που ανακτώνται είναι ίσος με τον αριθμό των υδατογραφημάτων που ενθέτονται, αποκλείοντας έτσι πρακτικά την περίπτωση λανθασμένης ανάκτησης.

5.2.3 Αξιολόγηση της μεθόδου

Η βασική μας υπόθεση είναι ότι η πιθανότητα της εύρεσης προϋπαρχόντων x τυχαίων ακολουθιών δυαδικών ψηφίων στην αρχική εικόνα I_o με κατώφλι t είναι φραγμένη, δηλαδή έχει μια ανώτατη τιμή. Βασιζόμενοι σε αυτό το γεγονός, ενθέτουμε ένα μεγάλο αριθμό υδατογραφημάτων στην υδατογραφημένη εικόνα I_w , εξαιρώντας έτσι την πιθανότητα αυτές οι υπογραφές να προϋπάρχουν.

Κάθε επίπεδο του μπλε καναλιού θεωρείται σαν μια τυχαία ακολουθία δυαδικών ψηφίων. Μια εικόνα συνήθως αποτελείται από συνεχόμενα μηδενικά ή άσσους στα περισσότερα σημαντικά επίπεδα και από τυχαία κατανομή στα λιγότερα σημαντικά επίπεδα. Συνεπώς, κατά την ανίχνευση των επιπέδων η πιθανότητα ενός δυαδικού ψηφίου να είναι το ίδιο με το προηγούμενο είναι μεγαλύτερη στα περισσότερα σημαντικά επίπεδα και από ότι στα λιγότερα σημαντικά. Αν και δε συμβαίνει σε όλες τις εικόνες, η θεώρηση και των 8 επιπέδων με τυχαία κατανομή των δυαδικών ψηφίων είναι πλεονεκτική για τις εκτιμήσεις μας, εφόσον οι πιθανότητες που υπολογίζονται έχουν ως όριο τις πραγματικές πιθανότητες (χωρίς την υπόθεση της τυχαίας κατανομής των δυαδικών ψηφίων στα επίπεδα) που είναι ακόμα χαμηλότερες.

Για μια τυχαία ακολουθία δυαδικών ψηφίων μήκους l , και ενός κατωφλίου t , η πιθανότητα P_t να υπάρχουν τουλάχιστον $l-t$ δυαδικά ψηφία ίδια με τα δυαδικά ψηφία του υδατογραφήματος w δίνεται από τη σχέση:

$$P_t = \sum_{i=0}^t \frac{\binom{l}{i}}{2^l}$$

Γενικά, η πιθανότητα ενός αριθμού x υδατογραφημάτων να βρεθούν σε ένα επίπεδο δυαδικών ψηφίων δίνεται από δυωνυμική κατανομή (*binomial distribution*) [Dou1999]. Χρησιμοποιώντας τα Bernoulli trials, αυτή η πιθανότητα έχει ως εξής:

$$P(x=k) = \binom{n}{x} p_t^x (1-p_t)^{n-x}$$

5.3. Αποτελέσματα

Σε αυτήν την ενότητα παρουσιάζονται διάφορες μετατροπές που συμβαίνουν στην εικόνα, μετά την ένθεση του υδατογραφήματος και τα αποτελέσματα από την ανάκτησή του.

Το υδατογράφημα, όπως ήδη συζητήθηκε, μεταβάλλει λίγο την αρχική εικόνα. Σκοπός κάθε μεθόδου υδατογράφησης είναι η ελαχιστοποίηση των μεταβολών που προκαλούνται στην αρχική εικόνα, έτσι ώστε να μην είναι εμφανείς σε κάποιο παρατηρητή. Για να υπάρχει ένας έλεγχος στο κατά πόσο η μέθοδος επηρεάζει την αρχική εικόνα, χρησιμοποιήθηκαν τρία κριτήρια: (α) μετρήσεις PSNR (*Peak Signal to Noise Ratio*) ανάμεσα στην αρχική και την υδατογραφημένη εικόνα, (β) μετρήσεις *ομοιότητας* για καθέναν πίνακα $m \times n$ δυαδικών ψηφίων και (γ) πειράματα, κάνοντας χρήση του ανθρώπινου οπτικού συστήματος (HVS).

5.3.1 Μετρήσεις PSNR

Εφόσον στη μέθοδο υδατογράφησης που προτείνεται ο αριθμός των υδατογραφημάτων αποφασίζεται από την ίδια τη μέθοδο με κριτήριο τις μετρήσεις PSNR, τότε όπως είναι αναμενόμενο το PSNR προαποφασίζεται να είναι σε αποδεκτά όρια (για παράδειγμα PSNR > 33dB). Στην εικόνα 5.1 φαίνεται η κατανομή των εικόνων για διαφορετικές μετρήσεις PSNR. Όπως φαίνεται λοιπόν από το διάγραμμα 5.1 οι περισσότερες εικόνες στις οποίες χρησιμοποιήθηκε η προτεινόμενη μέθοδος υδατογράφησης είναι κοντά στα 33dB. Επιπλέον, ο λόγος PSNR όλων των εικόνων που υδατογραφήθηκαν με την προτεινόμενη μέθοδο είναι πάνω από 33dB, έτσι όπως απαιτείται άλλωστε. Ενδεικτικά μόνο αναφέρεται ότι οι μετρήσεις PSNR εικόνων ύστερα από επίθεση είναι για παράδειγμα περίπου 27dB για JPEG Medium συμπίεση και περίπου 20dB για περιστροφή κατά 0.5°.

Κατά την προτεινόμενη μέθοδο σε μια συγκεκριμένη εικόνα εντίθεται ένας συγκεκριμένος αριθμός υδατογραφημάτων $n(i)$, όπου $i \in [0...7]$ (τα επίπεδα του μπλε καναλιού), επιτυγχάνοντας το μικρότερο αριθμό αλλαγών στα δυαδικά ψηφία, ύστερα από χρήση της *ομοιότητας*. Είναι λοιπόν αναμενόμενο, οι μετρήσεις PSNR με την προτεινόμενη μέθοδο, για συγκεκριμένο αριθμό $n(i)$ υδατογραφημάτων, να είναι οι μεγαλύτερες ή τουλάχιστον ίσες με μετρήσεις PSNR οποιασδήποτε άλλης μεθόδου που ενθέτει τον ίδιο αριθμό $n(i)$ υδατογραφημάτων.

Εικόνα 5.1: Κατανομή εικόνων για διάφορες μετρήσεις PSNR

Στην εικόνα 5.1 παρουσιάζονται τα αποτελέσματα από τις μετρήσεις PSNR που έγιναν σε ένα σύνολο εικόνων χρησιμοποιώντας τον ίδιο αριθμό υδατογραφημάτων, τόσο με την προτεινόμενη μέθοδο, όσο και με τυχαία εισαγωγή των υδατογραφημάτων. Στον πίνακα 5.1 φαίνονται οι μετρήσεις PSNR μόνο για 5 εικόνες.

<i>Εικόνες</i>	<i>Dimensions</i>	<i>$\Sigma n(i)$</i>	<i>Our Method (dB)</i>	<i>Random (dB)</i>
Acropol	681 x 411	1109	35,404	32,322
Baboon	512 x 512	1404	33,753	30,402
F-15	732 x 500	2415	33,612	31,104
Kid	487 x 703	1852	34,877	31,601
Flower	640 x 480	1793	34,088	30,994

Πίνακας 5.1: Σύγκριση PSNR για 5 εικόνες

5.3.2 Μετρήσεις ομοιότητας

Ένας άλλος τρόπος για να μετρήσει κανείς το βαθμό των αλλαγών που επήλθαν σε μια εικόνα από μια μέθοδο υδατογράφησης είναι οι μετρήσεις ομοιότητας σε καθένα από τους $m \times n$ πίνακες που αναφέρθηκαν πιο πάνω. Εφόσον η συγκεκριμένη μέθοδος τροποποιεί μόνο το μπλε κανάλι από το RGB (δηλαδή 8 $m \times n$ πίνακες), μετά την εισαγωγή του υδατογραφήματος, είναι φανερό ότι παραμένουν άλλοι 16 $m \times n$ πίνακες (8 πίνακες για το κόκκινο κανάλι και 8 για το πράσινο) που είναι 100% ίδιοι με τους αρχικούς πίνακες.

Οι μετρήσεις που γίνονται αφορούν μόνο το μπλε κανάλι, όπου εφαρμόζονται και οι τροποποιήσεις. Η συγκεκριμένη μέθοδος επηρεάζει περισσότερο τα λιγότερο σημαντικά ψηφία και ελάχιστα τα περισσότερο σημαντικά ψηφία. Στον πίνακα 5.2 στη 2^η στήλη φαίνονται οι επί τοις εκατό μετρήσεις ομοιότητας για κάθε επίπεδο του μπλε καναλιού μεταξύ των αρχικών εικόνων και των υδατογραφημένων, για ένα σύνολο 250 υδατογραφημένων εικόνων με τη συγκεκριμένη μέθοδο.

<i>Bit Level</i>	<i>Our Method</i>	<i>Random Embedding</i>
0	99.93%	99.91%
1	99.68%	99.27%
2	99.49%	99.03%
3	99.12%	98.48%
4	98.70%	98.06%
5	98.54%	97.82%
6	98.31%	97.51%
7	98.02%	97.12%

Πίνακας 5.2: Μέσος όρος της ομοιότητας (επί τοις 100)

Στην 3^η στήλη του πίνακα 5.2 φαίνεται οι επί τοις εκατό μετρήσεις ομοιότητας για κάθε επίπεδο του μπλε καναλιού μεταξύ των αρχικών και των υδατογραφημένων εικόνων, για το ίδιο σύνολο εικόνων που υδατογραφήθηκαν με τυχαία εισαγωγή πολλαπλών υδατογραφημάτων, ίδιου όμως αριθμού σε κάθε επίπεδο. Με την προτεινόμενη μέθοδο τροποποιείται ο ελάχιστος αριθμός δυαδικών ψηφίων για συγκεκριμένο αριθμό υδατογραφημάτων. Συνεπώς, οι μετρήσεις ομοιότητας είναι αρκετά υψηλότερες από αυτές της τυχαίας ένθεσης.

5.3.3 Ανθρώπινο οπτικό σύστημα (HVS)

Εφόσον ένας από τους κύριους στόχους της υδατογράφησης είναι η παραγωγή υδατογραφημένων εικόνων που να θεωρούνται από το ανθρώπινο οπτικό σύστημα πανομοιότυπες με τις αρχικές εικόνες, όλες οι εικόνες που παράγονται μετά την υδατογράφηση ελέγχονται από ανθρώπινους παρατηρητές. Η προτεινόμενη μέθοδος τροποποιεί ένα μικρό αριθμό δυαδικών ψηφίων στο μπλε κανάλι, οπότε αυτές οι αλλαγές παραμένουν απαρατήρητες, καθώς το ανθρώπινο μάτι είναι λιγότερο ευαίσθητο σε αλλαγές του μπλε καναλιού. Όλες οι υδατογραφημένες εικόνες με την

προτεινόμενη μέθοδο ελέγχθησαν από ανθρώπινους παρατηρητές και δεν παρατηρήθηκε ορατό υδατογράφημα.

Στην εικόνα 5.2 φαίνεται ένα τυπικό παράδειγμα αρχικής και υδατογραφημένης εικόνας με $n(i) = [9, 58, 204, 305, 410, 834, 919, 1556]$ αριθμό υδατογραφημάτων (σύνολο 4295 υδατογραφήματα), όπου i είναι το κάθε επίπεδο δυαδικών ψηφίων (από το περισσότερο σημαντικό στο λιγότερο σημαντικό). Το υδατογράφημα w που χρησιμοποιήθηκε σε αυτό το παράδειγμα ήταν η λέξη "Michalis" και οι μετρήσεις PSNR μεταξύ της αρχικής εικόνας και της υδατογραφημένης είναι PSNR= 35.2dB.

Εικόνα 5.2: Αρχική εικόνα - Υδατογραφημένη εικόνα

Στην εικόνα 5.3 φαίνεται ένα άλλο παράδειγμα αρχικής και υδατογραφημένης εικόνας μετά από $n(i) = [8, 25, 98, 313, 655, 816, 1427, 1472]$ αριθμό υδατογραφημάτων (σύνολο 4814 υδατογραφήματα). Το υδατογράφημα w σε αυτό το πείραμα είναι "Giannis0" και οι μετρήσεις PSNR είναι PSNR= 35.0dB.

Εικόνα 5.3: Αρχική εικόνα - Υδατογραφημένη εικόνα

Στην εικόνα 5.4 φαίνεται ένα άλλο παράδειγμα αρχικής και υδατογραφημένης εικόνας μετά από $n(i) = [1, 2, 20, 31, 70, 107, 142, 139]$ αριθμό υδατογραφημάτων (σύνολο 512 υδατογραφήματα). Το υδατογράφημα w σε αυτό το πείραμα είναι "Spyridon" και οι μετρήσεις PSNR είναι $PSNR = 34.4\text{dB}$.

Εικόνα 5.4: Αρχική εικόνα - Υδατογραφημένη εικόνα

Στην εικόνα 5.5 παρουσιάζεται η συγκεκριμένη εφαρμογή η οποία υλοποιήθηκε σε DELPHI.

Εικόνα 5.5: Εφαρμογή υδατογράφησης

5.3.4 Επιθέσεις και ανάκτηση

Η ανθεκτικότητα της προτεινόμενης μεθόδου εξετάστηκε με τη διεξαγωγή πάνω από 500 πειραμάτων. Σε αυτήν την ενότητα παρουσιάζονται τα συνολικά αποτελέσματα των πειραμάτων. Στην αρχική εικόνα I_o ενθέτονται υδατογραφήματα παράγοντας την υδατογραφημένη εικόνα I_w , συνεπώς η υδατογραφημένη εικόνα μετά τις επιθέσεις θα συμβολίζεται ως I_a . Οι επιθέσεις έχουν πάντα ως σκοπό να αφαιρέσουν το υδατογράφημα από τις εικόνες I_w , η παραγόμενη λοιπόν εικόνα I_a παρόλες τις επιθέσεις θα εμπεριέχει ακόμα έναν αριθμό υδατογραφημάτων. Αν ο αριθμός αυτός είναι αρκετά υψηλός, συγκρινόμενος με την πιθανότητα λανθασμένης ανάκτησης (δηλαδή με την περίπτωση που συμπτωματικά προϋπάρχουν υδατογραφήματα στην εικόνα I_a) τότε το υδατογράφημα θεωρείται ανακτήσιμο.

Οι τύποι των επιθέσεων που χρησιμοποιήθηκαν στην εικόνα I_w είναι: περιστροφή (μέχρι 1°), αλλαγή διαστάσεων (μέχρι 5%), θόλωμα εικόνας (*blur*), συμπίεση JPEG (χαμηλή, μεσαία και υψηλή) και κόψιμο εικόνας (*cropping*) (μέρους της εικόνας ή αφαίρεση μιας οριζόντιας ή κατακόρυφης γραμμής). Επιπλέον, εφαρμόστηκε και συνδυασμός των παραπάνω επιθέσεων (μέχρι 4 συνεχόμενες επιθέσεις).

Για την ανάκτηση του υδατογραφήματος επιλέχθηκε ως καλύτερο *κατώφλι* το $t=10$ για μήκος υπογραφής $l=64$. Για μια εικόνα μεγέθους 307,200 εικονοστοιχείων (640x480), το άνω όριο της πιθανότητας της τυχαίας εύρεσης 5 υδατογραφημάτων (σε όλα τα επίπεδα) είναι 1.8×10^{-13} (με χρήση των εξισώσεων που δόθηκαν πιο πάνω). Χρησιμοποιώντας τη βασική μας υπόθεση, ότι η πιθανότητα της εύρεσης προϋπαρχόντων x τυχαίων ακολουθιών δυαδικών ψηφίων στην αρχική εικόνα I_o με κατώφλι t είναι άνω φραγμένη, θεωρούμε κάθε υδατογράφημα ανακτημένο με επιτυχία, με πιθανότητα λανθασμένης ανάκτησης χαμηλότερη από 10^{-6} .

<i>Images</i>	<i>Rotate</i>	<i>Rescale</i>	<i>Crop P</i>	<i>Crop L</i>
Recovered	100%	100%	100%	100%
Not Recovered	0%	0%	0%	0%

Πίνακας 5.3: Περιστροφή, αλλαγή διαστάσεων, κόψιμο μέρους εικόνας και αφαίρεση μιας οριζόντιας ή κατακόρυφης γραμμής

<i>Images</i>	<i>Blur</i>	<i>Jpeg L</i>	<i>Jpeg M</i>	<i>Jpeg H</i>
Recovered	100%	95%	99%	100%
Not Recovered	0%	5%	1%	0%

Πίνακας 5.4: Θόλωμα εικόνας, συμπίεση JPEG (χαμηλή, μεσαία και υψηλή ποιότητα)

<i>Images</i>	<i>JM+Ro</i>	<i>Cr+Res</i>	<i>Cr+B</i>	<i>4-attack</i>
Recovered	100%	100%	100%	93%
Not Recovered	0%	0%	0%	7%

Πίνακας 5.5: Πολλαπλές επιθέσεις

Στους πίνακες 5.3 και 5.4 παρουσιάζεται ο αριθμός των εικόνων που επικυρώθηκαν ως υδατογραφημένες μετά από μια μοναδική επίθεση, ενώ στον πίνακα 5.5 παρουσιάζεται ο αριθμός των εικόνων που επικυρώθηκαν ως υδατογραφημένες μετά από συνδυασμό πολλαπλών συνεχόμενων επιθέσεων.

Σύμφωνα με τα αποτελέσματα που παρουσιάστηκαν στους πίνακες 5.3 και 5.4, είναι φανερό ότι η προτεινόμενη μέθοδος είναι 100% ασφαλής έναντι επιθέσεων όπως είναι η περιστροφή εικόνων, η αλλαγή διαστάσεων, και το θόλωμα της εικόνας. Αλλά και σχετικά με τη συμπίεση JPEG, η μέθοδός μας παράγει υπέροχα αποτελέσματα ακόμα και με υψηλή συμπίεση, δηλαδή χαμηλή ποιότητα εικόνας, χωρίς όμως να μπορούμε να εγγυηθούμε την επικύρωση των υδατογραφημένων εικόνων σε όλες τις περιπτώσεις.

Η προτεινόμενη μέθοδος ανθίσταται αρκετά καλά όταν υπάρχουν δύο συνεχόμενες επιθέσεις (πίνακας 5.5), όπως μεσαία συμπίεση JPEG και περιστροφή (2^η στήλη), ή κόψιμο εικόνας και αλλαγή διαστάσεων (3^η στήλη) καθώς και κόψιμο εικόνας και θόλωμα (4^η στήλη). Αλλά ακόμα και στην περίπτωση τεσσάρων συνεχόμενων επιθέσεων, όπως JPEG high, ακολουθούμενο από περιστροφή, αλλαγή διαστάσεων και θόλωμα, έχουμε αρκετά καλά αποτελέσματα ανάκτησης (4^η στήλη).

5.3.5 Μεμονωμένα παραδείγματα

Αντιπροσωπευτικά αποτελέσματα από όλους τους τύπους των επιθέσεων παρουσιάζονται για 5 χαρακτηριστικές εικόνες. Στον πίνακα 5.6 φαίνεται το όνομα

των εικόνων, οι διαστάσεις τους, τα υδατογραφήματα που ανακτήθηκαν και η πιθανότητα λανθασμένης ανάκτησης για κάθε τύπο επίθεσης. Αυτός ο πίνακας παρουσιάζει παραδείγματα και πιθανότητες λανθασμένης ανάκτησης για επιθέσεις όπως είναι η περιστροφή (Rot), η αλλαγή διαστάσεων (Res), το κόψιμο της εικόνας (Crop) και οι τέσσερες επιθέσεις συνδυασμένες.

<i>Image</i>	<i>Dims</i>	<i>Rot</i>	<i>P</i>	<i>Res</i>	<i>P</i>
Kariat	672x405	631	10^{-3115}	196	10^{-869}
Maize	640x480	319	10^{-1464}	59	10^{-229}
Arch	400x594	569	10^{-2817}	142	10^{-619}
Pills	748x518	372	10^{-1693}	58	10^{-218}
Pepp	512x512	142	10^{-0612}	128	10^{-546}

<i>Image</i>	<i>Crop</i>	<i>P</i>	<i>All</i>	<i>P</i>
Kariat	807	10^{-4069}	15	10^{-51}
Maize	611	10^{-2975}	22	10^{-77}
Arch	703	10^{-3544}	18	10^{-64}
Pills	572	10^{-2710}	14	10^{-44}
Pepp	299	10^{-1384}	10	10^{-32}

Πίνακας 5.6: Παραδείγματα ανάκτησης

5.4. Συμπεράσματα

Είναι φανερό από όλο το σύνολο των πειραμάτων ότι η προτεινόμενη μέθοδος τροποποιεί ανεπαίσθητα την αρχική εικόνα. Αξίζει να σημειωθεί ότι οι μετρήσεις PSNR των υδατογραφημένων εικόνων ήταν υψηλότερες από αυτές που έγιναν ύστερα από επιθέσεις. Με αυτήν τη μέθοδο επιτεύχθηκαν πολύ καλά αποτελέσματα σε όλους τους τύπους των επιθέσεων, ακόμα και σε συνεχόμενες πολλαπλές επιθέσεις. Η συγκεκριμένη μέθοδος θα μπορούσε να διαφοροποιηθεί αν τροποποιούσε τον τρόπο ανίχνευσης της εικόνας με διάφορους τρόπους αναζήτησης και ένθεσης του υδατογραφήματος [Arm1999]. Με αυτόν τον τρόπο μπορεί να αυξηθεί και η πολυπλοκότητα του κλειδιού. Η υδατογραφημένη εικόνα θα προστατεύεται έτσι καλύτερα από πιθανές επιθέσεις που γίνονται από γνώστες της

μεθόδου υδατογράφησης, εφόσον και η υπογραφή, αλλά και ο τρόπος ένθεσης (*scan pattern*) θα αποτελεί μέρος του κλειδιού.

Κεφάλαιο 6

Μέθοδος υδατογράφησης στο πεδίο συχνοτήτων

6.1. Εισαγωγή

Σε αυτό το κεφάλαιο παρουσιάζεται μια ασφαλής μέθοδος υδατογράφησης στο πεδίο των συχνοτήτων και πιο συγκεκριμένα με χρήση των wavelets [Arm2001]. Η μέθοδος αυτή εφαρμόζεται σε κείμενα που έχουν περάσει από το σαρωτή και τα μεταχειριζόμαστε πλέον σαν εικόνες. Το υδατογράφημα ύστερα από μια προεπεξεργασία στην οποία υπόκειται, εντίθεται στους συντελεστές που αντιπροσωπεύουν τις λεπτομέρειες σε μια εικόνα. Πειραματικά αποτελέσματα αποδεικνύουν ότι αυτή η μέθοδος δεν επηρεάζει οπτικά μια εικόνα και επιπλέον το υδατογράφημα αποδεικνύεται ότι είναι ανθεκτικό, εφόσον μπορεί να ανιχνευτεί ακόμα και μετά από τροποποιήσεις της εικόνας. Μια τέτοια τεχνική θα μπορούσε να φανεί χρήσιμη σε βάσεις δεδομένων των μουσείων, που αποθηκεύουν και σαρώνουν πολύτιμα έγγραφα.

Οι τεχνικές υδατογράφησης των ψηφιακών εικόνων μπορούν να ταξινομηθούν σε δύο κύριες κατηγορίες: στην πρώτη περιλαμβάνονται τεχνικές που ενθέτουν το υδατογράφημα στο χωρικό πεδίο μιας εικόνας ([Arm2000, Kut1998]),

ενώ στη δεύτερη περιλαμβάνονται τεχνικές που μετασχηματίζουν την εικόνα στο πεδίο των συχνοτήτων ([Kun1998, Bar2000]). Σε αυτό το κεφάλαιο λοιπόν προτείνεται μια μέθοδος υδατογράφησης βασιζόμενη στο πεδίο των συχνοτήτων και συγκεκριμένα σε Wavelets. Ο μετασχηματισμός των Wavelet είναι πλεονεκτικότερος έναντι άλλων γνωστών μετασχηματισμών, όπως είναι ο Διακριτός Μετασχηματισμός Fourier [Pol2000]. Η προτεινόμενη τεχνική σκοπό έχει να ενθέσει επιπλέον πληροφορία σε σαρωμένο κείμενο (*scanned text*), έτσι ώστε αυτή να παραμένει ανιχνεύσιμη ακόμα και μετά από τροποποιήσεις της εικόνας, και άρα να πιστοποιείται έτσι η γνησιότητα του αντικειμένου ή ο νόμιμος κάτοχος.

Στην υλοποίηση της μεθόδου λαμβάνει χώρα και ένα στάδιο προεπεξεργασίας του υδατογραφήματος [Tse2000]. Ως υδατογράφημα W μπορούν να επιλεγούν άλλα σαρωμένα κείμενα. Το στάδιο προεπεξεργασίας του υδατογραφήματος είναι απαραίτητο για να συνδυαστεί η οπτική αφάνειά του καθώς και το απρόσβλητό του. Ο παράγοντας *ομοιότητα* (Similarity ή *Similar*) εισάγεται για την ανίχνευση του υδατογραφήματος. Η μέθοδος αυτή αποδεικνύεται ανθεκτική σε συμπίεση JPEG καθώς σε άλλους μετασχηματισμούς, ενώ οι οπτικές διαφορές μεταξύ της αρχικής εικόνας και της υδατογραφημένης είναι ανεπαίσθητες.

6.2. Μετασχηματισμός Wavelet

Ο Διακριτός Μετασχηματισμός Wavelet (*Discrete Wavelet Transform - DWT*) είναι μια ορθογώνια συνάρτηση, που μπορεί να εφαρμοστεί σε πεπερασμένο αριθμό δεδομένων. Η βάση των wavelet είναι ένα σύνολο συναρτήσεων που ορίζονται από την επαναλαμβανόμενη διαφορική εξίσωση:

$$\phi(x) = \sum_{k=0}^{M-1} c_k \phi(2x - k)$$

όπου τα όρια του αθροίσματος καθορίζονται από τον συγκεκριμένο αριθμό των μη μηδενικών συντελεστών M .

Οι μετασχηματισμοί wavelet περικλείουν ένα άπειρο σύνολο. Οι διάφορες οικογένειες των wavelet διαφέρουν ως προς τον διακανονισμό ανάμεσα στο κατά πόσο συμπαγείς είναι οι συναρτήσεις της βάσης στο χώρο και στο κατά πόσο ομαλές (*smooth*) είναι [Gra1995]. Κάποιες από τις πιο γνωστές οικογένειες wavelet είναι των Haar και Daubechies.

Η πολυεπίπεδη ανάλυση (*Multi-Resolution Analysis - MRA*) είναι ένα χρήσιμο εργαλείο για την απεικόνιση των διαφόρων βάσεων των wavelet. Η MRA, καθώς δηλώνει και το όνομά της, αναλύει το σήμα σε διαφορετικές συχνότητες και με διαφορετική ανάλυση (*resolution*).

Εικόνα 6.1: Ένα επίπεδο αποσύνθεσης Wavelet

Στην αρχική εικόνα εφαρμόζονται μια σειρά από βαθυπερατά και υψηπερατά φίλτρα και αναλύουν την εικόνα σε αντίστοιχες υποζώνες. Η κάθε εικόνα μπορεί να θεωρηθεί σαν ένα δισδιάστατο σήμα και η wavelet αποσύνθεση παράγει τέσσερα τεταρτημόρια, όπως φαίνεται στην εικόνα 6.1, ένα που περιλαμβάνει μόνο χαμηλές συχνότητες και άλλα τρία που περιλαμβάνουν υψηλές συχνότητες (low-low, low-high, high-low, high-high).

Εικόνα 6.2: Γενικό διάγραμμα των τεχνικών υδατογράφησης

6.3. Η τεχνική υδατογράφησης

Το γενικό μοντέλο της προτεινόμενης τεχνικής υδατογράφησης παρουσιάζεται στην εικόνα 6.2. Αποτελείται από δύο μέρη, το στάδιο κωδικοποίησης και το στάδιο αποκωδικοποίησης. Στο πρώτο εντίθεται το υδατογράφημα W στην αρχική εικόνα I , παράγοντας την υδατογραφημένη εικόνα I' . Αντίθετα στο δεύτερο στάδιο

ελέγχεται η παρουσία ή η απουσία του υδατογραφήματος W . Αξίζει να τονιστεί ότι η διαδικασία ένθεσης διατηρεί την εικόνα σχεδόν ίδια.

6.3.1 Διαδικασία κωδικοποίησης

Όπως ήδη έχει αναφερθεί, η συγκεκριμένη τεχνική ενθέτει το υδατογράφημα στο πεδίο των wavelet, που είναι πλεονεκτικότερο συγκρινόμενο με άλλες τεχνικές στο πεδίο των συχνοτήτων ή στο χωρικό πεδίο. Η συγκεκριμένη τεχνική αντιμετωπίζει επιτυχώς τις δύο αντικρουόμενες απαιτήσεις: (1) η υδατογραφημένη εικόνα I' να είναι οπτικά όμοια με την αρχική εικόνα I και (2) το υδατογράφημα να είναι ανθεκτικό για να επιζεί σε πιθανές παραμορφώσεις της εικόνας.

Η διαδικασία κωδικοποίησης αποτελείται από δύο στάδια, την προεπεξεργασία του υδατογραφήματος και την ένθεσή του. Στο στάδιο της προεπεξεργασίας το υδατογράφημα W , το οποίο είναι ίδιων διαστάσεων ($n \times n$) όπως και η αρχική εικόνα, κβαντίζεται, έτσι ώστε κάθε εικονοστοιχείο του W είναι είτε μηδέν, είτε ένας θετικός ακέραιος $alpha$. Όσο πιο μικρό είναι το $alpha$ που επιλέγεται, τόσο το υδατογράφημα παραμένει αόρατο.

Το κβαντισμένο πλέον υδατογράφημα W_Q αναλύεται κατά wavelet σε ένα μόνο επίπεδο, δίνοντας τέσσαρες υποζώνες, που έχουν τις μισές διαστάσεις του W ($n/2 \times n/2$). Στη συνέχεια το πρώτο επίπεδο της αποσύνθεσης κατά wavelet υπερθέτεται στις ήδη κβαντισμένες τιμές του υδατογραφήματος W_Q , όπως φαίνεται στο σχήμα 6.3. Το αποτέλεσμα είναι η παραγωγή τεσσάρων μη επικαλυπτόμενων πινάκων, όπου καθένας έχει τις μισές διαστάσεις της εικόνας I ($n/2 \times n/2$). Στο τέλος αυτοί οι τέσσαρις υποπίνακες υπερθέτονται μεταξύ τους παράγοντας έτσι το τελικό υδατογράφημα W_{final} , το οποίο είναι αυτό που θα ενθεθεί στην εικόνα και στο εξής θα συμβολίζεται με W . Η προεργασία του υδατογραφήματος συμβάλλει στην ενίσχυση της ικανότητας ώστε να είναι ανιχνεύσιμο, ακόμα και μετά από πιθανές παραποιήσεις.

Η αρχική εικόνα I έχει επίσης αποσυντεθεί κατά wavelet για ένα επίπεδο, παράγοντας τέσσαρις υποζώνες συντελεστών I_C . Αξίζει να σημειωθεί ότι το παραγόμενο υδατογράφημα έχει τις ίδιες διαστάσεις όπως οι υποζώνες των συντελεστών I_C . Για να γίνει η ένθεση του υδατογραφήματος W , το τελευταίο προσθέτεται στους συντελεστές κάθε υποζώνης I_C που περιέχει τις διαφορές της εικόνας ύστερα από τα υπεραπλά φίλτρα ως εξής:

$$I'_c(o) = I_c(o) + W$$

όπου o είναι οι υποζώνες των υψηλών συχνοτήτων, $o = \{LH, HL, HH\}$.

Εικόνα 6.3: Διαδικασία ένθεσης

Για την ένθεση επιλέχθηκαν οι συντελεστές των διαφορών της εικόνας εκμεταλλευόμενοι τα χαρακτηριστικά του ανθρώπινου οπτικού συστήματος (HVS). Αυτοί οι συντελεστές αναπαριστούν τις ακμές και τα περιγράμματα της εικόνας (υψηλές συχνότητες), όπου οι μικρές παραμορφώσεις στις ακμές δεν είναι δυνατόν να είναι φανερά ορατές. Με αυτό τον τρόπο επιτυγχάνεται η μη ορατή υποβάθμιση της υδατογραφημένης εικόνας I' . Αντίθετα, οι μικρές παραμορφώσεις στους συντελεστές των χαμηλών συχνοτήτων (LL υποζώνη) επηρεάζουν ορατά τις λείες περιοχές της εικόνας. Για την τελική παραγωγή της υδατογραφημένης εικόνας I' , εφαρμόζεται ο αντίστροφος διακριτός μετασχηματισμός wavelet (*Inverse Discrete Wavelet Transform - IDWT*) όπως φαίνεται στο σχήμα 6.4.

Εικόνα 6.4: Η διαδικασία υδατογράφησης

6.3.2 Διαδικασία αποκωδικοποίησης

Η εικόνα που δημοσιεύεται στο διαδίκτυο ή οπουδήποτε αλλού είναι η υδατογραφημένη εικόνα I' . Είναι λοιπόν αναμενόμενο η εικόνα I' να υποστεί πολλές πιθανές τροποποιήσεις (ηθελημένες ή αθέλητες) που μπορεί να αλλάξουν ορατά την εικόνα I' . Το υδατογράφημα W θα πρέπει να είναι αρκετά ανθεκτικό, έτσι ώστε να εμπεριέχεται ακόμα και στη διαταραγμένη εικόνα I^* .

Κατά τη διαδικασία αποκωδικοποίησης η διαταραγμένη εικόνα I^* θα χρησιμοποιηθεί για να αποδειχθεί αν περιέχει ή όχι άλλα δεδομένα. Γι' αυτήν τη διαδικασία δεν απαιτείται η αρχική εικόνα I , γεγονός που κάνει τη μέθοδο πιο εφαρμόσιμη.

Όπως αναφέρθηκε θα χρησιμοποιηθεί ο DWT, για την αποσύνθεση της εικόνας I^* σε ένα επίπεδο. Οι παραγόμενοι συντελεστές που περιγράφουν τις λεπτομέρειες της εικόνας θα συγκριθούν με το υδατογράφημα W , κάνοντας χρήση της ομοιότητας Sim ως μέτρο ανίχνευσης του υδατογραφήματος.

$$Sim = \frac{I^* \bullet W}{W \bullet W}$$

όπου I^* είναι η διαταραγμένη εικόνα, W το υδατογράφημα και το σύμβολο $\bullet$ δηλώνει το εσωτερικό γινόμενο.

Για την ολική ομοιότητα *Similar* υπολογίζεται η μέση τιμή και των τριών κατευθύνσεων (LH, HL, HH)

$$Similar = average(Sim)$$

Το όριο τιμών της ομοιότητας *Similar* είναι προφανώς $[0, 1]$, όπου το "1" δηλώνει τη βεβαιότητα ύπαρξης του υδατογραφήματος W και το "0" ακριβώς το αντίθετο. Φυσικά, μετά από οποιαδήποτε επίθεση η τιμή του *Similar* μεταβάλλεται αντίστοιχα.

6.4. Πειραματικά αποτελέσματα

Σε αυτήν την ενότητα παρουσιάζονται τα πειραματικά αποτελέσματα, στα οποία αποδεικνύεται ότι η ένθεση με χρήση του μετασχηματισμού wavelet επιτυγχάνει και την ανθεκτικότητα, αλλά και τη μη ορατότητα του υδατογραφήματος.

Η ισχύς της προτεινόμενης μεθόδου παρουσιάζεται με ένα αριθμό πειραμάτων. Κάθε φορά υπολογίζεται η ομοιότητα *Similar* και ο λόγος σήματος προς θόρυβο (*Signal to Noise Ratio SNR*).

Στα πειράματα χρησιμοποιήθηκαν κείμενα που τα μεταχειριστήκαμε σαν εικόνες τόσο για την αρχική εικόνα I , όσο και για το υδατογράφημα W , με μέγεθος δυνάμεις του δύο ($2^m \times 2^m$). Η υδατογραφημένη εικόνα I' , καθώς και οι εικόνες I και W φαίνονται στο σχήμα 6.5.

<u>Initial Text</u>	<u>Watermark text</u>	<u>Initial Text</u>
In this text a watermark will be embedded. We aim to build a robust watermarking technique, in which the watermark will be invisible. The size of this image is 256 x 256.	This is the watermark. It is a text, which is manipulated as an image. It's size is 256 x 256. In our case is the same to the size of the original image. The size of these fonts is 12 points (bold).	In this text a watermark will be embedded. We aim to build a robust watermarking technique, in which the watermark will be invisible. The size of this image is 256 x 256.
(a)	(b)	(c)

Εικόνα 6.5: (a) Η αρχική εικόνα, (b) το υδατογράφημα και (c) η υδατογραφημένη εικόνα

Σε κάθε πείραμα, η ομοιότητα *Similar* δηλώνει την ανθεκτικότητα του υδατογραφήματος W , ενώ ο λόγος σήματος προς θόρυβο (*SNR*) αποτελεί ένα αντικειμενικό μέτρο σύγκρισης των αλλαγών που έχει υποστεί η εικόνα.

<i>Εικόνες</i>	<i>Similar</i>
Αρχική εικόνα I	0.03
Υδατογραφημένη εικόνα I'	1.00

Πίνακας 6.1: Μετρήσεις ομοιότητας για την αρχική και την υδατογραφημένη εικόνα

Για επιβεβαίωση υπολογίστηκε η *ομοιότητα Similar* τόσο για την αρχική εικόνα, όσο και για την υδατογραφημένη. Ενδεικτικά, στον πίνακα 6.1 παρουσιάζονται τα αποτελέσματα της *Similar* για τις εικόνες του σχήματος 6.5. Μετρήθηκε λοιπόν η *Similar* να είναι 0.03 για την αρχική εικόνα και 1.00 για την υδατογραφημένη εικόνα. Αυτό σημαίνει ότι η μετρική *Similar* δεν είναι ελαττωματική. Επιπλέον φαίνεται ότι η πιθανότητα προ-ύπαρξης του υδατογραφήματος στην εικόνα είναι πολύ μικρή, μια και το υδατογράφημα που χρησιμοποιήθηκε δεν είναι εντελώς τυχαίο. Έτσι, η μετρική *Similar* δηλώνει τη βέβαια ύπαρξη του υδατογραφήματος στην τελική εικόνα.

Εικόνα 6.6: Ομοιότητα έναντι της συμπίεσης JPEG

Η συμπίεση είναι από τους πιο κοινούς χειρισμούς στις εικόνες. Εφαρμόστηκε συμπίεση κατά JPEG στις υδατογραφημένες εικόνες για διαφορετικό ποσοστό συμπίεσης. Η συγκεκριμένη μέθοδος αποδεικνύεται ανθεκτική για μεσαίο ποσοστό συμπίεσης (Εικόνα 6.6) έτσι ώστε η διαταραγμένη εικόνα I^* να εμφανίζεται ορατά το ίδιο. Για παράδειγμα, όταν το ποσοστό συμπίεσης είναι 30% (δηλαδή JPEG7) η αντίστοιχη τιμή της *Similar* είναι 0.76 (βλέπε Εικόνα 6.7a). Καθώς ο ρυθμός συμπίεσης αυξάνει, η παραμόρφωση γίνεται ολοένα και πιο ορατή και η ανίχνευση του W καταλήγει να είναι προβληματική. Είναι λοιπόν αναμενόμενο με την αύξηση του ρυθμού συμπίεσης ο λόγος SNR να μειώνεται (βλέπε Εικόνα 6.8).

(a)

(b)

(c)

Εικόνα 6.7: (a) Η υδατογραφημένη εικόνα με κωδικοποίηση JPEG (ποιότητα 70%), (b) η υδατογραφημένη εικ. με Gaussian θόρυβο και (c) η υδατογραφημένη εικ. με φωτεινά εφέ

Εικόνα 6.8: SNR έναντι JPEG συμπίεσης

Μια άλλη πολύ τυπική επίθεση είναι η επίδραση που έχει ο θόρυβος πάνω σε μια εικόνα. Η συγκεκριμένη μέθοδος φαίνεται ιδιαίτερα ανθεκτική στο θόρυβο. Η εικόνα 6.7b παρουσιάζει μια υδατογραφημένη εικόνα, μετά από προσθήκη Gaussian θορύβου, στην οποία η τιμή της *Similar* επιβεβαιώνει την ύπαρξη του W ($Similar = 0.52$).

Με την εφαρμογή βαθυπερατών φίλτρων στην ήδη υδατογραφημένη εικόνα I' είναι αναμενόμενο να χάνονται οι λεπτομέρειες της εικόνας στην παραγόμενη εικόνα I^* . Παρόλα αυτά η ομοιότητα *Similar* δίνει ελπιδοφόρα αποτελέσματα για την ανίχνευση του υδατογραφήματος W .

Αντιθέτως, όταν εφαρμόζονται υπερπερατά φίλτρα στην ήδη υδατογραφημένη εικόνα I' , η τιμή της ομοιότητας *Similar* αγγίζει το 0.94, συμπεραίνοντας με πλήρη βεβαιότητα ότι η συγκεκριμένη μέθοδος είναι κατά πολύ ανθεκτική σε παραμορφώσεις φίλτρων, που διαχωρίζουν τις ακμές μιας εικόνας.

Ένα επίσης από τα πειράματα που πραγματοποιήθηκαν ήταν η έκθεση της υδατογραφημένης εικόνας I' σε φως (Εικόνα 6.7c). Παρόλο που η διαταραγμένη εικόνα I^* είναι εμφανώς αλλαγμένη από τα φωτεινά εφέ, η ανίχνευση του υδατογραφήματος W δεν είναι προβληματική.

<i>Εικόνες</i>	<i>Similar</i>	<i>SNR (dB)</i>
Watermarked image I'	1.00	44.39
I' & blurring	0.44	24.17
I' & sharpen	0.94	43.01
I' & noise (Uniform distribution)	0.56	27.43
I' & noise (Gaussian distribution)	0.52	22.45
I' & lighting effects	0.51	29.83

Πίνακας 6.2: Πειραματικά αποτελέσματα

Τα πειράματα που πραγματοποιήθηκαν έγιναν με χρήση του Matlab έκδοση 5.3.0.10183 (R11). Η οικογένεια των wavelet που χρησιμοποιήθηκαν ήταν η *Haar* οικογένεια, η παράμετρος *alpha* επιλέχθηκε να είναι "1" για τις εικόνες που παρουσιάστηκαν, ενώ το μέγεθος των εικόνων (I και W) είναι 256×256.

6.5. Συμπεράσματα

Σ' αυτό το κεφάλαιο παρουσιάστηκε μια μέθοδος υδατογράφησης κειμένων που αντιμετωπίστηκαν σαν εικόνες. Σαρωμένα κείμενα χρησιμοποιήθηκαν τόσο για την αρχική I όσο και για την υδατογραφημένη εικόνα W . Το αρχικό υδατογράφημα πέρασε πρώτα από ένα στάδιο προεργασίας με σκοπό να συνδυάσει τη διακριτικότητα και την ανθεκτικότητα. Εφαρμόστηκε ο μετασχηματισμός DWT για ένα μόνο στάδιο αποσύνθεσης της αρχικής εικόνας I , καθώς και του τελικού υδατογραφήματος. Η διαδικασία ένθεσης έλαβε χώρα μόνο στους συντελεστές που περιέχουν τις λεπτομέρειες της εικόνας I .

Χρησιμοποιήθηκε η μετρική της ομοιότητας *Similar* ως κριτήριο για την ανίχνευση του υδατογραφήματος. Τα πειραματικά αποτελέσματα έδειξαν ότι η προτεινόμενη μέθοδος έχει αρκετά καλή συμπεριφορά σε συμπίεση JPEG και το υδατογράφημα W παραμένει ανιχνεύσιμο ακόμα και σε υψηλούς ρυθμούς. Αλλά και μετά από άλλες τροποποιήσεις της υδατογραφημένης εικόνας αποδεικνύεται ότι η προτεινόμενη μέθοδος μπορεί να χαρακτηριστεί ανθεκτική, διατηρώντας ένα από τα

κύρια πλεονεκτήματα της μεθόδου, ότι δηλαδή διατηρείται το υδατογράφημα εντελώς αόρατο, αφήνοντας το αρχικό σαρωμένο κείμενο σχεδόν ανέπαφο.

Κεφάλαιο 7

Μελλοντική έρευνα

7.1. Ερευνητικά ζητήματα

Στην παρούσα διδακτορική διατριβή έγινε προσπάθεια να αντιμετωπιστεί *συλλογικά* το πρόβλημα της προστασίας των πνευματικών δικαιωμάτων και η πιστοποίηση της αυθεντικότητας προτείνοντας όσο το δυνατόν πιο ολοκληρωμένες λύσεις. Η επίλυση του προβλήματος ωστόσο δεν γίνεται να αναληφθεί μόνο από ένα άτομο. Θα πρέπει να συνεργαστούν πολλοί άνθρωποι και από διαφορετικές ειδικότητες και αρμοδιότητες. Εδώ επιχειρήθηκε να φανεί το μέγεθος του προβλήματος και προτάθηκε η πιθανή αντιμετώπισή του, προσθέτοντας έτσι και το δικό μας λιθαράκι στην όλη προσπάθεια.

Εφόσον το θέμα της προστασίας των πνευματικών δικαιωμάτων θα μας απασχολήσει κατά πολύ στο μέλλον, το πρώτο που θα πρέπει να γίνει είναι μια ενημερωτική καμπάνια πάνω στο ζήτημα που να στοχεύει να μην στους πολίτες, αλλά κυρίως στα παιδιά. Ο σεβασμός σε θέματα των πνευματικών δικαιωμάτων είναι κάτι που κτίζεται μέρα με τη μέρα και καλό θα είναι να υπάρχει χωρίς τον εξαναγκασμό της επιβολής.

Η σωστή ενημέρωση είναι εξίσου πολύ σημαντική και σε όλους τους χρήστες του Διαδικτύου. Πολλές φορές οι χρήστες παρανομούν είτε από αμέλεια, είτε από άγνοια, δίχως να γνωρίζουν τις συνέπειες. Έτσι, κατά πρώτον θα πρέπει να

ενημερώνονται για την ύπαρξη προστατευόμενων ψηφιακών αντικειμένων στις σελίδες που επισκέπτονται και κατά δεύτερον για τη νομοθεσία που τα περιβάλλει. Αναφορικά με το πρώτο, εκτός από την απλή αναγραφή των προστατευόμενων ψηφιακών αντικειμένων, ίσως η ύπαρξη ενός διαφορετικού φυλλομετρητή (browser) στον οποίο να ειδοποιείται αμέσως ο χρήστης για την ύπαρξή τους (αλλάζοντας για παράδειγμα μορφή του δρομέα - cursor) θα βοηθούσε κατά πολύ. Όσο για τη νομοθεσία, έχουν γίνει σημαντικά βήματα τελευταία, χωρίς να είναι ξεκάθαρο ακόμα ποιοι είναι οι νόμοι που διέπουν την ολότητα του Διαδικτύου.

Στην περίπτωση που έχουν εξασφαλιστεί όλα τα παραπάνω, προτείνονται μέθοδοι υδατογράφησης και γενικότερα μέθοδοι απόκρυψης πληροφορίας που θα χρησιμοποιούνται για την προστασία των πνευματικών δικαιωμάτων. Δεν είναι δυνατόν να καθοριστεί μια ομάδα μεθόδων γενικά αποδεκτών για όλες τις περιπτώσεις, διότι η κάθε μέθοδος αποδίδει ανάλογα με την εφαρμογή. Ίσως το πιο αποδοτικό θα ήταν ένα σύστημα πολλαπλής υδατογράφησης που να αποτελείται από μεμονωμένες αποδοτικές τεχνικές.

Στη συγκεκριμένη διδακτορική διατριβή προτάθηκαν μια μέθοδος απόκρυψης πληροφορίας για την προστασία των πνευματικών δικαιωμάτων και την πιστοποίηση της αυθεντικότητας, καθώς και δύο τεχνικές υδατογράφησης, μία εφαρμοσμένη στο χωρικό πεδίο και μία εφαρμοσμένη στο πεδίο συχνότητων.

Η μέθοδος απόκρυψης πληροφορίας δανείζεται έννοιες από την κρυπτογραφία και εφαρμόζεται σε μεγάλες εικόνες, εισάγοντας ένα δύσκολο στιγμιότυπο, δηλαδή έναν τρία χρωματίσιμο γράφο. Ο γράφος μαζί με τον χρωματισμό του αποτελεί το κλειδί και στην ουσία η γνώση του χρωματισμού του γράφου είναι εκείνη που πιστοποιεί το νόμιμο κάτοχο και άρα είναι ξεκάθαρο πού πρέπει να αποδοθούν τα πνευματικά δικαιώματα. Για να μην αποκαλυφθεί όλος ο χρωματισμός του γράφου σε μια πιθανή διαμάχη και άρα το κλειδί, εφαρμόζεται το πρωτόκολλο των διαντιδραστικών αποδείξεων μηδενικής γνώσης (ZKIP) για δύσκολα υπολογιστικά προβλήματα, όπως είναι το πρόβλημα χρωματισμού των γράφων. Η διαδικασία της ένθεσης έγινε με χρήση του μετασχηματισμού wavelets, παρέχοντας καλή ποιότητα των παραγόμενων εικόνων και ανθεκτικότητα σε περιπτώσεις επιθέσεων.

Μελλοντική έρευνα θα μπορούσε να διεξαχθεί σε πιο αποδοτικούς τρόπους ένθεσης της πληροφορίας, καθώς και στη Θεωρία της Υπολογιστικής Πολυπλοκότητας (*Computational Complexity Theory*) για το *χαρακτηρισμό* των δύσκολων στιγμιότυπων. Μέχρι τώρα τέτοιοι χαρακτηρισμοί είναι είτε ευριστικής

φύσεως, είτε πολύ θεωρητικοί για να χρησιμοποιηθούν στην πράξη. Επιπλέον, θα ήταν καλό να συσχετιστούν η δυσκολία (*hardness*) των υπογράφων ενός δεδομένου γράφου με τη δυσκολία του γράφου.

Στα τελευταία κεφάλαια παρουσιάζονται δύο τεχνικές υδατογράφησης (στο χωρικό πεδίο και στο πεδίο συχνοτήτων). Η τεχνική που εφαρμόστηκε στο χωρικό πεδίο εκμεταλλεύεται τυχόν ομοιότητες του υδατογραφήματος με τις αρχικές εικόνες για να επιλεγούν οι θέσεις ένθεσης. Η τεχνική αυτή θα μπορούσε να τροποποιηθεί αν η αναζήτηση των ομοιοτήτων δεν γινόταν σε σειριακά δυαδικά ψηφία, αλλά σε δυαδικά ψηφία που θα είχαν άλλη διάταξη. Όσο για την τεχνική υδατογράφησης που εφαρμόστηκε στο πεδίο συχνοτήτων μια πολύ καλή τροποποίηση θα ήταν να αντικατασταθεί το εισαγόμενο υδατογράφημα με έναν τρία χρωματίσιμο γράφο, όπως και στην τεχνική απόκρυψης πληροφορίας. Μόνο που σε αυτήν την περίπτωση θα έπρεπε να φροντίσουμε το μέγεθος των σαρωμένων κειμένων να είναι αρκετά μεγάλο, έτσι ώστε να είναι μεγάλο και το μέγεθος του γράφου που εισάγεται και επομένως να αποτελεί ο χρωματισμός του ένα δύσκολο επιλύσιμο πρόβλημα. Επιπλέον, και οι δύο αυτές τεχνικές θα μπορούσαν να χρησιμοποιηθούν σε συνδυασμό με κάποια άλλη τεχνική για την προστασία των πνευματικών δικαιωμάτων και την πιστοποίηση της αυθεντικότητας των ψηφιακών εικόνων.

Σύμφωνα με τον Craver [Cra1996] οι αόρατες υπογραφές και τα αόρατα υδατογραφήματα δεν μπορούν να αποφανθούν για τη νόμιμη κατοχή των ψηφιακών αντικειμένων με τις *τωρινές* μεθόδους υπογραφής των ψηφιακών αντικειμένων ή με τις *τωρινές* τεχνικές υδατογράφησης. Με τη διαφορά ότι ο όρος *τωρινές* αναφέρεται στις τεχνικές που προτάθηκαν μέχρι το 1996. Παρόλα αυτά είναι φανερό ότι δίχως να υπάρχει μια πρότυπη κοινά αποδεκτή μέθοδος μπορεί ο οποιοσδήποτε να ισχυριστεί τη νόμιμη κατοχή ενός ψηφιακού αντικειμένου. Για να προχωρήσει ωστόσο η επιστημονική κοινότητα σε μια τέτοια πρότυπη και κοινά αποδεκτή μέθοδο, θα πρέπει πρώτα να είναι πεπεισμένη για την αποδοτικότητα της μεθόδου. Οι δουλειές που παρουσιάστηκαν εδώ θα μπορούσαν να δρομολογηθούν σε μια τέτοια διαδικασία.

Εκείνο που διαφαίνεται είναι ότι στο μέλλον κάθε σοβαρή επιχείρηση και κάθε οργανισμός που θα δημοσιεύει ψηφιακό υλικό στο Διαδίκτυο θα επιθυμεί να είναι κατοχυρωμένα τα πνευματικά δικαιώματα. Ένα πολλαπλό σύστημα υδατογράφησης και απόκρυψης πληροφορίας, όπου από τη μια θα εισάγεται ένα δύσκολο στιγμιότυπο (ένας τρία-χρωματίσιμος γράφος), το χρωματισμό του οποίου θα τον

γνωρίζει μόνο ο νόμιμος κάτοχος, και από την άλλη θα υπάρχουν οι κλασσικές τεχνικές υδατογράφησης, ενδεχομένως να παρέχει τη βέλτιστη λύση.

Βιβλιογραφία

- [Ach2000] D. Achlioptas, C. Gomez, H. Kautz, and B. Selman, "Generating satisfiable problem instances," in *Proceedings of AAAI 2000 Conference*, 2000.
- [ACK2002] S. Armeni, D. Christodoulakis, I. Kostopoulos, Y. Stamatiou, M. Xenos, "Proving Copyright Ownership using Hard Instances of Computationally Intractable Problems," *Journal of Discrete Mathematical Sciences & Cryptography*, Academic Forum, 2002.
- [Ajt1996] M. Ajtai, "Generating hard instances of lattice problems," *Electronic Colloquium on Computational Complexity*, ECCC Report TR96-007, 1996.
- [All2004] L. Allison, "Law, ethics, the media and the InterNet," Available online at <http://www.csse.monash.edu.au/~lloyd/tilde/InterNet/Law/index.html>, accessed 2004.
- [ArC2001] S. Armeni, D. Christodoulakis, I. Kostopoulos, Y. C. Stamatiou, and M. Xenos, "Proving copyright ownership using hard instances of combinatorial intractable problems," In *Proc. 8th Panhellenic Conference in Informatics* (November 8-10, Nicosia, Cyprus, 2001), Y. Manolopoulos and S. Evripidou (eds.), [acceptance rate < 60%], pp. 137-145, Livanis Publications, 2001.
- [ArC2002] S. M. Armeni, D. N. Christodoulakis, D. K. Koukopoulos and Y. C. Stamatiou, "Ethic Aspects of Security on Information Systems," *Int.*

Conference on Electronic Resources and the Social Role of Libraries in the Future (CRIMEA2002), June 8-16, Sudak, Ukraine, 2002.

- [ArL2002] S. Armeni, S. Lioli, D. Christodoulakis, "Watermarking: from ethics to praxis," A Scholarly Symposium at the University of Memphis, *The Ethics of Electronic Information in the 21st Century (EEI21)*, October 18-21, Memphis, USA, 2001. Published in "*Ethics and Electronic Information*" by McFarland & Company, Inc. Publishers, pp. 138-147, ISBN 0-7864-1409-X, 2002.
- [Arm1999] S. Armeni, D. Christodoulakis, I. Kostopoulos, Y. Stamatiou, "Multiple signature embedding using consecutive pixel distribution," *Workshop on Watermarking and Copyright Enforcement*, October 22-23, Paris, France, 1999.
- [Arm2000] S. Armeni, D. Christodoulakis, I. Kostopoulos, Y. Stamatiou, M. Xenos, "A Transparent Watermarking Method for Color Images," *First Balkan Conference on Signal Processing, Communications, Circuits and Systems*, June 2-3, Istanbul, Turkey 2000.
- [Arm2001] S. Armeni, M. Sifakaki, D. Christodoulakis, "A Text Wavelet-based Watermarking Technique," *5th WSES Multiconference on Circuits, Systems, Communications and Computer (CSCC 2001)*, Rethymnon, Crete, Greece, July 8 – 15, 2001. Published in "Advances in Scientific Computing, Computational Intelligence and Applications", ISBN: 960-8052-36-X, pp.38-42.
- [Arm2003] Spyridoula M. Armeni, Dimitris N. Christodoulakis, Ioannis Kostopoulos, Polychronis D. Kountrias, Yannis C. Stamatiou, Michalis Xenos, "An Information Hiding Method Based on Computational Intractable Problems," {επιλέχθηκαν 31 στα 104, συνέχεια του [ArC2001]}, Y. Manolopoulos et al. (Eds.): PCI 2001, LNCS 2563, pp. 262-278, 2003, Springer Verlag Berlin Heidelberg, 2003.

- [Bar2000] M. Barni, F. Bartolini, A. Piva, "Digital Watermarking of Visual Data: State of the Art and New trends," *Proceedings of European Signal Processing Conference EUSIPCO 2000*, Tampere, Finland, pp. 1657–1664, September 5–8, 2000.

- [Ben1996] W. Bender, D. Grul, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, Vol. 35, No. 3-4, 1996.

- [Bla2000] D. Blackman and M. Leake, "Towards a universal world of computer ethics," *2nd Australian Institute of Computer Ethics Conference*, 2000.

- [Che1991] P. Cheeseman, B. Kanefsky, and W. M. Taylor, "Where the really hard problems are," in *Proc. of the International Joint Conference on Artificial Intelligence*, Vol. 1, pp. 331-337, 1991.

- [Coo1997] S. Cook and D. Mitchel, "Finding hard instances of the satisfiability problem: A survey," in *Satisfiability Problem: Theory and Applications*, DIMACS series in Discrete Mathematics and Theoretical Computer Science, American Mathematical Society, Vol. 25, pp. 1-17, 1997.

- [Cor1996] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth, "On the Lambert W function," manuscript, Computer Science Department, University of Waterloo, *Advances in Computational Mathematics*, Vol. 5, pp. 329-359, 1996.

- [Cox1996] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "A secure, robust watermark for multimedia," *Workshop on Information Hiding*, Newton Institute, Univ. of Cambridge, May 1996.

- [Cra1996] S. Craver, N. Memon, B.-L. Yeo, and M. Yeung, "Can invisible watermarks resolve rightful ownerships?," *IBM Research Report*, RC 20509, 1996.

- [Cra1999] S. Craver, "Zero knowledge watermark detection," *3rd International Workshop on Information Hiding (IHW'99)*, 1999, LNCS 1768, pp. 101-116, Springer Verlag, Berlin Heidelberg, 2000.
- [Dou1999] E. R. Dougherty, "Random processes for images and signal processing," *SPIE/IEEE Series on Imaging Science & Engineering*, 1999.
- [Fab1999] A. Fabien, P. Peticolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-A survey," *IEEE special issue on Protection of Multimedia Content*, Vol. 87, No. 7, pp. 1062-1078, July 1999.
- [Gar1979] M. R. Garey and D. S. Johnson, "*Computers and intractability, a guide to the theory of NP-completeness*," W.H. Freeman and Company, 1979.
- [GNU2004] "GNU - Philosophy of the GNU project," Available online at <http://www.gnu.org>, accessed 2004.
- [Gra1995] Amara Graps, "An Introduction to Wavelets," *IEEE Computational Science and Engineering*, Vol. 2, No. 2, 1995.
- [Hay1997] B. Hayes, "Computing science: Can't get no satisfaction," *American Scientist*, March-April, 1997.
- [Hew2004] Foreword by E-Minister Patricia Hewitt MP, "Electronic signatures – signing up to the digital economy," white paper, Available online at <http://www.itpapers.com/>, accessed 2004.
- [Hir1996] K. Hirotsugu, "An image digital signature system with ZKIP for the graph isomorphism," *International Conference on Image Processing (ICIP)*, 1996.

- [INF2004] INFOSEC, "*National information systems security GLOSSARY*," Available online at <http://www.nstissc.gov/Assets/pdf/4009.pdf>, accessed 2004.
- [Joh1997] D. G. Johnson, "Ethics online," *Communication of the ACM*, 40, No. 1, pp. 60–65, January 1997.
- [JoN2004] Neil F. Johnson, Available online at <http://www.watermarkingworld.org/WMLArchive/9908/msg00020.html>, accessed 2004.
- [Kan1781] I. Kant, (1781), "*Kritik der reinen Vernunft*," Available online at <http://www.netzhaus.ch/kantcd/>, accessed 2001.
- [Kan1785] I. Kant, (1785), "*Essay Three {8.77–87} Of The injustice Of counterfeiting books*," Available online at <http://www.hkbu.edu.hk/~ppp/fne/essay3.html>, accessed 2004.
- [Kap2000] A. C. Kaporis, L. M. Kirousis, and Y. C. Stamatiou, "A note on the non-colorability threshold of a random graph," *Electronic Journal of Combinatorics*, Vol. 7, #R29, 2000.
- [Kat1982] "*Histoire de la Philosophie – La Revolution Kantienne*," Encyclopedie de la Pleiade, Editions Gallimard, Paris 1973 – "*History of Philosophy*," Greek Translation by Kyriakou S. Katsimani, second edition, Educational Institute of National Bank, Athens 1982.
- [Kat2000] Stefan Katzenbeisser, Fabien A. P. Petitcolas, "*Information hiding techniques for steganography and digital watermarking*," Artech House Books, Boston – London, ISBN: 1-58053-035-4, 2000.
- [Kir1994] S. Kirkpatrick and B. Selman, "Critical behavior in the satisfiability of random boolean expressions," *Science*, Vol. 264, pp. 1297-1301, 1994.

- [Koe2004] C. Koenig, "Über den apriorischen Ursprung der Sittlichkeit in der Vernunft, Hausarbeit zum Hauptseminar "Kants Vernunftssittlichkeit", " Available online at <http://www.uni-koeln.de/phil-fak/fs-philol/>, accessed 2004.
- [Kou1999] D. K. Koukopoulos, Y. C. Stamatiou, "A compressed-domain watermarking algorithm for mpeg Layer 3," *Multimedia and Security Workshop at ACM Multimedia'01*, Ottawa, Canada, October 1999.
- [Kre1998] J. Kreie and T. P. Cronan, "How men and women view ethics," *Communications of the ACM*, 41, No. 9, pp. 70–76, September 1998.
- [Kun1998] Deepa Kundur and Dimitrios Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition," *Proceedings of the IEEE International Conference*, Vol. 5, pp. 2969–2972, May 1998.
- [Kut1997] Kutter, M., F. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation," in *Proceedings of the SPIE 3022, Storage and Retrieval for Image and Video Databases V*, pp. 518-526, 1997.
- [Kut1998] M. Kutter, F. Jordan and F. Bossen, "Digital Signature of Color Images Using Amplitude Modulation," *Journal of Electronic Imaging*, Vol. 7, No. 2, pp. 326–332, April 1998.
- [Kut1999] M. Kutter, F.A.P. Petitcolas, "A fair benchmark for image watermarking systems," *Proceedings of SPIE: Security and Watermarking of Multimedia Contents*, Vol. 3657, pp. 226-239, San Jose, California, January, 1999.
- [Kut2000] M. Kutter and F. Hartung, "Introduction to watermarking techniques," In Katzenbeisser, S., Petitcolas, F.A.P. (Eds.), *Information Hiding Techniques for Steganography and Digital Watermarking*, Boston-London, ISBN 1-58053-035-4, Artech House, INC., 2000.

- [Leh1995] B. Lehman and R. Brown, "*Intellectual property and the national information infrastructure – The report of the working group on intellectual property rights – Information infrastructure task force*," ISBN 0-9648716-0-1, 1995.

- [Lin2000] C.-Y. Lin, "Watermarking and digital signature techniques for multimedia authentication and copyright protection," PhD Thesis, Columbia University, 2000.

- [Mal1999] S. Mallat, "*A wavelet tour of signal processing*," Academic Press, Second Edition, 1999.

- [Mot1999] M. Motoki and R. Uehara, "Unique solution instance generation for the 3-Satisfiability (3SAT) problem," Technical Report C-129, Dept. of Math. and Comp. Sciences Tokyo Institute of Technology, 1999.

- [Nik1996] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP-96)*, Vol. 4, pp. 2168-2171, May 1996.

- [NPC2004] "NP-Complete Theory," Available online at <http://www.mutah.edu.jo/userhomepages/CS252/npcomplete.html>, accessed 2004.

- [Pap1994] C. H. Papadimitriou, "*Computational complexity*," Addison-Wesley, 1994.

- [Pet1999] F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding – Survey," *Proc. of the IEEE, Special Issue on Protection of Multimedia Content*, 87, No. 7, pp. 1062-1078, July 1999.

- [Pol2000] R. Polikar, "*The Wavelet Tutorial*," Available online: <http://www.polikar.iastate.edu/~rpolikar/WAVELETS/Wttutorial.html>
or

<http://www.public.iastate.edu/~rpolikar/WAVELETS/Wttutorial.html>,
accessed 2000.

- [QuG1998] G. Qu and M. Potkonjak, "Analysis of watermarking techniques for graph coloring problem," *ACM*, pp. 190-193, 1998.
- [Rap1997] R. Rapaport , "PR finds a new cool tool," *Forbes* pp. 101-108, 6 Oct. 1997.
- [Sol2002] K. Solanski, N. Jacobsen, S. Chandrasekaran, U. Madhow, and B. S. Manjunath, "Introducing perceptual criteria into quantization based embedding," in *Proc. of International Conference on Acoustics Speech and Signal Processing*, 2002.
- [Ste1994] W. Richard Stevens, "*The Protocols (TCP/IP Illustrated)*," Volume 1, Addison-Wesley, January 1994.
- [Ten2004] "*The ten commandments of computer ethics*," Available online at <http://www.hilton.kzn.school.za/library/computers/compethics.htm>, accessed April 2004.
- [Tse2000] S. Tsekeridou and I. Pitas, "Embedding Self-Similar Watermarks in the Wavelet Domain," *Proc. of ICASSP*, 2000.
- [Voy1998] G. Voyatzis, N. Nikolaidis and I. Pitas, "Digital Watermarking: An Overview," *Proc. of EUSIPCO'98*, September 8-11, Rhodes, Greece, 1998.
- [Web2004] "*Webopedia - The #1 Online Encyclopedia Dedicated to Computer Technology*," Available online at <http://www.webopedia.com/TERM/c/cryptography.html>, accessed 2004.
- [WIPO2004] "*WIPO - World Intellectual Property Organization*," Available online at <http://www.wipo.int>, accessed 2004.

ΘΕΡΜΗ ΠΑΡΑΚΛΗΣΗ ΝΑ ΜΗΝ ΛΗΦΘΟΥΝ ΥΠΟΨΗ
ΤΥΧΟΝ ΣΥΝΤΑΚΤΙΚΑ Ή ΓΡΑΜΜΑΤΙΚΑ ΛΑΘΗ Ή ΠΑΡΑΛΗΨΕΙΣ

ΕΥΧΑΡΙΣΤΩ