Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων

Πτυχιακή Εργασία

Τίτλος: Κρυπτογράφηση και Υδατογράφηση 2D εικόνας

Ευφροσύνη Αλεξοπούλου(ΑΜ:2002)
Περσεφόνη Κοντόκαλου(ΑΜ:1955)

Επιβλέπων καθηγητής: Τριανταφυλλίδης Γεώργιος

Επιτροπή Αξιολόγησης:

Ημερομηνία παρουσίασης: 18/05/2012

Ευχαριστίες

Αρχικά, θα θέλαμε να εκφράσουμε τις θερμές μας ευχαριστίες στον επιβλέποντα καθηγητή της παρούσας εργασίας κ. Τριανταφυλλίδη Γεώργιο για την καθοδήγηση και την πολύτιμη βοήθεια του καθ' όλη τη διάρκεια συγγραφής της πτυχιακής εργασίας.

Επίσης, ευχαριστούμε τις οικογένειες μας και τέλος τους φίλους μας για την αμέριστη συμπαράσταση, στήριξη και υπομονή που έδειξαν όλο αυτό το χρονικό διάστημα μέχρι την ολοκλήρωση των σπουδών μας.

Abstract

This study aims to analyze patterns of encryption and digital watermarking of a two dimensional image. This study was developed with various techniques. Reference is made in the history of cryptography and of watermarking, in cryptosystems and watermarking species as well as in encryption and watermarking methods.

Also, we apply these methods, like the attacks and distortions that accepts watermarked image and give their results.

Finally, there is an appendix describing the algorithms that we used to implement applications.

Σύνοψη

Η παρούσα εργασία έχει σκοπό την ανάλυση των τρόπων της κρυπτογράφησης και της ψηφιακής υδατογράφησης μιας δυσδιάστατης εικόνας. Η μελέτη αυτή αναπτύσσεται με διάφορες τεχνικές. Γίνεται αναφορά στην ιστορία της κρυπτογράφησης και της υδατογράφησης, στα είδη κρυπτοσυστημάτων και υδατογραφημάτων καθώς και στις μεθόδους κρυπτογράφησης και υδατογράφησης.

Επίσης, εφαρμόζουμε τις μεθόδους αυτές, όπως και τις επιθέσεις και παραμορφώσεις που δέχεται μια υδατογραφημένη εικόνα και παραθέτουμε τα αποτελέσματα τους.

Τέλος, υπάρχει παράρτημα που περιγράφει τους αλγορίθμους που χρησιμοποιήσαμε για την υλοποίηση των εφαρμογών.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Λίστα Πινάκων

Αρκτικόλεξα

CBC Cipher Block Chaining

CDMA Code Division Multiple Access

DCT Discrete Cosine Transform

DFT Discrete Fourier Transform

DWT Discrete wavelet Transform

ECB Electronic Codebook

FFT Fast Fourier Transform

HVS Human Visual System

JPEG Joint Photographic Experts Group

LSB Least Significant Bit

PSNR Peak to Noise Ratio

RGB Red Green Blue

RLE Run Length Encoding

SNR Signal to Noise Ratio

Εισαγωγή

1.1 Κίνητρο για την διεξαγωγή της εργασίας

Οι εξελίξεις στον χώρο της τεχνολογίας και ειδικότερα στον χώρο της πληροφορικής οδηγούν όλο και πιο συχνά στην ανάπτυξη εφαρμογών που απαιτούν χρήση υπολογιστών. Ο ρυθμός διείσδυσης του Internet αυξάνεται συνεχώς και έτσι δημιουργείται η ανάγκη προστασίας της γνησιότητας και των πνευματικών δικαιωμάτων των ψηφιακών εικόνων, αφού διάφοροι χρήστες έχουν την δυνατότητα να αποθηκεύσουν και να τροποποιήσουν ψηφιακές εικόνες που δεν τους ανήκουν. Η κρυπτογράφηση και ψηφιακή υδατογράφηση, ακόμη πιο σύγχρονη, αποτελούν μεθόδους για την προστασία από την παράνομη αντιγραφή και χρήση εικόνων.

1.2 Σκοπός της εργασίας

Ο σκοπός της εργασίας είναι η ανάλυση των τρόπων της κρυπτογράφησης και της ψηφιακής υδατογράφησης μιας δισδιάστατης εικόνας και η ανάπτυξη αυτής της μελέτης με διάφορες μεθόδους. Στόχος της πτυχιακής είναι να πληροφορήσει σχετικά με τις εφαρμογές, τα στάδια της διαδικασίας και την ασφάλεια έναντι διαφόρων επιθέσεων.

1.3 Ανάλυση κεφαλαίων

Το κεφάλαιο 2 ξεκινάει με κάποια γενικά χαρακτηριστικά της κρυπτογράφησης και της ψηφιακής υδατογράφησης, όπως την ιστορία τους ανά περιόδους.

Στο κεφάλαιο 3 γίνεται αναφορά στην ορολογία, σε βασικές λειτουργίες της κρυπτογράφησης καθώς και στα είδη κρυπτοσυστημάτων. Επίσης, γίνεται ανάλυση στις μεθόδους της κρυπτογράφησης και αναφορά στις εφαρμογές της. Όσο αφορά την ψηφιακή υδατογράφηση παρουσιάζονται οι εφαρμογές, οι στόχοι και τα στάδια της καθώς και οι τύποι υδατογραφημάτων.

Στο κεφάλαιο 4 παρουσιάζονται οι τεχνικές της κρυπτογράφησης και υδατογράφησης μαζί με τα αποτελέσματα των εφαρμογών τους.

Τέλος, στα κεφάλαια 5 και 6 αναλύονται οι επιθέσεις και παραμορφώσεις που μπορούν να παρεμποδίσουν τον σκοπό του υδατογραφήματος, όσο και οι εφαρμογές- αποτελέσματα σύμφωνα με αυτές τις επιθέσεις.

Κεφάλαιο 2

Ιστορία Κρυπτογράφησης και Υδατογράφησης

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" και είναι ένας επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας, η οποία ασχολείται με την μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για δύο ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη. Η λέξη **κρυπτολογία** αποτελείται από την ελληνική λέξη "κρυπτός" και την λέξη "λόγος" και χωρίζεται σε δύο κλάδους: Την Κρυπτογραφία και την Κρυπτανάλυση με παρεμφερή κλάδο την **Στεγανογραφία** και αντίστοιχα την Στεγανοανάλυση.

Η **Στεγανογραφία** προέρχεται από της λέξεις στεγανός + γραφή και είναι η διαδικασία κατά την οποία κρύβουμε κάποια πληροφορία, που θέλουμε να στείλουμε σε κάποιον παραλήπτη, μέσα σε ένα μέσο. Ως μέσο εδώ μπορεί να οριστεί οποιοδήποτε υλικό αντικείμενο ή άυλο (π.χ. άυλο αντικείμενο μπορεί να είναι τα αρχεία ενός ηλεκτρονικού υπολογιστή). Ο σκοπός της στεγανογραφίας είναι η αποστολή της επιθυμητής πληροφορίας κρυμμένη μέσα στο μέσο, έτσι ώστε να μην γίνει αντιληπτή από ανεπιθύμητα άτομα, άλλα μόνο από τον παραλήπτη που εμείς θέλουμε να διαβάσει την πληροφορία, τον οποίο παραλήπτη εμείς έχουμε ενημερώσει για την ύπαρξη της κρυμμένης πληροφορίας και τον τρόπο με τον οποίο μπορεί να την ανακτήσει. Για μεγαλύτερη ασφάλεια, τον τρόπο με τον οποίο έγινε η στεγανογράφηση της πληροφορίας και τον τρόπο με τον οποίο μπορούμε να ανακτήσουμε την πληροφορία πρέπει να τον γνωρίζει μόνο ο αποστολέας και ο παραλήπτης.

Όσο αφορά τα θέματα ασφάλειας, η στεγανογραφία προσφέρει προστασία της κρυμμένης πληροφορίας για όσο δεν γίνεται αντιληπτή η ύπαρξη της πληροφορίας αυτής. Αν γίνει αντιληπτή η ύπαρξη της κρυμμένης πληροφορίας τότε είναι θέμα χρόνου η ανάκτησή της, από ανεπιθύμητα άτομα, αν η πληροφορία δεν είναι κρυπτογραφημένη. Ο κλάδος που ασχολείται με την ανάκτηση των στεγανογραφικά κρυμμένων πληροφοριών λέγεται στεγανάλυση.

Επίσης πρέπει να ξεκαθαριστεί πως η στεγανογραφία δεν είναι μέθοδος κρυπτογραφίας. Η στεγανογραφία έχει ως σκοπό να αποκρύψει την ύπαρξη της πληροφορίας, σε αντίθεση με την κρυπτογραφία που σκοπεύει στην μετατροπή της πληροφορίας σε μη κατανοητή μορφή έτσι ώστε ακόμα και αν γίνει αντιληπτή η ύπαρξη της πληροφορίας να μην μπορεί να διαβαστεί από άτομα που δεν είναι κάτοχοι του κλειδιού αποκρυπτογράφησης. Συνεπώς για την επίτευξη μεγαλύτερης ασφάλειας μπορούμε να συνδυάσουμε τη στεγανογραφία με την κρυπτογράφηση. Για παράδειγμα μπορούμε ένα αρχείο κειμένου (.txt) πρώτα να το κρυπτογραφήσουμε και ύστερα να το κρύψουμε μέσα σε μια εικόνα (.gif), πάντοτε με την χρήση του κατάλληλου λογισμικού. Έτσι αν γίνει αντιληπτή η ύπαρξη του κειμένου μέσα στην εικόνα και το μέσο στεγανάλυσης ανακτηθεί, από ανεπιθύμητα άτομα, δεν θα μπορεί παρόλα αυτά να διαβαστεί, λόγο το ότι είναι κρυπτογραφημένη.

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή μετατροπή της πληροφορίας από μια κανονική κατανοητή μορφή σε έναν γρίφο, που χωρίς την γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στην γλωσσική δομή. Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση.

2.1 Ιστορική Αναδρομή Κρυπτογράφησης

2.1.1 Πρώτη Περίοδος Κρυπτογράφησης (1900 π.Χ. – 1900 μ.Χ.)

Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

Όπως προκύπτει από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (με βάση τον Kahn). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας. η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Χαρακτηριστικό παράδειγμα χρήσης της στεγανογραφίας στα παλιά χρόνια είναι η αφήγηση ενός ιστορικού γεγονότος από τον Ηρόδοτο. Ο Ηρόδοτος αναφέρει στην ‘Ηροδότου Ιστορία’ πως στην αρχαία Ελλάδα ο Δημάρατος, Έλληνας ο οποίος ζούσε στην Περσία, θέλοντας να ειδοποιήσει τη Σπάρτη ότι ο Ξέρξης σκόπευε να εισβάλει στην Ελλάδα, αφαίρεσε το κερί από την πλάκα γραφής, χάραξε το μήνυμα του πάνω στο ξύλο και μετά κάλυψε και πάλι την πλάκα με κερί. Η πλάκα φαινόταν ακριβώς με μία κενή και έτσι ξεγέλασε αυτούς που του έκαναν έλεγχο. Μία άλλη ιδιοφυής μέθοδος αναφέρεται πάλι από τον Ηρόδοτο κατά την οποία ξυρίστηκε το κεφάλι ενός αγγελιαφόρου και δερματοστίκτηκε πάνω ένα μήνυμα το οποίο και εξαφανίστηκε μόλις φύτρωσαν μαλλιά (στεγανογραφία).

Επιπλέον πολλές τέτοιες τεχνικές αναπτύχθηκαν ή αναφέρθηκαν από τον Αινεία όπως κρυμμένα γράμματα μέσα στις σόλες των αγγελιαφόρων ή στα σκουλαρίκια των γυναικών και σημειώσεις οι οποίες μεταφέρονταν από περιστέρια. Ο Αινείας επίσης είσαγε την απόκρυψη πληροφοριών σε κείμενο αλλάζοντας το ύψος των γραμματοσειρών ή κάνοντας πολύ μικρές τρύπες πάνω ή κάτω από τα γράμματα ενός κειμένου. Αυτή η τεχνική τροποποιήθηκε και εφαρμόστηκε κατά την διάρκεια του 17^{ου} αιώνα από τον Wilkins (1614-1672), ο οποίος αντί των τρυπών χρησιμοποίησε αόρατο μελάνι για να τυπώσει πολύ μικρές τελείες και να αποκρύψει κάποιο μήνυμα. Οι Γερμανοί κατάσκοποι επαναχρησιμοποίησαν τη μέθοδο αυτή τόσο στον πρώτο όσο και στον δεύτερο Παγκόσμιο Πόλεμο.

Ακόμη ένα παράδειγμα προέρχεται από το χώρο της Αρχιτεκτονικής. Οι καλλιτέχνες έχοντας καταλάβει ότι κοιτάζοντας ένα γλυπτό ή ένα πίνακα από διαφορετικές οπτικές γωνίες μπορείς να δεις διαφορετικά πράγματα, χρησιμοποίησαν τα έργα τέχνης τους καμουφλάροντας σ’ αυτά επικίνδυνες για την εποχή πολιτικές πεποιθήσεις και αιρετικές ιδέες . Ένα τέτοιο αριστούργημα είναι το Vaxierbild του Sho (1530), το οποίο με την πρώτη ματιά φαίνεται να είναι ένα τοπίο, αλλά παρατηρώντας το προσεκτικά από τη σωστή οπτική γωνία αποκαλύπτονται πορτρέτα διάσημων βασιλιάδων.

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφεύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση την μέθοδο της αντικατάστασης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη», Εικόνα 1, ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες,

ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Αν ο παραλήπτης είχε μια πανομοιότυπη σκυτάλη, με την ίδια διάμετρο, τότε μπορούσε να διαβάσει το μήνυμα τυλίγοντας τη περγαμηνή γύρω της. Το τύλιγμα της περγαμηνής σε σκυτάλη διαφορετικής διαμέτρου έδινε μια σειρά ανακατεμένων γραμμάτων σε, φαινομενικά, τυχαία σειρά. Φυσικά ένας υπομονετικός «εχθρός» μπορούσε να δοκιμάζει διαδοχικά σκυτάλες διαφορετικής διαμέτρου, ώσπου να πετύχει τη «σωστή».

Εικόνα 1: Η Σπαρτιατική Σκυτάλη, μια πρώιμη συσκευή για την κρυπτογράφηση

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στην στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Ο Καίσαρας χρησιμοποίησε και άλλα, πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

Στην διάρκεια του Μεσαίωνα, η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της.

Η εξέλιξη, τόσο της κρυπτολογίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Στο γνωστό μυθιστόρημα «Χίλιες και μία νύχτες» κυριαρχούν οι λέξεις-αινίγματα, οι γρίφοι, τα

λογοπαίγνια και οι αναγραμματισμοί. Έτσι, εμφανίστηκαν βιβλία που περιείχαν κρυπταλφάβητα, όπως το αλφάβητο «Dawoudi» που πήρε το όνομα του από τον βασιλιά Δαυίδ. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας, επινοήθηκε από αυτούς γύρω στον 14ο αιώνα. Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Ο Ιταλός Giovanni Batista Porta, το 1563, δημοσίευσε το περίφημο για την κρυπτολογία βιβλίο «De furtivis literarum notis», με το οποίο έγιναν γνωστά τα πολυαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα, στα οποία, δύο γράμματα αντικαθίστανται από ένα.

Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλλος Vigenere, του οποίου ο πίνακας πολύ-αλφαβητικής αντικατάστασης, χρησιμοποιείται ακόμη και σήμερα. Ο κώδικας του Vigenere αναπτύχθηκε για να καλύψει τις αδυναμίες του κώδικα του Καίσαρα, πάνω στον οποίο βασίστηκε. Δημιουργήθηκε από το διπλωμάτη Blaise de Vigenere (1523-1596) και χρησιμοποιεί αντί για ένα, 26 αλφάβητα, καθένα από τα οποία σχηματίζεται από το προηγούμενο με κυκλική εναλλαγή ενός γράμματος. Όλα μαζί απεικονίζονται σε έναν πίνακα (ταμπλό), το ταμπλό του Vigenere, που παρατίθεται παρακάτω. Ακόμη απαιτείται μια λέξη-κλειδί, η οποία καθορίζει με ποια σειρά του πίνακα θα γίνει η αντικατάσταση. Δηλαδή με βάση το πρώτο γράμμα της λέξεως κλειδί αντιστοιχούμε το γράμμα του αρχικού κειμένου με το γράμμα από το κρυπτογραφικό αλφάβητο που βρίσκεται στην ίδια σειρά με το πρώτο γράμμα της λέξεως κλειδί. Το ίδιο γίνεται και με τα επόμενα γράμματα των λέξεων, ενώ θεωρούμε ως βάση για τη μεταφορά του αρχικού μηνύματος σε κρυπτογραφημένη μορφή την διαδοχική επανάληψη της λέξεως-κλειδί.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Εικόνα 2: Ταμπλό του Vigenere

Ο C.Wheatstone, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία αποτέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές.

Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το 3000 π.Χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της

εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός Ιησουΐτης Αθανάσιος Κίρχερ εξέδωσε ένα λεξικό ερμηνείας τους, με τίτλο «Oedipus Aegyptiacus». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλεύσουν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς την σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο τρεις φορές. Μία με ιερογλυφικά, μία στα ελληνικά και μία σε ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν, μοιράστηκαν την δόξα της ερμηνείας τους.

Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ. Χρονολογικά, οι γραφές αυτές κατατάσσονται ως εξής:

- 3000-1600 π.Χ. : Εικονογραφική (Ιερογλυφική) γραφή
- 1850-1450 π.Χ.: Γραμμική γραφή Α
- 1450-1200 π.Χ.: Γραμμική Γραφή Β

Η Κρητική εικονογραφική (ή ιερογλυφική) γραφή δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή, η οποία εξαντλείται σε περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με την γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στον Δίσκο της Φαιστού, Εικόνα 3, που ανακαλύφθηκε το 1908 στην νότια Κρήτη.

Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με την μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με την βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Εικόνα 3: Ο Δίσκος της Φαιστού

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς (Sir Arthur Evans), τον μεγάλο Άγγλο αρχαιολόγο, που ανάσκαψε συστηματικά την Κνωσό το 1900. Ο ίδιος ονόμασε αυτή τη γραφή γραμμική, επειδή τα γράμματα της είναι γραμμές (ένα γραμμικό σχήμα) και όχι σφήνες, όπως στην σφηνοειδή γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Η γραμμική γραφή Α είναι μάλλον η γραφή των Μινωιτών (από το μυθικό Μίνωα, βασιλιά της Κνωσού), των κατοίκων της αρχαίας Κρήτης και από αυτή ίσως να προήλθε το σημερινό ελληνικό αλφάβητο. Τα γράμματα της γραμμικής γραφής χαράζονταν με αιχμηρό αντικείμενο πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονταν σε φούρνους. Οι περισσότερες από τις επιγραφές με Γραμμική γραφή Α (περίπου 1500) είναι λογιστικές και περιέχουν εικόνες ή συντομογραφίες των εμπορεύσιμων προϊόντων και αριθμούς για υπόδειξη της ποσότητας ή οφειλής.

Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη, αν και ορισμένα πρόσφατα ευρήματα καταδεικνύουν ότι μπορεί να αποτέλεσε μέσο γραφής και αλλού, αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στο Μουσείο Ηρακλείου. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη. Ο Evans έδωσε και την ονομασία στην Γραμμική Γραφή Β, επειδή αναγνώρισε ότι πρόκειται για συγγενική γραφή με την γραμμική Α, πιο πρόσφατη ωστόσο και εξελιγμένη. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με την γραμμική γραφή Β βρέθηκαν στην Κνωσό, στα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και την Τίρυνθα.

Σήμερα αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη.

Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά φυλάσσονταν σε αρχειοφυλάκια και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια.

Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες. Συστηματικά, με την γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. Ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στην συνέχεια, όμως, αρκετοί προσχώρησαν στην άποψή του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου, είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Enigma. Προσπάθησε να μεταφέρει την πείρα του στην Κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων έφερε το πολυπόθητο αποτέλεσμα. Το 1953 κατέγραψαν τα συμπεράσματά τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο Κρυπτανάλυσης.

Η αποκρυπτογράφηση της Γραμμικής Β απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι Μυκήνες. Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα ανάλογο της κατάκτησης του Έβερεστ, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

2.1.2 Δεύτερη Περίοδος Κρυπτογράφησης (1900 μ.Χ. – 1950 μ.Χ.)

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά την μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια.

Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η Κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν

επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια αυτής της περιόδου η Κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma (Εικόνα 4).

Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασίζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη

και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του, όπως ο Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη.

Εικόνα 4: Η μηχανή Αίνιγμα (Enigma)

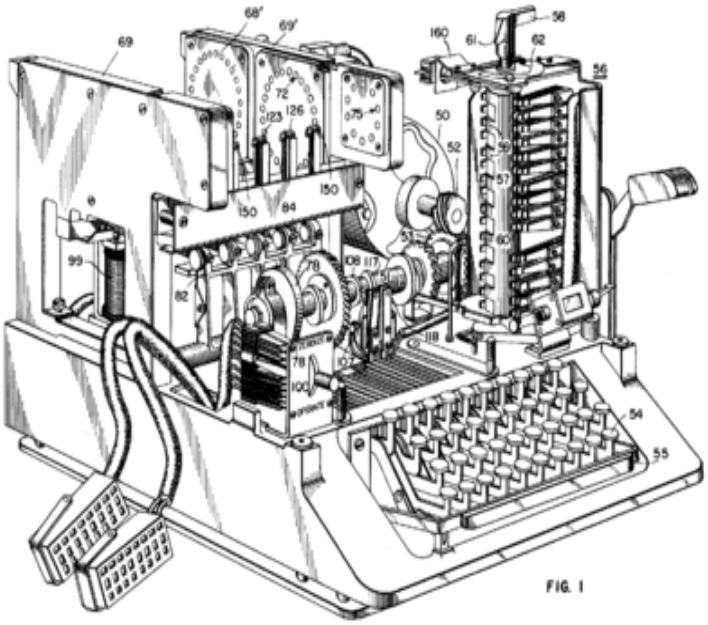
Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας αποκρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με την βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus και, δυστυχώς, καταστράφηκε με το τέλος του Πολέμου. Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το 1940) έσπασαν αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στην Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, (που καλείται Purple), και χρησιμοποίησε, επίσης, διάφορες παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αποκλήθηκε "Μηχανή-Μ" από τις ΗΠΑ, ενώ μια άλλη αναφέρθηκε ως «Red» (Κόκκινη). Μια ομάδα του αμερικανικού στρατού, η αποκαλούμενη SIS, κατάφερε να σπάσει το ασφαλέστερο ιαπωνικό διπλωματικό σύστημα κρυπτογράφησης (μια ηλεκτρομηχανική συσκευή, η οποία αποκλήθηκε "Purple" από τους Αμερικανούς) πριν καν ακόμη αρχίσει ο Β΄ Παγκόσμιος Πόλεμος. Οι Αμερικανοί αναφέρονται στο αποτέλεσμα της Κρυπτανάλυσης, ειδικότερα της μηχανής Purple, αποκαλώντας το ως Magic (Μαγεία).

Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA (Εικόνα 5). Και τα δύο ήταν

ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές εν τούτοις βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών M-94. Οι Βρετανοί πράκτορες της Υπηρεσίας "SOE" χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά). Οι Γερμανοί, ώρες πριν την
Απόβαση της Νορμανδίας συνέλαβαν ένα μήνυμα - ποίημα του Πολ Βερλέν, για το οποίο, χωρίς να το έχουν αποκρυπτογραφήσει, ήταν βέβαιοι πως προανήγγελλε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την προειδοποίηση.

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις, συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.



Εικόνα 5: κρυπτομηχανή SIGABA

2.1.3 Τρίτη Περίοδος Κρυπτογράφησης (1950 μ.Χ. - Σήμερα)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το 1949 δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (Communication Theory of Secrecy Systems) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της

Επικοινωνίας» (Mathematical Theory of Communication), μαζί με τον Warren Weaver. Αυτά, εκτός από τις άλλες εργασίες του επάνω στην θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την Κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακά τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Εντούτοις, το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς την αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με την χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης.

Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε
να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

2.2 Ιστορική Αναδρομή Υδατογράφησης

Η Ψηφιακή Υδατογραφία βασίζεται στην επιστήμη της Στεγανογραφίας. Τα πρώτα υδατογραφήματα σε χαρτί έκαναν την εμφάνιση τους μαζί με την τέχνη της κατασκευής χειροποίητου χαρτιού περίπου 7 αιώνες πριν. Το παλαιότερο υδατογραφημένο κομμάτι χαρτιού που έχει βρεθεί , χρονολογείται στο 1292 στην πόλη Fabriano της Ιταλίας, μια πόλη με μεγάλη επιρροή στην ανάπτυξη βιομηχανιών χαρτιού. Στα τέλη του 13^{ου} αιώνα, λειτουργούσαν περίπου 40 μύλοι χαρτιού και ο καθένας από αυτούς παρήγαγε χαρτί με διαφορετική μορφή, ποιότητα και τιμή. Όμως το χαρτί που φτιαχνόταν είχε τραχεία επιφάνεια και δεν ήταν κατάλληλο για γραφή. Η πρώτη ύλη χαρτιού επεξεργαζόταν από ειδικούς τεχνίτες και έτσι η επιφάνεια αποκτούσε λεία υφή. Το επεξεργασμένο χαρτί γινόταν κατάλληλο για γράψιμο και ήταν πλέον έτοιμο προς πώληση. Ο ανταγωνισμός τόσο μεταξύ των παραγωγών όσο και μεταξύ των εμπόρων ήταν πολύ υψηλός και δύσκολα μπορούσαν να κρατηθούν αρχεία πιστοποίησης για την προέλευση, την ποιότητα και τον τύπο χαρτιού. Η εισαγωγή της υδατογράφησης ήταν ο καλύτερος τρόπος για να εξαλείψουν οποιαδήποτε πιθανότητα σύγχυσης. Μετά την εφεύρεση τους, οι υδατογραφήσεις διαδόθηκαν αστραπιαία σε όλη την Ιταλία και την Ευρώπη. Αν και στην αρχή χρησιμοποιήθηκαν για τη φίρμα του χαρτιού, στη συνέχεια χρησιμοποιήθηκαν ως ένδειξη ποιότητας, του τύπου, της χρονολόγησης και της αυθεντικότητας του χαρτιού.

Το λεξικό του χαρτιού ορίζει το υδατογράφημα σαν μια τροποποίηση της δομής και της αδιαφάνειας ενός φύλλου χαρτιού όταν είναι ακόμα υγρό έτσι ώστε το μοτίβο να είναι εμφανές στο στεγνό φύλλο όταν βρίσκεται απέναντι από το φως. Χρησιμοποιήθηκαν τρεις τεχνικές για να παράγουν υδατογραφήματα.

Στην πρώτη τεχνική χρησιμοποιούνταν σύρματα, λυγισμένα μέταλλα ή ξύλινα σχήματα που τοποθετούνταν στο καλούπι πλαισίου ή υφάσματος για να παραχθούν υδατογραφήματα σε χειροκίνητα καλούπια. Το αποτέλεσμα αυτής της τεχνικής είναι κάποιες περιοχές να έχουν λιγότερη πυκνότητα ινών δίνοντας έτσι μια ελαφριά εικόνα όταν το τελικό χαρτί βρισκόταν απέναντι στο φως.

Η δεύτερη τεχνική, ονομαζόταν τονική μέθοδος ή σημάδι, και παρήγαγε συνεχή τονικά υδατογραφήματα όμοια με ασπρόμαυρες φωτογραφίες και επέτρεπε την παραγωγή αριστουργηματικών υδατογραφημάτων. Το σχέδιο του υδατογραφήματος χαράζονταν με το χέρι σε ένα κομμάτι κεριού σε τρισδιάστατη μορφή. Αυτό το πρωτότυπο κεριού χρησιμοποιούνταν για την δημιουργία ενός θηλυκού καλουπιού με τη βοήθεια του οποίου παραγόταν το χαρτί. Η τεχνική αυτή δημιούργησε πολύ όμορφα δείγματα υδατογραφημάτων.

Η τρίτη και τελευταία τεχνική, ήταν το πιεσμένο ή ανάγλυφο υδατογράφημα. Το υδατογράφημα, σε μορφή σχεδίου πάνω σε ελαστική πλάκα, πιεζόταν πάνω στο υγρό χαρτί κατά τη φάση της πίεσης της μηχανής του χαρτιού. Η ποιότητα αυτού του υδατογραφήματος ήταν κατώτερη σε σχέση με της προηγούμενες τεχνικές, γιατί κατά τη διαδικασία πίεσης της μηχανής, το υγρό χαρτί εμφανίζει ήδη μια αρκετά υψηλή συνοχή και έτσι επιτρέπει μόνο περιορισμένες τοπικές αλλοιώσεις στη δομή του χαρτιού.

Από την εμφάνιση του υδατογραφήματος γίνονταν προσπάθειες για να παραποιηθεί και για να προσομοιωθεί. Οι προσπάθειες αυτές είχαν απώτερο σκοπό τις λαθραίες εφαρμογές. Επίσης, τα υδατογραφήματα είχαν μεγάλη χρησιμότητα στα δικαστήρια ως αποδείξεις με χαρακτηριστικό παράδειγμα μια περίπτωση στη Γαλλία το 1887, γνωστή ως Des Decorations. Τα υδατογραφήματα από δύο γράμματα συγκρίθηκαν και η απόδειξη τους οδήγησε στη δίωξη ενός βουλευτή, την πτώση ενός υπουργείου και τέλος την παραίτηση του προέδρου Grevy.

Τα υδατογραφήματα είναι ένα αναπόσπαστο κομμάτι της βιομηχανίας χαρτιού. Προσφέρουν ένα επίπεδο αόρατης ασφάλειας έχοντας ως βάση τη χρονολόγηση του χαρτιού, την αυθεντικοποίηση και την προέλευση του. Αυτό το επίπεδο ασφάλειας, αν και ήταν χαμηλό, εμπόδιζε τον κόσμο για τα προηγούμενα 700 χρόνια από την αντιγραφή και νοθεία των εγγράφων.

Στις μέρες μας, αντιμετωπίζουμε κάτι παρόμοιο με αυτό πριν από 700 χρόνια μόνο που τώρα αφορά τα ψηφιακά έγγραφα. Τα ψηφιακά έγγραφα όπως οι εικόνες, δεν έχουν μέσο για να προστατέψουν (χαρτί) αλλά το ίδιο το περιεχόμενο χρειάζεται προστασία. Αρχικός σκοπός των υδατογραφημάτων ήταν να προσθέτουν αόρατη πληροφορία υπό την μορφή εικόνας ή κειμένου σε ένα φύλλο χαρτιού. Αυτή η ιδέα μπορεί πολύ εύκολα να εφαρμοσθεί και σε ψηφιακά δεδομένα.

Οι πρώτες δημοσιεύσεις που επικεντρώνονται στο θέμα της υδατογράφησης ψηφιακών εικόνων εκδόθηκε από τον Tanaka το 1990 και από τους Carroni και Tirkel το 1993. Η τελευταία δημοσίευση επινόησε τη λέξη υδατογράφημα. Η ψηφιακή υδατογράφηση έχει γίνει αντικείμενο μεγάλης μελέτης και εξελίσσεσαι με πάρα πολύ γρήγορους ρυθμούς από το 1995 και έπειτα.

Εικόνα 6: Πίνακας ζωγραφικής με υδατογραφημένο λογότυπο

Εικόνα 7: Υδατογραφημένο γερμανικό χαρτονόμισμα του 1922

Εικόνα 8: Υδατογραφημένο γραμματόσημο

Κεφάλαιο 3

Κρυπτογράφηση Και Ψηφιακή Υδατογράφηση

3.1 Κρυπτογράφηση

Η κρυπτογράφηση εικόνας είναι μία τεχνική για μετάδοση πληροφορίας μέσω καναλιών επικοινωνίας, χωρίς κάποιος τρίτος να μπορεί να διαβάσει και να ερμηνεύσει αυτή την πληροφορία, έστω και αν αντιληφθεί την παρουσία της. Έτσι η κρυπτογράφηση έχει γίνει ένα από τα σπουδαιότερα και βασικότερα εργαλεία για τον έλεγχο εισόδου, για αυθεντικοποίηση, για ψηφιακές υπογραφές και για ασφαλείς ανταλλαγές μηνυμάτων. Η κρυπτογράφηση χρησιμοποιείται σε διάφορες εφαρμογές επιβάλλοντας προστασία σε πληροφορίες των πιστωτικών καρτών, σε μηνύματα του ηλεκτρονικού ταχυδρομείου, και γενικά σε μεταδιδόμενα δεδομένα. Η κρυπτογράφηση αντιπροσωπεύει την τέχνη της προστασίας της πληροφορίας με την μετατροπή της σε μη αναγνώσιμη μορφή που ονομάζεται κρυπτογράφημα (cipher text). Μόνο αυτοί που κατέχουν το μυστικό κλειδί μπορούν να αποκρυπτογραφήσουν τα κωδικοποιημένα δεδομένα στην αρχική τους μορφή. Τα κωδικοποιημένα μηνύματα μπορούν μερικές φορές να σπάσουν με την Κρυπτανάλυση. Η κρυπτογράφηση μπορεί γενικά να διαχωριστεί σε συμμετρική και ασύμμετρη.

3.1.1 Βασικές Λειτουργίες Κρυπτογράφησης

Η κρυπτογράφηση παρέχει 4 βασικές λειτουργίες:

- **Εμπιστευτικότητα(Confidentially)**:Εμπιστευτικότητα είναι η ιδιότητα των δεδομένων ή πληροφοριών να είναι προσπελάσιμα μόνο από τις εξουσιοδοτημένες προς τούτο οντότητες. Η εμπιστευτικότητα αναφέρεται στο περιεχόμενο ηλεκτρονικών εγγράφων ή, γενικά, αρχείων και μηνυμάτων, στην ύπαρξή τους και στην ταυτότητα αυτών που εκτελούν ενέργειες και ανταλλάσσουν μηνύματα. Επίσης, αναφέρεται στο χρόνο και την ποσότητα μηνυμάτων που ανταλλάσσονται. Η εμπιστευτικότητα, μερικές φορές, καλείται και «ιδιωτικότητα» ή «μυστικότητα» ή «προστασία του απορρήτου».
- **Ακεραιότητα(Integrity)**: Η ακεραιότητα είναι η ιδιότητα των δεδομένων και πληροφοριών και των υπολογιστικών και επικοινωνιακών πόρων να τροποποιούνται μόνο από εξουσιοδοτημένες οντότητες κατά εξουσιοδοτημένο τρόπο. Η ακεραιότητα έχει να κάνει με την ακρίβεια και τη συνέπεια στη λειτουργία συστημάτων και διεργασιών. Τα δεδομένα σε κάθε σύστημα πρέπει να παραμένουν πλήρη και ορθά. Η ακεραιότητα διατηρείται όταν διατηρούνται και οι ιδιότητες: η ακρίβεια, η μη τροποποίηση ή τροποποίηση από εξουσιοδοτημένους χρήστες ή διεργασίες, με συνέπεια, κατά αποδεκτό τρόπο. Έχουν αναγνωριστεί τρεις καθοριστικές συνιστώσες του όρου ακεραιότητα: οι «εξουσιοδοτημένες ενέργειες», ο «διαχωρισμός και η προστασία αγαθών» και, τέλος, «η ανίχνευση και διόρθωση σφαλμάτων».
- **Μη απάρνηση(non-repudiation)**: είναι η ιδιότητα η οποία αποτρέπει μια οντότητα από το να αρνηθεί προηγούμενες δεσμεύσεις ή ενέργειες. Όταν προκύψουν αμφισβητήσεις που οφείλονται στο γεγονός ότι μια οντότητα αρνείται ότι είχαν γίνει ορισμένες ενέργειες, είναι απαραίτητο μέσον προκειμένου να αποσαφηνίσει την κατάσταση. Παραδείγματος χάρη, μια οντότητα μπορεί να δώσει

εξουσιοδότηση για την αγορά ενός αγαθού από μια άλλη οντότητα και αργότερα να αρνηθεί ότι είχε παραχωρηθεί τέτοια εξουσιοδότηση. Είναι απαραίτητη μια διαδικασία που εμπλέκει ένα έμπιστο τρίτο μέλος για να άρει την αμφισβήτηση.

- **Πιστοποίηση(authentication)**: είναι η ιδιότητα που σχετίζεται με την ταυτοποίηση. Αυτή η λειτουργία εφαρμόζεται στις δύο οντότητες και την ίδια την πληροφορία. Δύο
μέλη που εισέρχονται σε μια επικοινωνία θα πρέπει να ταυτοποιήσουν το ένα το άλλο. Για την πληροφορία που μεταβιβάζεται μέσω ενός καναλιού θα πρέπει να πιστοποιείται η αυθεντικότητά της ως προς την πηγή προέλευσης, την ημερομηνία προέλευσης, το περιεχόμενο των δεδομένων, την ώρα αποστολής, κτλ. Γι' αυτούς τους λόγους αυτή η πλευρά της κρυπτογραφίας συνήθως υποδιαιρείται σε δύο κύριες κλάσεις: την πιστοποίηση αυθεντικότητας της οντότητας και πιστοποίηση αυθεντικότητας της πηγής των δεδομένων. Η πιστοποίηση αυθεντικότητας της πηγής των δεδομένων έμμεσα παρέχει την ακεραιότητα των δεδομένων (γιατί εάν ένα μήνυμα είναι τροποποιημένο, έχει αλλάξει η πηγή).

3.1.2 Ορολογία

Η επιθυμία προστασίας του περιεχομένου μηνυμάτων οδήγησε στην επινόηση και χρήση κρυπτογραφικών τεχνικών και συστημάτων τα οποία επιτρέπουν το μετασχηματισμό μηνυμάτων ή δεδομένων κατά τέτοιον τρόπο ώστε να είναι αδύνατη η υποκλοπή του περιεχομένου τους κατά τη μετάδοσή ή αποθήκευσή τους και, βεβαίως, την αντιστροφή του μετασχηματισμού. Η διαδικασία μετασχηματισμού καλείται **κρυπτογράφηση** και η αντίστροφή της **αποκρυπτογράφηση**. Η συνάρτηση ή το σύνολο των κανόνων, στοιχείων και βημάτων που καθορίζουν την κρυπτογράφηση και την αποκρυπτογράφηση ονομάζεται **κρυπτογραφικός αλγόριθμος**. **Αρχικό κείμενο (plaintext)** είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης. **Κλειδί (key)** είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης. Η υλοποίηση του κρυπτογραφικού αλγόριθμου καλείται **κρυπτογραφικό σύστημα.** Μερικές φορές, ο κρυπτογραφικός αλγόριθμος καλείται και κωδικοποιητής (cipher). Κρυπτογραφημένο κείμενο (cipher text) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο. Πρωτόκολλα που χρησιμοποιούν κρυπτογραφικούς αλγόριθμους καλούνται κρυπτογραφικά πρωτόκολλα. Κρυπτανάλυση (cryptanalysis) είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

3.1.3 Τυπικό σύστημα κρυπτογράφησης – αποκρυπτογράφησης

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στην μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

3.1.3.1 Βασικές Έννοιες

Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει την δυνατότητα σε 2 πρόσωπα, έστω τον Κώστα και την Βασιλική, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας αντίπαλος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

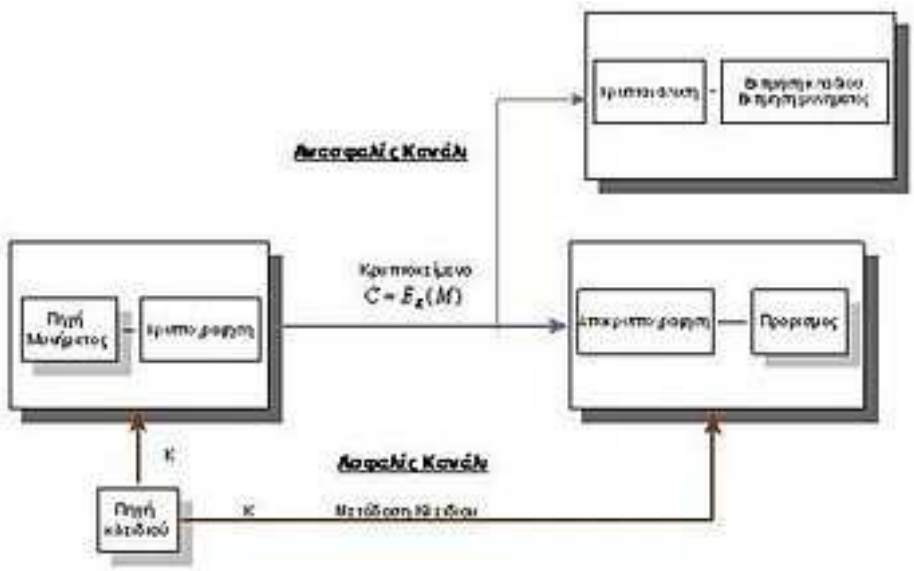
Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P,C,k,E,D):

- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων.
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων.
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος.
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση.
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης.
- Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μέσα από τον χώρο P και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, τον χώρο C και τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P.

Το σύστημα της Εικόνας 9 λειτουργεί με τον ακόλουθο τρόπο :

1. Ο αποστολέας επιλέγει ένα κλειδί μήκους n από τον χώρο κλειδιών με τυχαίο τρόπο, όπου τα n στοιχεία του K είναι στοιχεία από ένα πεπερασμένο αλφάβητο.
2. Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.
3. Ο αποστολέας δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων.
4. Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (έναν γρίφο) και η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.
5. Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις 2 τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

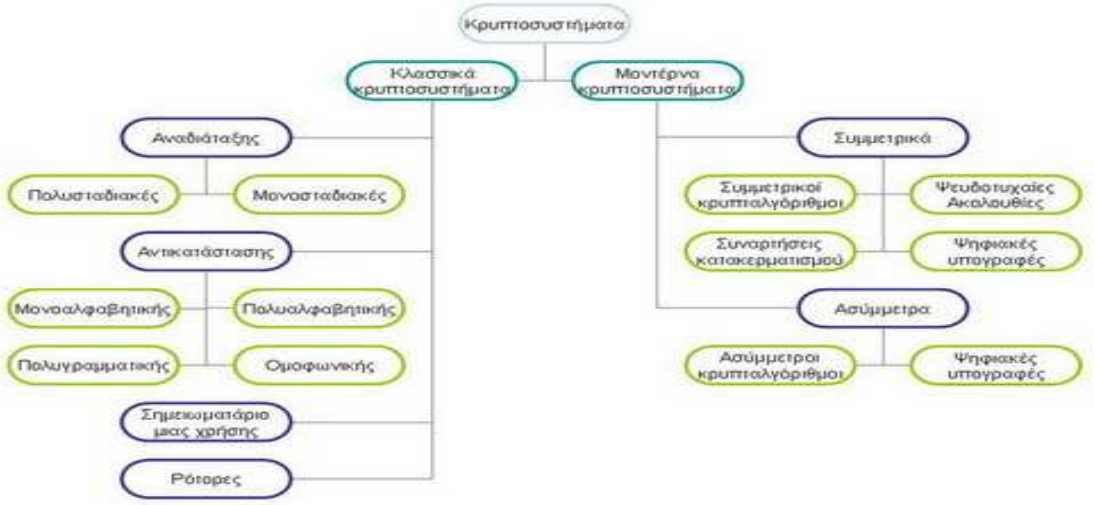
Ο αντίπαλος παρακολουθεί την επικοινωνία, ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση για την κλείδα που χρησιμοποιήθηκε και δεν μπορεί να αναδημιουργήσει το μήνυμα. Αν ο αντίπαλος επιλέξει να παρακολουθεί όλα τα μηνύματα θα προσανατολιστεί στην εξεύρεση του κλειδιού. Αν ο αντίπαλος ενδιαφέρεται μόνο για το υπάρχον μήνυμα θα παράγει μια εκτίμηση για την πληροφορία του μηνύματος.



Εικόνα 9: Μοντέλο Τυπικού Κρυπτοσυστήματος

3.1.4 Είδη Κρυπτοσυστημάτων

Υπάρχουν δύο μεγάλες κατηγορίες τα Κλασσικά Κρυπτοσυστήματα και τα Μοντέρνα Κρυπτοσυστήματα (Συμμετρικά κρυπτοσυστήματα και Ασύμμετρα κρυπτοσυστήματα).



Εικόνα 10: Είδη Κρυπτοσυστημάτων

3.1.4.1 Συμμετρικά Κρυπτοσυστήματα

Συμμετρικό κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά την διαδικασία της κρυπτογράφησης αποκρυπτογράφησης ένα κοινό κλειδί (Εικόνα 11). Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Εικόνα 11: Μοντέλο Συμμετρικού Κρυπτοσυστήματος

Τα στάδια της επικοινωνίας της εικόνας είναι τα ακόλουθα:

1. Ο Κώστας ή η Βασιλική αποφασίζει για ένα κλειδί το οποίο το επιλέγει τυχαία μέσα από τον κλειδοχώρο.
2. Η Βασιλική αποστέλλει το κλειδί στον Κώστα μέσα από ένα ασφαλές κανάλι.
3. Ο Κώστας δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
4. Κρυπτογραφεί το μήνυμα με το κλειδί που έλαβε από την Βασιλική και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται.
5. Η Βασιλική λαμβάνει την κρυπτοσυμβολοσειρά και στην συνέχεια με το ίδιο κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

Λίστα Συμμετρικών Κρυπταλγορίθμων

- Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

Δέσμης (Block Ciphers), οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.

Ροής (Stream Ciphers), οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να την διαχωρίζουν σε τμήματα.

a) **Συμμετρικοί Κρυπταλγόριθμοι Τμήματος** (Block Ciphers) :

Data Encryption Standard, 3-Way, Blowfish, CAST, CMEA, Triple-DES, DEAL FEAL, GOST, IDEA, LOKI, Lucifer, MacGuffin, Twofish

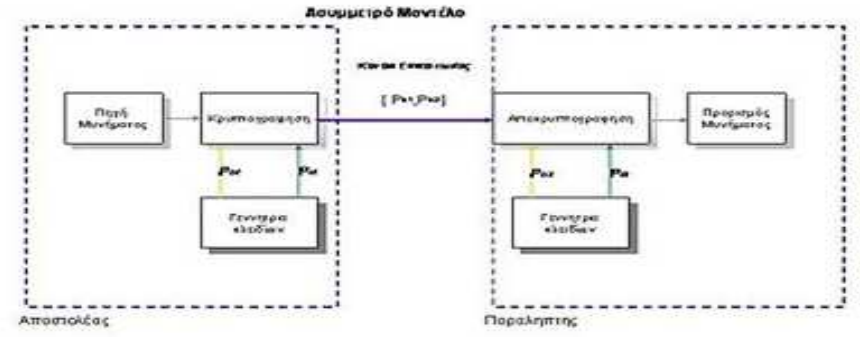
MARS, MISTY, MMB, NewDES, RC2, RC5, RC6 REDOC, Rijndael, Safer, Serpent, SQUARE, Skipjack, Tiny Encryption Algorithm

b) **Συμμετρικοί Κρυπταλγόριθμοι ροής** (Stream Ciphers) :

ORYX, RC4, SEAL

3.1.4.2 Ασύμμετρα Κρυπτοσυστήματα

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού (Κρυπτογράφηση Δημόσιου Κλειδιού) δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι : ότι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο .Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στην δημιουργία των ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) και στα Ψηφιακά πιστοποιητικά.



Εικόνα 12: Μοντέλο Ασύμμετρου Κρυπτοσυστήματος

Τα στάδια της επικοινωνίας της Εικόνας 12 είναι τα ακόλουθα:

1. Η γεννήτρια κλειδιών του Μένιου παράγει 2 ζεύγη κλειδιών,
2. Η γεννήτρια κλειδιών της Ελένης παράγει 2 ζεύγη κλειδιών
3. Η Ελένη και ο Μένιος ανταλλάσσουν τα δημόσια ζεύγη
4. Ο Μένιος δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
5. Κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί της Ελένης και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται
6. Η Ελένη λαμβάνει την κρυπτοσυμβολοσειρά και στην συνέχεια με το ιδιωτικό της κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

- **<u>Λίστα Ασύμμετρων Κρυπταλγορίθμων</u>**
  RSA, Ανταλλαγή κλειδιού Diffie–Hellman, DSA, Paillier, El Gamal, Κρυπτογραφία ελλειπτικών καμπυλών (ECC)

3.1.5 Συμμετρικοί Κρυπταλγόριθμοι Τμήματος

Η πλειοψηφία των συμμετρικών κρυπταλγορίθμων στις σύγχρονες εφαρμογές αποδίδεται σε κρυπταλγόριθμους τμήματος. Η σχετικά μεγαλύτερη ασφάλεια που παρέχουν οι κρυπταλγόριθμοι τμήματος έναντι των κρυπταλγορίθμων ροής καθιστούν τους κρυπταλγόριθμους τμήματος ως πρώτη επιλογή. Ωστόσο, σε εφαρμογές όπου η ταχύτητα έχει μεγαλύτερη

προτεραιότητα από την ασφάλεια, προτιμούνται οι κρυπταλγόριθμοι ροής. Ένας κρυπταλγόριθμος τμήματος είναι συνήθως μια επαναληπτική εφαρμογή μιας κρυπτογραφικής πράξης η οποία αποτελείται από μία ή περισσότερες κρυπτογραφικές συναρτήσεις, σε διάταξη τέτοια ώστε να επιτρέπεται η διαδοχική σύνδεση της πράξης αυτής με τον εαυτό της ή με διαφορετικές πράξεις.

Το αποτέλεσμα της σύνδεσης αυτής αποτελεί το κρυπτογραφικό γινόμενο, το οποίο υπό κατάλληλες συνθήκες μπορεί να καταστήσει ένα κρυπτοσύστημα ασφαλές. Το κάθε συστατικό του κρυπτογραφικού γινομένου αποτελεί το γύρο του κρυπταλγόριθμου. Σε κάθε γύρο τροφοδοτείται το αποτέλεσμα του προηγούμενου γύρου και το αντίστοιχο κλειδί του γύρου. Η ακολουθία των κλειδιών όλων των γύρων αποτελεί το πρόγραμμα κλειδιού και προκύπτει από κάποιο αρχικό κλειδί.

Στον πρώτο γύρο τροφοδοτείται το απλό κείμενο, ενώ το αποτέλεσμα του τελευταίου γύρου αποτελεί το κρυπτοκείμενο. Ο αριθμός των γύρων εξαρτάται από την κρυπτογραφική δύναμη του κάθε γύρου. Γενικά το κρυπτογραφικό γινόμενο δύο σχετικά αδύναμων κρυπτογραφικών πράξεων ισοδυναμεί σε μια κρυπτογραφική πράξη η οποία είναι κατά πολύ κρυπτογραφικά δυνατότερη από τις επιμέρους πράξεις. Σύμφωνα με τον Shannon, αυτό ονομάζεται φαινόμενο της χιονοστιβάδας (avalanche effect), όπου οι επιμέρους πράξεις μπορεί να παρουσιάζουν χαμηλή σύγχυση και διάχυση, αλλά το αποτέλεσμα του κρυπτογραφικού γινομένου ενισχύει σημαντικά τις ποσότητες των δύο αυτών χαρακτηριστικών.

3.1.5.1 Τρόποι και Μέθοδοι Κρυπτογράφησης

Οι τρόποι λειτουργίας (modes of operation) είναι τρόποι διασύνδεσης κρυπταλγόριθμων τμήματος, με στόχο την περαιτέρω αύξηση της κρυπτογραφικής δύναμης και την αποτελεσματικότερη απόκρυψη πιθανών υπολειμμάτων πληροφορίας του απλού κειμένου που μπορεί να υπάρχει στο κρυπτοκείμενο. Υπάρχουν τέσσερις τυποποιημένοι τρόποι λειτουργίας σύμφωνα με το πρότυπο FIPS 81, και αρκετοί μη τυποποιημένοι τρόποι λειτουργίας. Οι δύο από τους τέσσερις τυποποιημένους τρόπους λειτουργίας είναι:

- ηλεκτρονικό κωδικοβιβλίο (electronic codebook, ECB)
- κρυπταλγόριθμος αλυσιδωτού τμήματος (cipher block chaining, CBC)

3.1.5.1.1 Ηλεκτρονικό κωδικοβιβλίο, ECB

Ο τρόπος λειτουργίας ECB αποτελεί την ευθεία συνδεσμολογία όπου το απλό κείμενο τροφοδοτείται στον κρυπταλγόριθμο και το κρυπτοκείμενο προκύπτει από την έξοδο όπως φαίνεται στην Εικόνα 13. Η ονομασία του τρόπου αυτού προέρχεται από την αναπαράσταση του κρυπτοσυστήματος ως ένα μεγάλο βιβλίο το οποίο περιέχει όλα τα ζεύγη απλού κειμένου και κρυπτοκειμένου για κάθε κλειδί.

Έτσι για έναν κρυπταλγόριθμο τμήματος με μέγεθος απλού κειμένου και κρυπτοκειμένου n bits και μέγεθος κλειδιού k bits, μπορούμε να φανταστούμε ότι το βιβλίο περιέχει 2k κεφάλαια, ένα για το κάθε κλειδί, και το περιεχόμενο του κάθε κεφαλαίου θα αποτελούνταν από 2×2k καταχωρήσεις, οι μισές ταξινομημένες ως προς το απλό κείμενο, και οι υπόλοιπες ταξινομημένες ως προς το κρυπτοκείμενο.

Εικόνα 13: Τρόπος λειτουργίας ECB

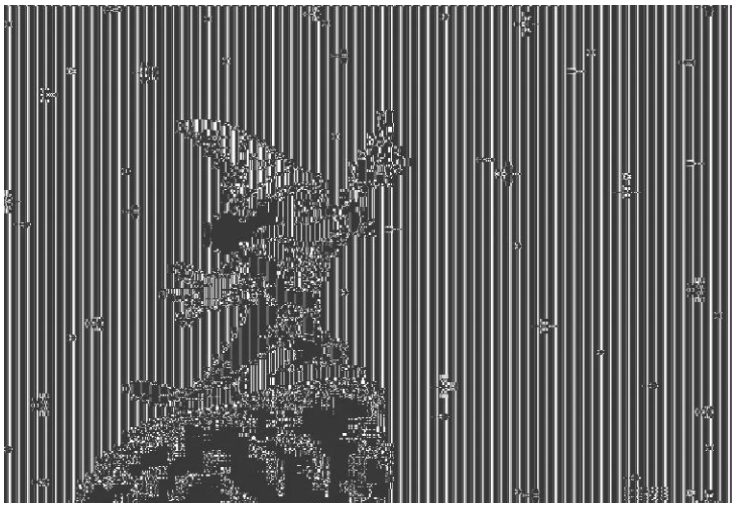
Το απλό κείμενο χωρίζεται σε τμήματα P = [p1p2…pl], όπου το κάθε τμήμα μεγέθους n bits τροφοδοτείται στον αλγόριθμο κρυπτογράφησης: ci = ek (pi) .

Η αναγκαία κατάτμηση του απλού κειμένου είναι και το μειονέκτημα της ECB λειτουργίας. Για όμοια τμήματα του απλού κειμένου, τα αντίστοιχα κρυπτοκείμενα που προκύπτουν είναι επίσης όμοια. Αυτό καθιστά την ECB ακατάλληλη για τις εφαρμογές στις οποίες υπάρχουν επαναλαμβανόμενα μοτίβα δεδομένων. Για παράδειγμα, στα δίκτυα ηλεκτρονικών υπολογιστών, τα δεδομένα που ανταλλάσσονται μεταξύ των υπολογιστών βασίζονται σε πρωτόκολλα επικοινωνίας τα οποία χρησιμοποιούν τυποποιημένα μηνύματα. Έτσι ο αντίπαλος είναι σε θέση να αναγνωρίζει τα
επαναλαμβανόμενα τμήματα του απλού κειμένου, καθώς και τις στιγμές κατά τις οποίες γίνεται η αλλαγή του κλειδιού κρυπτογράφησης. Αυτή η διαρροή της πληροφορίας για τις περισσότερες εφαρμογές δεν είναι επιτρεπτή.

Χαρακτηριστική περίπτωση της ακαταλληλότητας της χρήσης της ECB λειτουργίας είναι η κρυπτογράφηση των εικόνων, όπου τα μοτίβα είναι βασικά δομικά στοιχεία της δισδιάστατης απεικόνισης. Στην Εικόνα 14 φαίνεται μια εικόνα ως απλό κείμενο, και στην Εικόνα 15, η εικόνα υπέστη κρυπτογράφηση με τον κρυπταλγόριθμο τμήματος DES. Αν και τα ακριβή χαρακτηριστικά δεν είναι φανερά,

Εικόνα 14: Απλό κείμενο σε μορφή εικόνας

ο αντίπαλος είναι σε θέση να διακρίνει τα αντικείμενα τα οποία απαρτίζουν την εικόνα. Επιπλέον, αν ο αντίπαλος είχε συναντήσει στο παρελθόν την εικόνα αυτή (μη κρυπτογραφημένη), θα είναι σε θέση να συσχετίσει την «κρυπτοεικόνα» με την «απλή εικόνα». Επομένως, η κρυπτογραφική δύναμη του κρυπταλγόριθμου τμήματος δεν είναι σε θέση να επηρεάσει το αποτέλεσμα της συνολικής ασφάλειας του συστήματος, εφόσον υπάρχει μεγάλη ποσότητα επαναλαμβανόμενων μοτίβων στο απλό κείμενο.



Εικόνα 15: Κρυπτογραφημένη εικόνα με ECB

Συμπεραίνουμε λοιπόν ότι, η αναγκαία κατάτμηση σε συνδυασμό με το γεγονός ότι το κάθε τμήμα κρυπτογραφείται ανεξάρτητα από τα υπόλοιπα τμήματα του απλού κειμένου δίνει το πλεονέκτημα στον αντίπαλο να αναγνωρίσει με αφαιρετικό τρόπο το περιεχόμενο του απλού κειμένου. Οι τρόποι λειτουργίας που ακολουθούν έχουν στόχο να επιδιορθώσουν αυτό το μειονέκτημα.

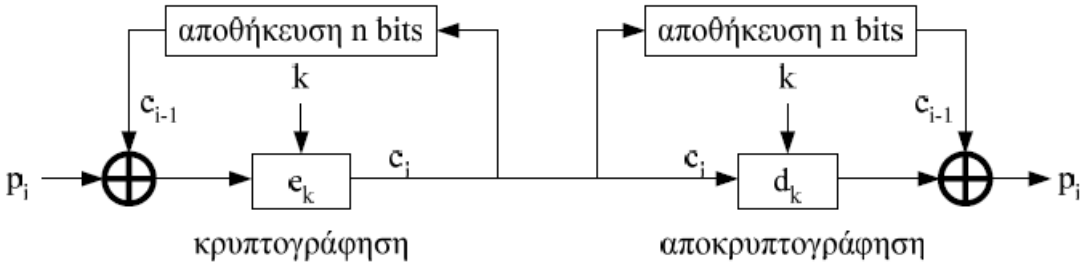
3.1.5.1.2 Κρυπταλγόριθμος αλυσιδωτού τμήματος, CBC

Η λειτουργία CBC παριστάνεται στην Εικόνα 16. Η κρυπτογράφηση ενός τμήματος του απλού κειμένου *pi* εξαρτάται και από το προηγούμενο τμήμα *pi*-1 με την ακόλουθη σχέση κρυπτογράφησης:

$$c_i = e_k(c_{i-1} \oplus p_i),$$

ενώ η αποκρυπτογράφηση ορίζεται από την:

$$p_i = d_k(c_i) \oplus c_{i-1}.$$



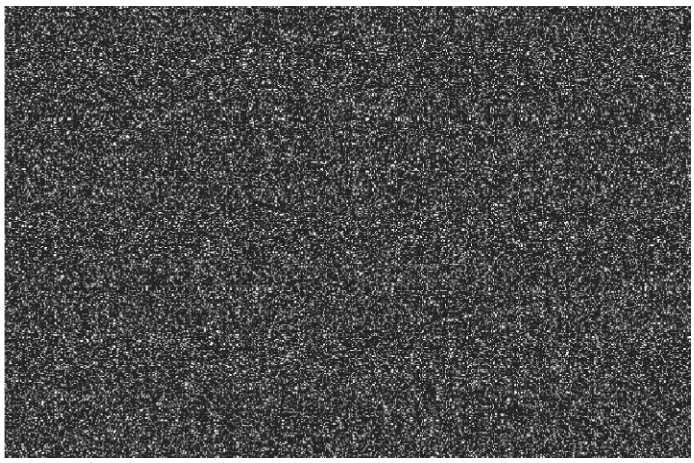
Εικόνα 16: Τρόπος λειτουργίας CBC

Η ορθότητα της σχέσης κρυπτογράφησης / αποκρυπτογράφησης είναι φανερή από:

$$p_i = d_k(c_i) \oplus c_{i-1} = c_{i-1} \oplus p_i \oplus c_{i-1} = (c_{i-1} \oplus c_{i-1}) \oplus p_i = p_i .$$

Μπορούμε να παρατηρήσουμε ότι η ποσότητα του κρυπτοκειμένου που εφαρμόζεται στην αποκλειστική διάζευξη είναι η ίδια τόσο στην πλευρά της κρυπτογράφησης, όσο και στην πλευρά της αποκρυπτογράφησης, και είναι αυτή που προκύπτει από την προηγούμενη κρυπτογράφηση.

Στην Εικόνα 17 παρουσιάζεται η Εικόνα 14 κρυπτογραφημένη με τον ίδιο κρυπταλγόριθμο DES, αλλά σε λειτουργία CBC. Τα επαναλαμβανόμενα μοτίβα που υπάρχουν στο απλό κείμενο δεν είναι πλέον φανερά στο κρυπτοκείμενο.



Εικόνα 17: Κρυπτογραφημένη εικόνα με CBC

Το αρχικό και το τελικό τμήμα

Για να καθορισθεί πλήρως η κρυπτογράφηση της λειτουργίας CBC, θα πρέπει να ορισθούν η αρχική τιμή c0, καθώς και το τελικό τμήμα του απλού κειμένου, στην περίπτωση που το μέγεθος του απλού κειμένου δεν είναι πολλαπλάσιο του n. Στην περίπτωση της κρυπτογράφησης του πρώτου τμήματος p1 είναι:

$$c_1 = e_k(c_0 \oplus p_1),$$

που σημαίνει ότι απαιτείται η ποσότητα c0. Αυτή η ποσότητα είναι το διάνυσμα αρχικοποίησης το οποίο θα πρέπει να είναι γνωστό τόσο κατά τη διαδικασία της κρυπτογράφησης, όσο και κατά τη διαδικασία της αποκρυπτογράφησης. Αν και η εμπιστευτικότητα του δεν είναι υποχρεωτική, αποτελεί κοινή πρακτική να στέλνεται στον αποδέκτη κρυπτογραφημένο με ECB.

Ένας δεύτερος λόγος που προτιμάται η κρυπτογραφημένη αποστολή του διανύσματος αρχικοποίησης, είναι η προστασία της ακεραιότητάς του, η οποία είναι σημαντικότερη από την εμπιστευτικότητα του διανύσματος. Η προστασία της ακεραιότητας πραγματοποιείται με τη χρήση συνάρτησης ακεραιότητας σε συνδυασμό με την κρυπτογράφηση ECB. Το διάνυσμα αρχικοποίησης διαιρείται σε δύο τμήματα, το πρώτο μήκους n-a bits και το δεύτερο μήκους a bits. Στο πρώτο τμήμα εφαρμόζεται κάποια μονόδρομη συνάρτηση hash, και τα πρώτα a bits του αποτελέσματος απαρτίζουν το δεύτερο τμήμα του διανύσματος. Με αυτόν τον τρόπο το δεύτερο τμήμα του διανύσματος αποτελεί τη σύνοψη του πρώτου τμήματος.

Στη συνέχεια το διάνυσμα κρυπτογραφείται και αποστέλλεται στον αποδέκτη. Ο αποδέκτης με τη σειρά του το αποκρυπτογραφεί και ελέγχει αν το δεύτερο τμήμα του διανύσματος είναι η σύνοψη του πρώτου. Στην περίπτωση που ο αντίπαλος προσβάλλει την ακεραιότητα του διανύσματος, αυτό θα γίνει αντιληπτό από τον αποδέκτη. Όσον αφορά το τελευταίο τμήμα του απλού κειμένου, υπάρχει το ενδεχόμενο το τμήμα αυτό να είναι μικρότερο του n. Αυτό συμβαίνει όταν το μέγεθος του κρυπτοκειμένου δεν είναι πολλαπλάσιο του n Στην περίπτωση αυτή προστίθενται μηδενικά στο τέλος, έως ότου το τμήμα έχει μέγεθος ίσο με n bits. Στις εφαρμογές στις οποίες τα δεδομένα ακολουθούν αυστηρή τυποποίηση και δεν είναι επιτρεπτό να συμπεριλαμβάνονται τα επιπλέον μηδενικά, τα τελευταία bits του τμήματος χρησιμοποιούνται για την καταγραφή του πλήθους των επιπρόσθετων μηδενικών. Για z μηδενικά, απαιτούνται log2(z) δυαδικές θέσεις.

3.1.6 Εφαρμογές Κρυπτογράφησης

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς

- Ασφάλεια συναλλαγών σε τράπεζες δίκτυα – ATM
- Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
- Σταθερή τηλεφωνία (cryptophones)
- Διασφάλιση Εταιρικών πληροφοριών
- Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
- Διπλωματικά δίκτυα (Τηλεγραφήματα)
- Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
- Ηλεκτρονική ψηφοφορία
- Ηλεκτρονική δημοπρασία
- Ηλεκτρονικό γραμματοκιβώτιο
- Συστήματα συναγερμών
- Συστήματα βιομετρικής αναγνώρισης
- Έξυπνες κάρτες

- Ιδιωτικά δίκτυα (VPN)

- World Wide Web
- Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
- Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)
- Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
- Τηλεδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

3.2 Ψηφιακή Υδατογράφηση

Η ψηφιακή υδατογράφηση, συνδυάζει δύο κομμάτια πληροφορίας, την πρωτότυπη και την προστιθέμενη (υδατογράφημα), ώστε να μπορούν να επεξεργαστούν ανεξάρτητα. Αυτή είναι και η διαφορά της από την κρυπτογραφία. Το watermarking αποτελεί την πιο σύγχρονη μέθοδο για την προστασία από την παράνομη αντιγραφή και χρήση εικόνων στο Internet.

Οι άνθρωποι από παλιά προσπαθούσαν να βρουν μεθόδους ώστε :

- Να μπορούν να μεταδίδουν πληροφορίες χωρίς να γίνονται αντιληπτοί από άλλους
- Αν γίνουν αντιληπτοί να είναι δύσκολο να ερμηνευθεί το μήνυμα
- Αν κλαπεί το μήνυμα ο παραβάτης να υφίσταται τις συνέπειες
- Να μπορούν να αποδείξουν την ιδιοκτησία τους.

Επομένως έχει ως στόχο την εξασφάλιση της εγκυρότητας ενός αντικειμένου, το αναμφισβήτητο της ταυτότητας του ιδιοκτήτη του και την αποκατάστασή του σε περίπτωση παραποίησης. Για το λόγο αυτό η ψηφιακή υδατογράφηση είναι ιδιαίτερα σημαντική για την μεταφορά ψηφιακών δεδομένων πολυμεσικού τύπου μέσω του παγκόσμιου ιστού.

Καθώς μεταφέρονται και παρουσιάζονται ψηφιακά δεδομένα μέσω του διαδικτύου, προκύπτει η ανάγκη για την χρήση ψηφιακών υδατογραφημάτων.

3.2.1 Τύποι Υδατογραφημάτων

Το υδατογράφημα είναι ένα σύνολο δυαδικών δεδομένων που προσαρτώνται στο ψηφιακό αντικείμενο του οποίου θέλουμε να προστατεύσουμε τα πνευματικά δικαιώματα. Τα ψηφιακά υδατογραφήματα θα μπορούσαν γενικά να χωριστούν σε δύο μεγάλες κατηγορίες, αυτά που γίνονται αντιληπτά από τον άνθρωπο (ορατά ψηφιακά υδατογραφήματα) και αυτά που δεν γίνονται αντιληπτά (αόρατα ψηφιακά υδατογραφήματα).

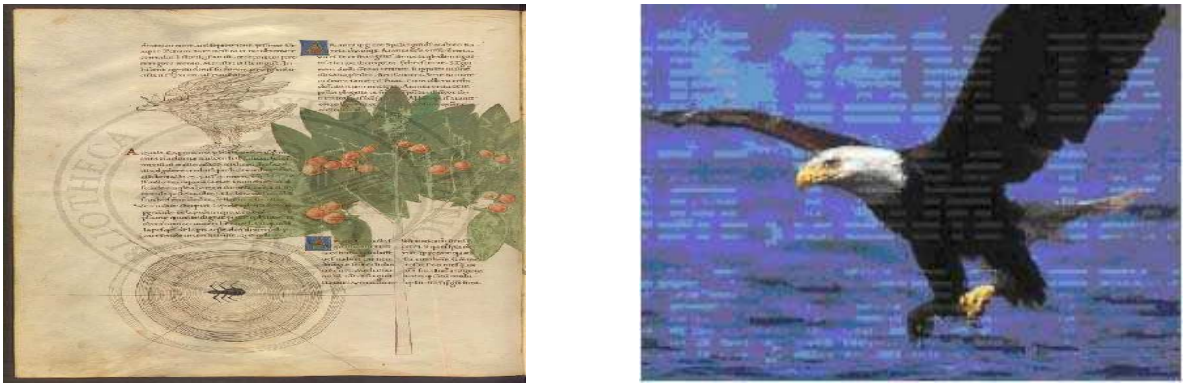
3.2.1.1 Ορατά Υδατογραφήματα

Τα ορατά ψηφιακά υδατογραφήματα χρησιμοποιούνται σχεδόν με τον ίδιο τρόπο όπως και οι πρόγονοί τους στο χαρτί, με στόχο την αναγνώριση της πηγής προέλευσης, την εξασφάλιση της ιδιοκτησίας και γιατί όχι, της διαφήμισης. Αφορούν στην ενσωμάτωση μιας ορατής εικόνας στο ψηφιακό τεκμήριο με τέτοιο τρόπο ώστε είναι ευδιάκριτη αλλά χωρίς να επηρεάζει την ποιότητα του περιεχομένου της αρχικής εικόνας.

Το υδατογράφημα έχει σκοπό να αποτρέψει την απομάκρυνση ή αντικατάστασή του, έτσι θα πρέπει να τοποθετηθεί κατάλληλα ώστε η απομάκρυνσή του να οδηγεί στην καταστροφή του αρχείου. Μπορεί να τοποθετηθεί με διάφορους τρόπους, επαναληπτικά σε όλη την εικόνα, δεξιά ή αριστερά, πάνω ή κάτω ή στο κέντρο της εικόνας. Τα ορατά ψηφιακά υδατογραφήματα

χρησιμοποιούνται για άμεση κατάδειξη του ιδιοκτήτη σε αντίθεση με τα αόρατα. Το βασικό τους πλεονέκτημα είναι ότι κατ' ουσίαν, περιορίζουν την εμπορική αξία του ψηφιακού αντικειμένου, χωρίς αυτό να χάνει τη χρησιμότητά του για νόμιμους και εξουσιοδοτημένους σκοπούς. Επομένως, τα ορατά ψηφιακά υδατογραφήματα πάνω σε ψηφιακά τεκμήρια, καθιστούν φανερό το γεγονός πως τα τεκμήρια αυτά ανήκουν σε κάποιον, χωρίς όμως αυτό να μειώνει την ανάγκη και την αξία της χρήσης τους.

Ένα ορατό υδατογράφημα μπορεί να λειτουργήσει είτε ως διαφήμιση είτε ως περιορισμός. Για παράδειγμα, αν ο ιδιοκτήτης επιθυμεί μπορεί να διαθέσει ελεύθερα χαμηλής ανάλυσης, ορατά υδατογραφημένες εικόνες, ώστε να παρέχει τις αμαρκάριστες εικόνες υψηλής ποιότητας για κάποιο αντίτιμο. Ακόμα κι αν τα αντίγραφα ήταν της ίδιας ανάλυσης, το ορατό υδατογράφημα θα αποθάρρυνε την παράνομη χρήση τους. Μία μέθοδος που θα έχει οικονομικό όφελος είναι η αναστρέψιμη υδατογράφηση. Η εικόνα υδατογραφείτε με ένα ορατό υδατογράφημα πριν από τη δωρεά διανομή της στο Internet. Στη συνέχεια το υδατογράφημα μπορεί να αφαιρεθεί για να ξαναδημιουργηθεί η αρχική εικόνα.

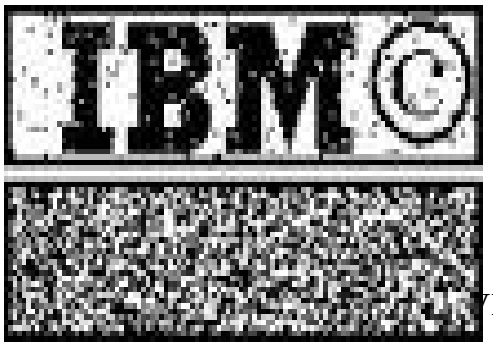


Εικόνα 18: Παραδείγματα με ορατό υδατογράφημα

3.2.1.2 Αόρατα Υδατογραφήματα

Τα αόρατα υδατογραφήματα αποτελούν δυαδική πληροφορία που ενσωματώνεται στην αρχική, αλλά παραμένει αόρατη και δεν την αλλοιώνει. Ο εντοπισμός αόρατου υδατογραφήματος σε ένα αρχείο γίνεται αλγοριθμικά, μέσω ειδικού συστήματος ανίχνευσης υδατογραφημάτων.

Παρακάτω παρουσιάζεται αριστερά μια υδατογραφημένη ψηφιακή εικόνα με το αόρατο υδατογράφημα πάνω δεξιά και δίπλα της το υδατογράφημα που προκύπτει από τη χρήση ενός συστήματος εντοπισμού υδατογραφημάτων και το αποτέλεσμα που δίνει το σύστημα για ένα κομμάτι της εικόνας που δεν περιέχει υδατογράφημα.



Εικόνα 19: Υδατογραφημένη με αόρατο υδατογράφημα

Εικόνα 20: Υδατογράφημα που προκύπτει

Τα αόρατα ψηφιακά υδατογραφήματα μπορούν να αποτρέψουν μια κλοπή-μη εξουσιοδοτημένη αντιγραφή, χρήση κ.τ.λ. μόνο όταν ο επίδοξος χρήστης έχει υποψία ότι το ψηφιακό τεκμήριο που πάει να κλέψει είναι υδατογραφημένο. Πέρα όμως από την ψυχολογική αποτροπή της παράνομης χρήσης, τα αόρατα ψηφιακά υδατογραφήματα προσδιορίζουν την πηγή, το δημιουργό, τον ιδιοκτήτη, τον εξουσιοδοτημένο χρήστη κ.τ.λ. ενός ψηφιακού τεκμηρίου. Έτσι, στόχο αποτελεί η μόνιμη και χωρίς δυνατότητα τροποποίησης, ενσωμάτωση πληροφοριών στα ψηφιακά τεκμήρια.

Σε πολλές περιπτώσεις πάντως, και οι δύο τύποι ψηφιακών υδατογραφημάτων αποδεικνύονται εξίσου αποτελεσματικοί. Πολλές εταιρείες μάλιστα, αναπτύσσουν λογισμικά τα οποία θέτουν πράκτορες (agents) υδατογραφημάτων σε «περιπολίες» στο διαδίκτυο με στόχο τον εντοπισμό μη εξουσιοδοτημένης χρήσης ψηφιακά υδατογραφημένων τεκμηρίων. Αξίζει εδώ να σημειωθεί πως τα λογισμικά υδατογράφησης αποδίδουν ένα μοναδικό υδατογράφημα σε κάθε ψηφιακό τεκμήριο για κάθε εξουσιοδοτημένο χρήστη.

Τα αόρατα υδατογραφήματα διακρίνονται σε εύθραυστα και ανθεκτικά. Τα εύθραυστα υδατογραφήματα δεν επιβιώνουν από ανεπιθύμητους μετασχηματισμούς στα αρχικά δεδομένα και επιτρέπουν τον έλεγχο ακεραιότητας τους και την ανίχνευση των μεταβολών. Αντίθετα, τα ανθεκτικά υδατογραφήματα διατηρούνται τόσο μετά από κοινές ενέργειες επεξεργασίας εικόνας, όσο και μετά από κακόβουλες επιθέσεις, όπως η συμπίεση, η χρήση φίλτρων, οι γεωμετρικές μετατροπές της εικόνας και άλλες μέθοδοι. Τα ανθεκτικά υδατογραφικά σχήματα διακρίνονται περαιτέρω σε «ενημερωμένα» (non-blind watermarking schemes) και «μη ενημερωμένα» (blind).

Τα «ενημερωμένα» σχήματα προϋποθέτουν τη γνώση των αρχικών δεδομένων για την εξαγωγή του υδατογραφήματος και χαρακτηρίζονται από μεγαλύτερη ανθεκτικότητα σε επιθέσεις. Στα «μη ενημερωμένα» ή «τυφλά» υδατογραφικά σχήματα η εξαγωγή του υδατογραφήματος δεν απαιτεί πρόσβαση στα αρχικά μη υδατογραφημένα δεδομένα, παρά μόνο γνώση ενός κλειδιού. Οι τεχνικές αυτές χωρίζονται σε δύο κατηγορίες τις τεχνικές που εφαρμόζονται στο πεδίο του χώρου /χρόνου (spatial/time domain) και εκείνες που χρησιμοποιούν κάποιο πεδίο μετασχηματισμού (transform domain).

Η πρώτη κατηγορία ενσωματώνει το υδατογράφημα στο πεδίο του χώρου (pixels) ή του χρόνου ενώ η δεύτερη κατηγορία χρησιμοποιεί μετασχηματισμένες μορφές των αρχικών δεδομένων, που προκύπτουν από τους διακριτούς μετασχηματισμούς Fourier (DFT), συνημίτονου (DCT), wavelet (DWT) κλπ.

3.2.2 Εφαρμογές Ψηφιακής Υδατογράφησης

Η ψηφιακή υδατογράφηση μπορεί να χρησιμοποιηθεί σε πολλές εφαρμογές στις οποίες χρειάζεται ενσωμάτωση πληροφορίας σε κάποια δεδομένα. Σε αρκετές περιπτώσεις

χρησιμοποιούνται διαφορετικές τεχνικές για την ενσωμάτωση δεδομένων. Παρόλο που οι τεχνικές αυτές παραμένουν ιδιαίτερα δημοφιλείς στην προσπάθεια κατοχύρωσης της πνευματικής ιδιοκτησίας (copyright), η κλίμακα των εφαρμογών τους συνεχώς διευρύνεται, περιλαμβάνοντας επίσης τον έλεγχο ακεραιότητας δεδομένων, την πιστοποίηση αποστολέα και παραλήπτη και την παρακολούθηση μετάδοσης δεδομένων. Αναλυτικότερα παρατίθενται παρακάτω οι εφαρμογές υδατογράφησης.

3.2.2.1 Προστασία Πνευματικών Δικαιωμάτων

Στις μέρες μας υπάρχει εκτενείς βιβλιογραφία και ευρεία χρήση υδατογραφημάτων για την ενσωμάτωση στοιχείων πνευματικής ιδιοκτησίας. Μέχρι πρόσφατα ο μόνος τρόπος προστασίας των πνευματικών δικαιωμάτων ήταν η κρυπτογραφία, της οποίας το βασικό μειονέκτημα είναι ότι δεν παρέχει προστασία στα δεδομένα από τη στιγμή της αποκρυπτογράφησης τους. Οι τεχνικές

υδατογράφησης συμπληρώνουν την κρυπτογραφία, αφού ενσωματώνουν στα αρχικά δεδομένα ένα υδατογράφημα που κατοχυρώνει την πνευματική ιδιοκτησία και δεν μπορεί να αποσπαστεί εύκολα ή η αφαίρεση του προκαλεί την υποβάθμιση της ποιότητας των αρχικών δεδομένων έτσι ώστε να χάνουν την αξία τους και να μην μπορούν να χρησιμοποιηθούν από επίδοξους «πειρατές». Συνεπώς, η εφαρμογή της προστασίας των πνευματικών δικαιωμάτων απαιτεί πολύ υψηλή ευρωστία ώστε να λειτουργεί σωστά και να έχει τα αναμενόμενα αποτελέσματα.

Στην εικόνα, μια γραπτή επισήμανση πνευματικών δικαιωμάτων μειονεκτεί σε σχέση με τη χρήση ενός μη αντιληπτού υδατογραφήματος το οποίο δεν αλλοιώνει το αισθητικό αποτέλεσμα και επίσης εξαλείφεται δύσκολα. Αντίθετα η γραπτή επισήμανση καλύπτει συνήθως ένα άκρο της εικόνας και αφαιρείται εύκολα. Επομένως, συμπεραίνουμε πως τα υδατογραφήματα είναι μια αρκετά αξιόπιστη και ασφαλής μέθοδος όσο αφορά την προστασία των πνευματικών δικαιωμάτων.

3.2.2.2 Ανίχνευση Συναλλαγών

Μια άλλη εφαρμογή της υδατογράφησης που έχει σχέση με την πάταξη της πειρατείας είναι η ταυτοποίηση του παραλήπτη μέσω της εμφύτευσης ειδικών αναγνωριστικών κωδικών και χρονικής σφραγίδας (time-stamp) στα ψηφιακά δεδομένα που προορίζονται για πώληση ή διανομή. Η πληροφορία που παρέχεται σχετικά με το νόμιμο παραλήπτη επιτρέπει τον εντοπισμό μεμονωμένων αντιγράφων του υλικού που έχουν διανεμηθεί παράνομα και την αναγνώριση του νόμιμου αγοραστή που ευθύνεται για την πειρατεία.

Στις εφαρμογές ανίχνευσης συναλλαγών το υδατογράφημα ενσωματώνεται στα αντίγραφα του ψηφιακού υλικού και καταγράφει τις συναλλαγές που έχουν γίνει σε αυτά. Η ενσωμάτωση του γίνεται είτε κατά τη διανομή του ψηφιακού αντικειμένου σε κάποιο πελάτη είτε κατά την αναπαραγωγή του αντικειμένου με αποτέλεσμα την μικρότερη επιβάρυνση του παρόχου του υλικού. Σε κάθε νόμιμη πώληση ή διανομή καταγράφεται ανά ξεχωριστό υδατογράφημα το οποίο χαρακτηρίζει τον κάθε νόμιμο παραλήπτη έτσι ώστε εάν το υλικό διαρρεύσει να μπορεί να εντοπιστεί η ταυτότητα του τελικού διανομέα των ψηφιακών αντικειμένων.

Ο χρήστης που διανέμει παράνομα το υλικό καλείται προδότης (traitor) και ο χρήστης που λαμβάνει το αντίγραφο καλείται πειρατής (pirate). Ο τύπος εφαρμογών ανίχνευσης των συναλλαγών καλείται επίσης ψηφιακό δαχτυλικό αποτύπωμα (fingerprinting) διότι ενσωματώνεται ένα διαφορετικό υδατογράφημα σε κάθε αντίγραφο που διανέμεται. Παραπέμπει έτσι στα ανθρώπινα δαχτυλικά αποτυπώματα που είναι ξεχωριστά στον κάθε ένα.

Εξαιτίας των επιθέσεων που μπορεί να συμβούν τα συστήματα ανίχνευσης συναλλαγών πρέπει να χαρακτηρίζονται από ασφάλεια και μεγάλη ανθεκτικότητα. Σε πολλές εφαρμογές απαιτείται η εξαγωγή του υδατογραφήματος να είναι εύκολη και με μικρή πολυπλοκότητα, όπως για παράδειγμα σε διαδικτυακές εφαρμογές όπου ειδικές μηχανές αναζήτησης (web crawlers) αναζητούν παράνομες υδατογραφημένες εικόνες.

3.2.2.3 Επισήμανση Χαρακτηριστικών (Feature Tagging)

Η υδατογράφηση επιτρέπει την ενσωμάτωση πληροφορίας όπως για παράδειγμα επικεφαλίδες, σχόλια, σε συγκεκριμένες περιοχές στην εικόνα. Η επισήμανση των χαρακτηριστικών τονίζει τα σημαντικά στοιχεία της εικόνας και δίνει επιπλέον βοηθητική πληροφορία στους εξουσιοδοτημένους χρήστες. Η προσθήκη επικεφαλίδων (captioning) και σχολίων (annotation) απευθείας στις εικόνες εξασφαλίζει τη μόνιμη σύνδεση των απεικονιζόμενων αντικειμένων με τη σχετική πληροφορία, χωρίς τον κίνδυνο απώλειας της πληροφορίας σε περίπτωση αλλαγής μορφοποίησης (format) του αρχείου και χωρίς περιττές απαιτήσεις σε μνήμη και εύρος ζώνης.

Τα υδατογραφήματα επισήμανσης χαρακτηριστικών δεν απειλούνται τις περισσότερες φορές από απόπειρες αλλοίωσης του, όμως υπάρχει πάντα ο κίνδυνος να τροποποιηθούν ενέργειες επεξεργασίας των εικόνων όπως από την κλιμάκωση ή την κοπή.

3.2.2.4 Μυστική Επικοινωνία (Data Hiding)

Υπάρχουν περιπτώσεις όπου η κρυπτογραφία αντενδείκνυται, όπως στην ανεπιθύμητη γνωστοποίηση της ύπαρξης επικοινωνίας μεταξύ δύο μερών, καθώς η μετάδοση κρυπτογραφημένου μηνύματος δημιουργεί υποψίες σχετικά με τη διακινούμενη πληροφορία. Η στεγανογραφία επιτρέπει την μυστική επικοινωνία προστατεύοντας τα επικοινωνούντα μέλη καθώς και τα μηνύματα τους από τον ανεπιθύμητο έλεγχο.

Το ενσωματωμένο σήμα χρησιμοποιείται για την ανταλλαγή μυστικής πληροφορίας μεταξύ δύο ατόμων, χωρίς να γνωρίζει κανείς άλλος για την μετάδοση.

3.2.2.5 Πιστοποίηση Αυθεντικότητας Δεδομένων (Data Authentication)

Ο έλεγχος της αυθεντικότητας των δεδομένων αποτελεί μια δημοφιλή εφαρμογή της υδατογράφησης τα τελευταία χρόνια τα «εύθραυστα» υδατογραφήματα δίνουν πληροφορίες σχετικά με το αν και ποια τμήματα έχουν υποστεί μεταβολές σε τυχόν τροποποιήσεις των δεδομένων που τα εμπεριέχουν. Τα υδατογραφήματα ελέγχου ακεραιότητας δεδομένων απαιτούν εξ ορισμού τον μικρότερο βαθμό ανθεκτικότητας.

Μια συνηθισμένη προσέγγιση είναι οι ψηφιακές υπογραφές που προέρχονται από τον κλάδο της κρυπτογραφίας. Στη μέθοδο αυτή χρησιμοποιείται ένα ασύμμετρο κλειδί κρυπτογράφησης το οποίο είναι διαφορετικό από το κλειδί για την αποκρυπτογράφηση της υπογραφής, και τα κλειδιά αυτά είναι γνωστά μόνο σε εξουσιοδοτημένους χρήστες. Στην περίπτωση που το ψηφιακό αντικείμενο καταλήξει σε κάποιο κακόβουλο χρήστη και ο οποίος το τροποποιήσει, οι εξουσιοδοτημένοι χρήστες συγκρίνουν την αρχική υπογραφή με αυτή που προκύπτει από το

ληφθέν μήνυμα και ανακαλύπτουν ότι οι ψηφιακές υπογραφές δεν ταιριάζουν και συνεπώς την παραποίηση.

Το μειονέκτημα των ψηφιακών υπογραφών είναι ότι μπορούν εύκολα να αφαιρεθούν η να χαθούν. Για παράδειγμα, όταν σε μια εικόνα η οποία περιέχει κάποια ψηφιακή υπογραφή, αλλάξει ο τύπος του αρχείου, θα έχει ως αποτέλεσμα την απώλεια της υπογραφής γιατί είναι πιθανόν να καταλαμβάνει αρκετό από το χώρο του νέου αρχείου. Μια αποδοτικότερη λύση είναι η ενσωμάτωση της υπογραφής στα αρχικά δεδομένα με τεχνικές ψηφιακής υδατογράφησης. Η υπογραφή αυτή αναφέρεται ως «σημάδι πιστοποίησης» (authentication mark). Η εισαγωγή τους εξασφαλίζει την μόνιμη σύνδεση της υπογραφής με τα αντίστοιχα δεδομένα. Το υδατογράφημα που θα ενσωματωθεί δεν πρέπει να προκαλεί παραποιήσεις στο αρχείο γιατί τότε δεν θα μπορεί να συγκριθεί με την ψηφιακή υπογραφή και έτσι το ψηφιακό αντικείμενο θα θεωρείται μη αυθεντικό. Αυτό λύνεται με την διάσπαση των δεδομένων σε δύο τμήματα: ένα τμήμα όπου δημιουργείται η ψηφιακή υπογραφή και ένα τμήμα στο οποίο ενσωματώνεται η υπογραφή.

Στις εφαρμογές πιστοποίησης αυθεντικότητας χρησιμοποιούνται τα εύθραυστα υδατογραφήματα (fragile watermarks), των οποίων το χαρακτηριστικό είναι η περιορισμένη ανθεκτικότητα έναντι σε παραποιήσεις του υλικού στο οποίο έχει ενσωματωθεί. Αν το υλικό περιέχει ένα εύθραυστο υδατογράφημα, τότε όταν κάποιος χρήστης εφαρμόσει αλλαγές στο υλικό θα τροποποιηθεί μαζί και το υδατογράφημα. Έτσι οι χρήστες του νέου παραποιημένου υλικού θα είναι σε θέση να εντοπίσουν το τροποποιημένο υδατογράφημα και να καταλάβουν πως το ψηφιακό αντικείμενο δεν είναι το αυθεντικό, αλλά κάποιο αντίγραφό του που έχει μετατραπεί. Αντίθετα, σε εφαρμογές όπου ενδιαφέρει το αν έγιναν πιο ουσιαστικές αλλαγές, όπως προσθήκη ή αφαίρεση

κάποιου αντικειμένου από την εικόνα, ενδείκνυται η χρήση των «ημι-εύθραυστων» υδατογραφημάτων (semi-fragile watermarks) τα οποία είναι ανθεκτικά σε δευτερεύουσας σημασίας μετατροπές, όπως στην περίπτωση συμπίεσης ενός αρχείου αλλά αλλοιώνονται από μεγαλύτερες αλλαγές στα δεδομένα του αρχείου.

Υπάρχουν όμως και περιπτώσεις όπου ενδιαφέρουν υδατογραφήματα τα οποία περιέχουν πληροφορίες για χαρακτηριστικά των δεδομένων, όπως ο μέσος όρος των blocks του αντικειμένου ή τα χαρακτηριστικά των ακμών του αντικειμένου. Εδώ ελέγχεται εάν κάποιο αντίγραφο του υλικού έχει τα ίδια χαρακτηριστικά με το πρωτότυπο. Συνεπώς στις εφαρμογές αυτές τα υδατογραφήματα θα πρέπει να είναι ανθεκτικά έναντι σε παραποιήσεις των αρχικών δεδομένων.

Κάποιες φορές χρειάζεται να γνωρίζουμε τι είδους αλλαγές έχουν γίνει σε κάποιο αντίγραφο ενός αντικειμένου. Για παράδειγμα, μπορεί κάποια εικόνα να έχει τμηματοποιηθεί σε blocks και κάθε ένα από αυτά να έχει το δικό του χαρακτηριστικό πιστοποίησης αυθεντικότητας. Έτσι, συγκρίνοντας τις ψηφιακές υπογραφές σε κάθε block μπορεί να διαπιστωθεί ποια έχουν παραποιηθεί και ποια είναι αυθεντικά.

3.2.3 Στόχοι Ψηφιακής Υδατογράφησης

Κατά τον σχεδιασμό των υδατογραφημάτων θα πρέπει να ληφθούν υπόψην κάποια χαρακτηριστικά, τα οποία είναι απαραίτητα για την αποτελεσματικότητά τους. Τα πιο σημαντικά είναι τα εξής:

1. Αξιοπιστία (robustness), πρέπει να αντιστέκονται σε ψηφιακές επιθέσεις που έχουν ως στόχο τη διαγραφή, την αλλαγή ή την αντικατάστασή τους παράνομα.

2. Δυνατότητα αποκωδικοποίησης (decodability), σε αόρατα υδατογραφήματα πρέπει να μπορούν να εντοπιστούν από τις αρμόδιες αρχές ακόμα κι όταν δεν είναι ορατά για το κοινό χρήστη.
3. Ελεγχόμενο μέγεθος. Το μέγεθος του υδατογραφήματος δεν μπορεί να είναι ανεξέλεγκτο. Όσο πιο μεγάλο είναι το μέγεθός του τόσο πιο δύσκολα ανακτάται.
4. Μη αποτροπή χρήσης (unobtrusiveness), και τα ορατά και τα αόρατα υδατογραφήματα πρέπει να είναι έτσι σχεδιασμένα, ώστε να μην αποτρέπουν τους χρήστες από την χρήση του υλικού που τα περιέχει.
5. Επιμονή (persistence).τα ψηφιακά υδατογραφήματα πρέπει να εξακολουθούν να υφίστανται σ' ένα ψηφιακό τεκμήριο, ακόμα κι αν αυτό τροποποιείται (π.χ. αλλαγή χρωμάτων των εικόνων, φιλτράρισμα, συμπίεση κ.τ.λ.).
6. Ανάκτηση υδατογραφήματος. Χρειάζονται μέθοδοι που να επιτρέπουν την ανάκτηση του, χωρίς την ανάγκη σύγκρισης με το αρχικό τεκμήριο.
7. Το υδατογράφημα δεν θα πρέπει να επηρεάζει την ποιότητα των αρχικών δεδομένων ώστε να μην τα υπερκαλύπτει
8. Το υδατογράφημα δεν θα πρέπει να μπορεί να αφαιρεθεί. Στη περίπτωση αφαίρεσής του το ψηφιακό αντικείμενο δεν είναι σωστά προστατευμένο.
9. Το υδατογράφημα θα πρέπει να επαναλαμβάνει την πληροφορία. Πρέπει να εισάγεται μικρή ποσότητα πληροφορίας η οποία να τοποθετείται σε περισσότερο από ένα μέρη του ψηφιακού αντικειμένου. Έτσι γίνεται δυσκολότερη η αφαίρεση του υδατογραφήματος.

3.2.4 Στάδια Υδατογράφησης

Υπάρχουν τρία στάδια κατά την υδατογράφηση οποιουδήποτε ψηφιακού τεκμηρίου και αυτά είναι τα εξής:

- Στο στάδιο της εισαγωγής ή ενσωμάτωσης (Embedding), το σύστημα δέχεται σαν εισόδους το υδατογράφημα και κάποιο κλειδί και δίνει σαν έξοδο το υδατογραφημένο περιεχόμενο.

- Στο στάδιο της επίθεσης (Attacking), επιχειρείται κάποια μετατροπή στο υδατογράφημα κατά την μετάδοση του υδατογραφημένου περιεχομένου. Η επίθεση αυτή συνήθως έχει σκοπό την τροποποίηση του υδατογραφήματος για την παραβίαση της προστασίας των πνευματικών δικαιωμάτων.
- Στο στάδιο της ανίχνευσης ή εντοπισμού (Detection ή Extraction), το υδατογράφημα, εάν δεν τροποποιήθηκε κατά τη μετάδοση του, μπορεί να εξαχθεί σωστά από το υδατογραφημένο περιεχόμενο. Οι ανθεκτικές εφαρμογές αναπαράγουν σωστά το υδατογράφημα, ακόμα και όταν αυτό έχει τροποποιηθεί αρκετά ενώ οι εύθραυστες αποτυγχάνουν σε αυτές τις περιπτώσεις. Το σύστημα ανίχνευσης δέχεται σαν είσοδο το υδατογραφημένο περιεχόμενο, το κλειδί και ανάλογα με την μέθοδο, το αρχικό περιεχόμενο ή το υδατογράφημα. Η έξοδος είναι το υδατογράφημα που ανιχνεύτηκε.

3.2.5 Ιδιότητες Υδατογράφησης

Οι ιδιότητες ψηφιακής υδατογράφησης αναφέρονται στην ανθεκτικότητα των συστημάτων σε κακόβουλες επιθέσεις, στην πολυπλοκότητα που χαρακτηρίζει της μεθόδους τους, καθώς και στην χωρητικότητα που διαθέτουν. Η σημασία της κάθε ιδιότητας εξαρτάται από τις απαιτήσεις της εφαρμογής. Οι ιδιότητες χωρίζονται σε εκείνες που σχετίζονται με τη διαδικασία της ενσωμάτωσης

του υδατογραφήματος, τη διαδικασία ανίχνευσης του υδατογραφήματος και με την ασφάλεια των συστημάτων.

3.2.5.1 Ευρωστία (Robustness)

Η ευρωστία αναφέρεται στη δυνατότητα ανίχνευσης του υδατογραφήματος που βρίσκεται σε κάποιο ψηφιακό αντικείμενο έπειτα από κακόβουλες επιθέσεις ή από διάφορες διαδικασίες επεξεργασίας των αρχικών δεδομένων. Τέτοιου είδους διαδικασίες επεξεργασίας αποτελούν στη περίπτωση των εικόνων: προσθήκη θορύβου, γραμμικό και μη γραμμικό φιλτράρισμα, κοπή, συμπίεση με απώλεια, και γεωμετρικοί μετασχηματισμοί (περιστροφή, κλιμάκωση κτλ), μετατροπή από αναλογική σε ψηφιακή μορφή και αντίστροφα.

Η ευρωστία δεν είναι απαραίτητο να υπάρχει για όλες τις παραπάνω επεξεργασίες σε κάθε εφαρμογή. Σε ορισμένες εφαρμογές όχι μόνο δεν είναι απαραίτητη η ύπαρξη της, αλλά πρέπει να αποφεύγεται, όπως για παράδειγμα στα «εύθραυστα» υδατογραφήματα τα οποία έχουν σαν χαρακτηριστικό τους την περιορισμένη ευρωστία. Από την άλλη μεριά υπάρχουν μέθοδοι οι οποίες καθιστούν τα υδατογραφήματα ανθεκτικά. Οι μέθοδοι αυτές χωρίζονται σε δύο κατηγορίες: η πρώτη κατηγορία περιλαμβάνει στρατηγικές οι οποίες χρησιμοποιούνται για την αποφυγή τροποποιήσεων στο υδατογράφημα, ενώ η δεύτερη κατηγορία περιλαμβάνει στρατηγικές οι οποίες επιτρέπουν τις τυχόν τροποποιήσεις στο υδατογράφημα με σκοπό τους την αντιστροφή των ενεργειών τους αυτών.

3.2.5.2 Χωρητικότητα (Capacity)

Η χωρητικότητα ή αλλιώς «φορτίο» δεδομένων (data payload) ορίζεται ως η ποσότητα της πληροφορίας που μπορεί να ενσωματωθεί, δηλαδή ο αριθμός των bits που υπάρχουν στο υδατογράφημα στη μονάδα του χρόνου ή ανά πακέτο δεδομένων. Για εικόνες, η χωρητικότητα αναφέρεται στον αριθμό των bits του υδατογραφήματος που μπορεί να ενσωματωθεί στην εικόνα. Ένα υδατογράφημα κωδικοποιεί N-bits, ενσωματώνει 2^N κρυφά μηνύματα. Η μεγαλύτερη χωρητικότητα επιτρέπει τη χρήση ενός ψηφιακού αντικειμένου μικρότερου μεγέθους για την ενσωμάτωση συγκεκριμένου μηνύματος, γεγονός που συνεπάγεται μείωση του απαιτούμενου εύρους μετάδοσης.

3.2.5.3 Διαφάνεια (Transparency)

Η ενσωμάτωση ενός υδατογραφήματος είναι μία διαδικασία που προσθέτει θόρυβο στα αρχικά δεδομένα και είναι απαραίτητο να γίνεται χωρίς την υποβάθμιση της ποιότητας του ψηφιακού αντικειμένου. Η διαφάνεια είναι πολύ σημαντική σε πολλές εφαρμογές, όπως σε περιπτώσεις κατοχύρωσης πνευματικών δικαιωμάτων. Η διαφάνεια ορίζεται επίσης ως «πιστότητα» (fidelity), δηλώνοντας την ομοιότητα ανάμεσα στα αρχικά και στα υδατογραφημένα δεδομένα.

3.2.5.4 Αποτελεσματικότητα Ενσωμάτωσης (Embedding Effectiveness)

Η αποτελεσματικότητα της ενσωμάτωσης ορίζεται ως η πιθανότητα η έξοδος του συστήματος ενσωμάτωσης να είναι ένα υδατογραφημένο περιεχόμενο. Τα συστήματα αυτά έχουν αποτελεσματικότητα μικρότερη από 100% αποτελούν την ιδανική πιθανότητα. Ανάλογα με την εφαρμογή μπορεί να προτιμηθεί η μείωση της αποτελεσματικότητας προκειμένου να επιτευχθεί

καλύτερη απόδοση των υπόλοιπων χαρακτηριστικών του συστήματος, αφού η πολύ υψηλή αποτελεσματικότητα που αγγίζει το 100% έχει πολύ υψηλό κόστος.

3.2.5.5 Τυφλή, Σχεδόν Τυφλή και Ενημερωμένη Ανίχνευση (Blind, Semi Blind and Informed Detection)

Τα συστήματα υδατογράφησης χωρίζονται σε δύο κατηγορίες ανάλογα με το αν χρησιμοποιούνται ή όχι τα αρχικά δεδομένα κατά την ανίχνευση του υδατογραφήματος. Τα συστήματα τυφλής ανίχνευσης δεν χρειάζονται καμία πληροφορία των αρχικών δεδομένων για τον εντοπισμό του υδατογραφήματος και ο αντίστοιχος ανιχνευτής καλείται «τυφλός ανιχνευτής» (blind detector). Τα συστήματα σχεδόν τυφλής ανίχνευσης χρειάζονται το υδατογράφημα. Τα συστήματα ενημερωμένης ανίχνευσης χρησιμοποιούν τα αρχικά δεδομένα ή ένα μέρος τους για την ανίχνευση υδατογραφήματος. Ο αντίστοιχος ανιχνευτής καλείται «ενημερωμένος ανιχνευτής» (informed detector).

Το είδος της ανίχνευσης εξαρτάται πάντα από το είδος της εφαρμογής που υλοποιεί. Για παράδειγμα, σε εφαρμογές ανίχνευσης συναλλαγών (transaction tracking) χρησιμοποιείται συνήθως ενημερωμένη ανίχνευση. Ο κάτοχος του υλικού χρησιμοποιεί τον ανιχνευτή για τον εντοπισμό παράνομων διανομών, ο οποίος έχει το αυθεντικό μη υδατογραφημένο υλικό και το χρησιμοποιεί μαζί με το παράνομο αντίγραφο. Αντίθετα, σε μία εφαρμογή έλεγχου αντιγράφων (copy control), ο ανιχνευτής πρέπει να διανεμηθεί σε όλους τους πελάτες μαζί με τη συσκευή αντιγραφής.

Τα συστήματα που χρησιμοποιούν ενημερωμένη ή τυφλή ανίχνευση ορίζονται επίσης ως «ιδιωτικά» ή «δημόσια» υδατογραφικά συστήματα αντίστοιχα.

3.2.5.6 Ρυθμός Ψευδώς Θετικών (False Positive Rate)

Ο όρος ρυθμός ψευδώς θετικών ορίζεται ως η πιθανότητα που υπάρχει στη διαδικασία ανίχνευσης να εντοπιστεί κάποιο υδατογράφημα στην περίπτωση όπου στην πραγματικότητα δεν υπάρχει. Η σημασία της πιθανότητας αυτής εξαρτάται από το είδος της εφαρμογής, αλλά θα πρέπει να είναι πολύ μικρή στα περισσότερα συστήματα υδατογράφησης.

Για τον υπολογισμό της πιθανότητας του ψευδών θετικών δοκιμών ενός υδατογραφήματος υπάρχουν δύο διαδικασίες οι οποίες εξαρτώνται από την εφαρμογή. Στην πρώτη διαδικασία δίνονται ένα συγκεκριμένο ψηφιακό αντικείμενο και τυχαία επιλεγμένα υδατογραφήματα. Ο ανιχνευτής εντοπίζει την ύπαρξη ή όχι αυτών των υδατογραφημάτων στο αντικείμενο. Στη δεύτερη διαδικασία, δίνονται ένα συγκεκριμένο υδατογράφημα και τυχαία επιλεγμένα ψηφιακά δεδομένα και το σύστημα

ανίχνευσης εντοπίζει αν υπάρχει το υδατογράφημα σε κάποιο από τα αντικείμενα. Η περίπτωση αυτή χρησιμοποιείται περισσότερο από την πρώτη καθώς η πιθανότητα λάθους είναι μικρότερη.

3.2.5.7 Ασφάλεια (Security)

Η ασφάλεια του υδατογραφικού συστήματος ορίζεται ως η ικανότητά του να αντιστέκεται σε κακόβουλες επιθέσεις οι οποίες έχουν ως σκοπό να αποτρέψουν την υλοποίηση του στόχου του. Οι επιθέσεις χωρίζονται σε τρεις κατηγορίες:

- **Μη εξουσιοδοτημένη αφαίρεση.** Στην κατηγορία αυτή αναφέρονται επιθέσεις που καταστούν το υδατογράφημα μη ανιχνεύσιμο και χωρίζεται σε τρεις υποκατηγορίες: τις επιθέσεις απαλοιφής (elimination attacks), τις επιθέσεις κάλυψης (masking attacks) και τις επιθέσεις συνομωσίας (collusion attacks). Οι επιθέσεις απαλοιφής έχουν ως στόχο τη δημιουργία δεδομένων σχεδόν όμοιων με των αρχικών και εξαλείφουν το υδατογράφημα, ώστε να μην υπάρχει καμία περίπτωση ανίχνευσής του. Οι επιθέσεις κάλυψης τροποποιούν το υδατογράφημα ώστε να μην μπορεί να εντοπιστεί από τους απλούς ανιχνευτές. Τέλος, στις επιθέσεις συνομωσίας ο επιτιθέμενος προμηθεύετε πολλά αντίγραφα του ίδιου υλικού τα οποία περιέχουν διαφορετικά υδατογραφήματα και συνδυάζοντας τα δημιουργεί ένα μη υδατογραφημένο αντίγραφο.
- **Μη εξουσιοδοτημένη ενσωμάτωση.** Η κατηγορία αυτή ονομάζεται πλαστογραφία και αναφέρεται στην ενσωμάτωση παράνομων υδατογραφημάτων σε κάποιο υλικό τα οποία δεν θα έπρεπε να υπάρχουν.
- **Μη εξουσιοδοτημένη ανίχνευση.** Οι επιθέσεις αυτής της κατηγορίας χωρίζονται σε τρία επίπεδα. Το πρώτο επίπεδο περιλαμβάνει τις επιθέσεις στις οποίες ο επιτιθέμενος εντοπίζει και αποκρυπτογραφεί την ενσωματωμένη πληροφορία. Το δεύτερο επίπεδο περιλαμβάνει τις επιθέσεις στις οποίες ο επιτιθέμενος εντοπίζει και ξεχωρίζει τα κρυφά μηνύματα αλλά δεν μπορεί να τα αποκρυπτογραφήσει. Τέλος, το τρίτο επίπεδο περιλαμβάνει επιθέσεις στις οποίες εντοπίζεται η ύπαρξη κάποιου υδατογραφήματος χωρίς να είναι δυνατό να χωριστούν μεταξύ τους ούτε να αποκρυπτογραφηθούν.

Οι δύο πρώτες κατηγορίες ονομάζονται ενεργητικές επιθέσεις (actives attacks) ενώ η τρίτη κατηγορία ονομάζεται παθητική επίθεση (passive attack).

3.2.5.8 Υδατογραφικά Κλειδιά (watermark keys)

Στα κρυπτογραφικά συστήματα η ασφάλεια επιτυγχάνεται με τη χρήση κρυφών κλειδιών τα οποία χρησιμοποιούνται για την κρυπτογράφηση αποκρυπτογράφηση μηνυμάτων. Σε πολλά υδατογραφικά συστήματα γίνεται χρήση κλειδιών για την εισαγωγή και ανίχνευση των υδατογραφημάτων αντίστοιχα.

Στους υδατογραφικούς αλγορίθμους, οι απαιτήσεις ως προς την ασφάλεια των υδατογραφημάτων διαφέρουν από αυτές των κρυπτογραφημάτων (cipher). Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί σε συστήματα υδατογράφησης για την αποτροπή μη εξουσιοδοτημένων ενσωματώσεων και ανίχνευσης υδατογραφημάτων, αλλά δεν μπορεί να χρησιμοποιηθεί στη περίπτωση της αφαίρεσης κάποιου υδατογραφήματος. Τα κλειδιά της ενσωμάτωσης και ανίχνευσης παρέχουν διαφορετικά επίπεδα ασφάλειας σε σχέση με αυτά της κρυπτογράφησης και για αυτό το λόγο θα πρέπει να χρησιμοποιούνται και τα δύο μαζί σε ένα σύστημα υδατογράφησης. Επομένως, το μήνυμα κρυπτογραφείται με το κρυπτογραφικό κλειδί (cipher key) και μετά ενσωματώνεται στα αρχικά δεδομένα με τη χρήση του υδατογραφικού κλειδιού (watermark key).

Τόσο η κρυπτογραφία όσο και η υδατογραφία χρησιμοποιούν τις εννοιολογίες του δημόσιου και ιδιωτικού κλειδιού.

- **Υδατογράφηση Δημοσίου κλειδιού.** Σε ένα σύστημα υδατογραφίας δημοσίου κλειδιού, η ψηφιακή εικόνα υδατογραφείται χρησιμοποιώντας ιδιωτικό κλειδί αλλά η παρουσία της υδατογραφίας μπορεί να ελεγχθεί χρησιμοποιώντας ένα δημόσιο

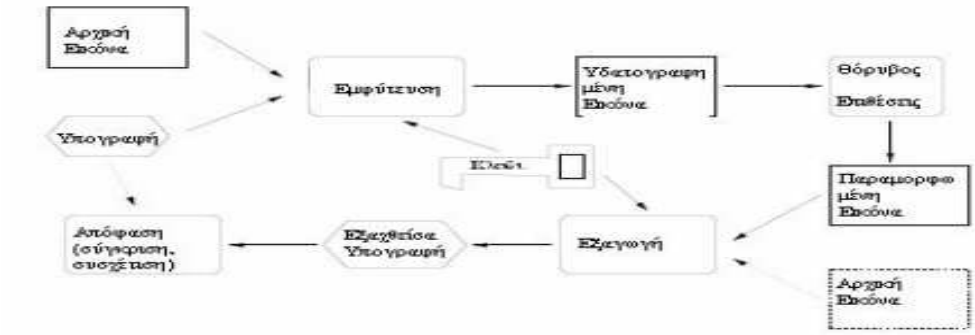
κλειδί. Φυσικά, όπως είναι αναμενόμενο, ο υπολογισμός του ιδιωτικού κλειδιού είναι πρακτικά ανέφικτος, παρά την διαθεσιμότητα του δημοσίου κλειδιού και του αλγορίθμου του συστήματος υδατογραφίας. Το μόνο που επιτρέπει το δημόσιο κλειδί είναι το διάβασμα της υδατογραφίας και δεν μπορεί να χρησιμοποιηθεί για να αφαιρεθεί ή να πλαστογραφηθεί η υδατογραφία. Η ασύμμετρη υδατογραφία μπορεί να θεωρηθεί ως ένας τρόπος πραγματοποίησης του συστήματος υδατογραφίας δημοσίου κλειδιού. Η υδατογραφία δημοσίου κλειδιού γενικά δεν χρειάζεται την παρουσία της αρχικής (αυθεντική) εικόνας κατά την διαδικασία της εξαγωγής (τυφλή). Μέχρι σήμερα, όλα τα γνωστά συστήματα υδατογραφίας δημοσίου κλειδιού επιτρέπουν σχεδόν πάντα την αφαίρεση ή την εισαγωγή πλαστής υδατογραφίας.

- **Υδατογράφηση Ιδιωτικού κλειδιού.** Στην υδατογραφία ιδιωτικού κλειδιού, το κλειδί που επιτρέπει την ανίχνευση της υδατογραφίας είναι το ίδιο με το κλειδί που χρησιμοποιείται για εμφύτευση και δεν επιτρέπεται σε κάποιο τρίτο να διαβάζει και να τροποποιεί την υδατογραφία. Δηλαδή χωρίς τη γνώση του ιδιωτικού κλειδιού είναι αδύνατο για κάποιο τρίτο να ανιχνεύσει κατά πόσο κάποια εικόνα είναι υδατογραφημένη ή όχι.

3.2.6 Διαδικασία Υδατογράφησης

Η διαδικασία υδατογράφησης μιας ψηφιακής εικόνας φαίνεται στην Εικόνα 21. Η αυθεντική (αρχική) εικόνα τροποποιείται με την εμφύτευση πληροφοριών σ' αυτήν, χρησιμοποιώντας μια ψηφιακή 'υπογραφή', σχηματίζοντας έτσι την υδατογραφημένη εικόνα. Εισάγεται επίσης και κάποια παραμόρφωση η οποία όμως πρέπει να είναι αρκετά μικρή ώστε να μην αποκρύπτει την υδατογραφία. Ακολούθως η υδατογραφημένη πλέον εικόνα μπορεί να 'κυκλοφορήσει' μεταξύ νομίμων και παρανόμων χρηστών. Κατά την διάρκεια αυτής της διανομής, μπορεί να προστεθεί στην εικόνα κάποια επιπλέον παραμόρφωση, σκόπιμα ή και μη, από lossy συμπιέσεις της εικόνας, από επαναδειγματοληψία ή από επιθέσεις στην υδατογραφία.

Κατά τη διαδικασία εξαγωγής (extraction process), σε μερικές εφαρμογές είναι απαραίτητη η παρουσία της αυθεντικής εικόνας για την εξαγωγή της κρυμμένης υπογραφής, ενώ σε μερικές άλλες εφαρμογές δεν χρειάζεται. Είναι αυτονόητο ότι είναι επιθυμητό η εξαγόμενη υπογραφή να έχει όσο το δυνατό λιγότερες διαφορές με την αυθεντική υπογραφή.



Εικόνα 21: Γενικό μοντέλο ψηφιακής υδατογράφησης

Βασική προϋπόθεση για μελέτη και κατανόηση των διαφόρων όψεων της ψηφιακής υδατογραφίας, είναι ο ορισμός ενός γενικού μοντέλου. Αυτό το μοντέλο περιέχει τέσσερα στάδια:

- Στάδιο εμφύτεψης (embedding stage).
- Στάδιο εξαγωγής (extraction stage)
- Στάδιο παραμόρφωσης (distortion stage) και
- Στάδιο απόφασης

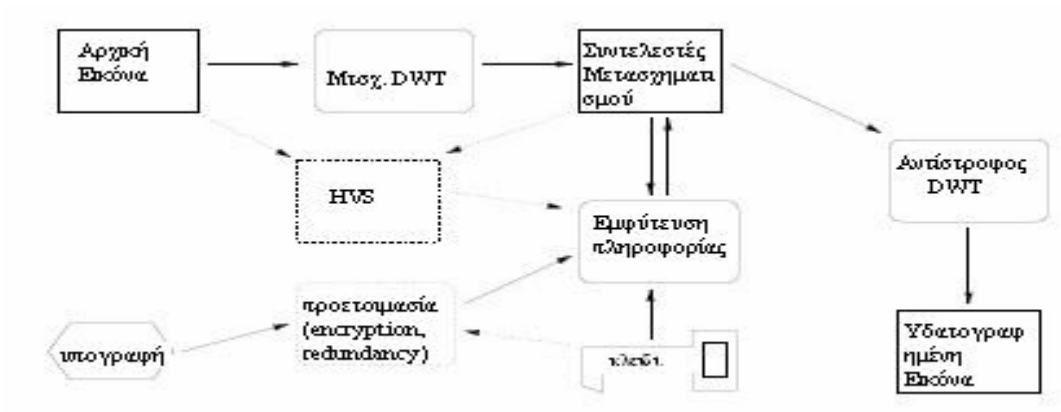
3.2.6.1 Στάδιο Εμφύτευσης

Όλοι σχεδόν οι εύρωστοι και ανθεκτικοί αλγόριθμοι ψηφιακής υδατογραφίας, πλην κάποιων εξαιρέσεων, δουλεύουν στο πεδίο μετασχηματισμού το οποίο προσφέρει πρόσβαση στις συνιστώσες συχνότητας της αρχικής εικόνας. Εάν το στάδιο του μετασχηματισμού παραληφθεί και εμφυτευτεί η υδατογραφία στο πεδίο του χώρου, πάλι μπορεί να σχεδιαστεί ένας απλός και αποδοτικός αλγόριθμος υδατογραφίας, χωρίς όμως ο αλγόριθμος αυτός να είναι και τόσο αποδοτικός στις διάφορες επιθέσεις.

Έτσι στο στάδιο της εμφύτευσης (Εικόνα 22), η αρχική εικόνα πρώτα μετασχηματίζεται σε ένα πεδίο το οποίο διευκολύνει την εμφύτευση πληροφοριών. Σε αυτό το σύγγραμμα ο μετασχηματισμός που χρησιμοποιείται είναι ο DWT (Discrete Wavelet Transform).

Η ψηφιακή υπογραφή (μήνυμα) η οποία εμφυτεύεται μπορεί να είναι κάποια δυαδική πληροφορία, μία μικρή εικόνα (logo) ή μια ακολουθία ψευδοτυχαίων αριθμών, η οποία μπορεί να δημιουργηθεί χρησιμοποιώντας μια γεννήτρια ψευδοτυχαίων αριθμών. Σε γενικές γραμμές η ψηφιακή υπογραφή πρέπει να κρυπτογραφηθεί για να αποσυσχετιστούν οι πληροφορίες που περιέχει.

Στη συνέχεια ένα υποσύνολο των συντελεστών του μετασχηματισμού τροποποιείται με την επεξεργασμένη πληροφορία της ψηφιακής υπογραφής. Μπορούμε να υιοθετήσουμε ένα μοντέλο ανθρώπινης αντίληψης για υπολογίσουμε το μέγεθος των εμφυτευμένων πληροφοριών. Διαλέγοντας ένα κατάλληλο μετασχηματισμό συχνότητας και επιλέγοντας μόνο ορισμένους συντελεστές (συνήθως στις χαμηλές και μεσαίες συχνότητες), μεγάλο μέρος του ανθρώπινου συστήματος όρασης (HVS) μοντελοποιείται εμμέσως. Ο μετασχηματισμός όσο περισσότερο προσεγγίζει τις ιδιότητες του HVS, τόσο πιο εύκολα μπορεί να μπει περισσότερη ενέργεια στο εμφυτευόμενο σήμα, χωρίς να προκαλεί αντιληπτές παραμορφώσεις.



Εικόνα 22 : Στάδιο Εμφύτευσης

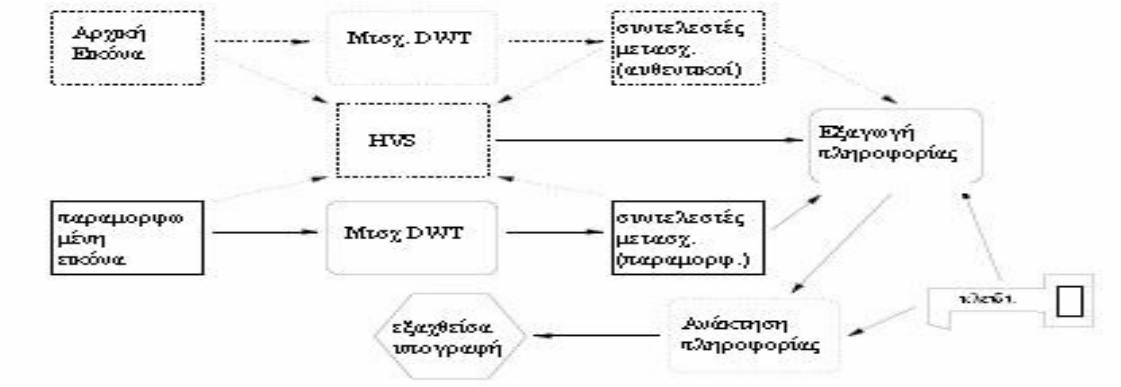
Τέλος, εφαρμόζεται ο αντίστροφος μετασχηματισμός πάνω στους τροποποιημένους συντελεστές (στο πεδίο του μετασχηματισμού) και σχηματίζεται η υδατογραφημένη εικόνα.

3.2.6.2 Διανομή Υδατογραφημένης Εικόνας

Η υδατογραφημένη εικόνα διανέμεται, με πιο συνηθισμένο μέσο πλέον το διαδίκτυο, με την διανομή να περιλαμβάνει τις πιο πολλές φορές lossy συμπίεση πριν την μετάδοση.
Κατά τη διάρκεια της μετάδοσης και διανομής της εικόνας προστίθενται διάφορες παραμορφώσεις και λάθη όχι μόνο με την συμπίεση αλλά και με την επαναδειγματοληψία, με την γάμμα διόρθωση καθώς και με άλλες κοινές εργασίες πάνω στην εικόνα. Ειδικά η γεωμετρική παραποίηση της εικόνας όπως μεγέθυνση, σμίκρυνση, περιστροφή και την γεωμετρική περικοπή (cropping) αποδεικνύεται να είναι εξαιρετικά επιβλαβής στην εμφυτευμένη υδατογραφία. Όλες οι παραποιήσεις της υδατογραφημένης εικόνας πρέπει να αντιμετωπιστούν ως επιθέσεις ούτως ώστε να ληφθούν τα απαραίτητα μέτρα για την αντιμετώπισή τους. Από την άλλη μεριά εκτός από τις συμπτωματικές υπάρχουν και οι ηθελημένες - εχθρικές επιθέσεις, οι οποίες σκοπό έχουν την αποδυνάμωση και απομάκρυνση της υδατογραφίας.

3.2.6.3 Στάδιο Εξαγωγής

Σε αυτό το στάδιο (Εικόνα 23) προσπαθούμε να εξάγουμε την ψηφιακή υπογραφή που κρύβει η εικόνα, με την εικόνα στις πλείστες των περιπτώσεων να έχει υποστεί αρκετά σοβαρές παραμορφώσεις όπως είδαμε στην προηγούμενη παράγραφο. Αυτό μπορεί να γίνει από την μεριά αυτού που έχει υδατογραφήσει την εικόνα, από κάποιο πελάτη που έχει παραλάβει την εικόνα ή ακόμη και από κάποιο νομική αρχή για προστασία των πνευματικών δικαιωμάτων. Στην πρώτη περίπτωση το μυστικό κλειδί που έχει χρησιμοποιηθεί για να υδατογραφηθεί η εικόνα είναι διαθέσιμο, και επιπλέον μπορεί



Εικόνα 23: Στάδιο Εξαγωγής

να είναι διαθέσιμη και η αρχική εικόνα. Το γεγονός αυτό διευκολύνει πάρα πολύ το σύστημα υδατογραφίας και η ανίχνευση της υδατογραφίας μπορεί να γίνει απευθείας. Τέτοια συστήματα στα οποία είναι διαθέσιμα τόσο το μυστικό κλειδί όσο και η αρχική εικόνα ονομάζονται όχι-τυφλά (non-blind) ή ιδιωτικά (private) συστήματα.

Στον αντίποδα είναι η περίπτωση όπου ούτε το μυστικό κλειδί αλλά ούτε και η αρχική εικόνα είναι διαθέσιμα κατά την διαδικασία εξαγωγής. Αυτά τα συστήματα υδατογραφίας ονομάζονται συστήματα υδατογραφίας δημοσίου κλειδιού (public key). Ωστόσο κανένα από τα συστήματα αυτά που έχουν δημιουργηθεί μέχρι σήμερα δεν είναι αξιόπιστο και είναι αμφίβολο αν

θα δημιουργηθεί ποτέ. Πρόσφατα έχουν παρουσιαστεί ασύμμετρα συστήματα υδατογραφίας τα οποία χρησιμοποιούν διαφορετικά κλειδιά κατά την εμφύτευση και την ανίχνευση.

Ένα σύστημα υδατογραφίας το οποίο επιτρέπει την εξαγωγή της ψηφιακής υπογραφής χωρίς την χρήση της αρχικής εικόνας, ονομάζεται τυφλό (blind) σύστημα υδατογραφίας. Υπάρχουν επίσης και κάποιες μέθοδοι ανίχνευσης ή εξαγωγής οι οποίοι βασίζονται σε κάποιες πληροφορίες ή χαρακτηριστικά της αρχικής εικόνας. Αυτά τα συστήματα ονομάζονται ημί-τυφλά (semi-blind) συστήματα υδατογραφίας.

Συνοψίζοντας, έχουμε τρεις βασικές μεθόδους εξαγωγής υδατογραφίας βασισμένες στη διαθεσιμότητα της αρχικής εικόνας :

- Τυφλή (blind)
- Ημι-τυφλή (semi-blind) και
- Όχι - τυφλή (non-blind)

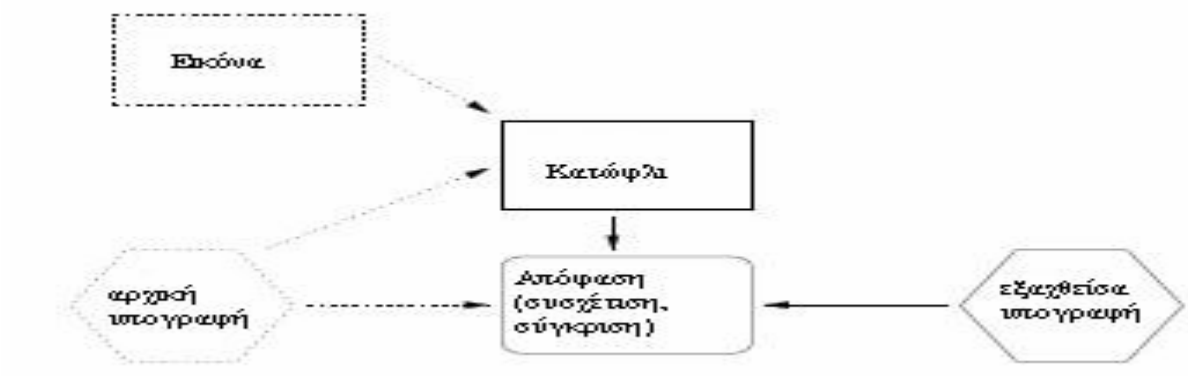
και τρεις βασικές μεθόδους βασισμένες στο κλειδί που χρειάζεται κατά την εξαγωγή της υδατογραφίας:

- Ιδιωτικού κλειδιού
- Δημόσιου κλειδιού και
- Ασύμμετρη

3.2.6.4 Στάδιο Απόφασης

Σε αυτό το στάδιο (Εικόνα 24), το σύστημα υδατογραφίας εξετάζει και αναλύει την εξαγόμενη πληροφορία. Το στάδιο απόφασης μπορεί να βγάλει διαφόρων τύπων αποτελέσματα, εξαρτώμενα στον τύπο της εφαρμογής καθώς και στο είδος της πληροφορίας που περιέχεται στην υδατογραφία.

Στις εφαρμογές ψηφιακής υδατογραφίας εικόνας, το αποτέλεσμα μπορεί να είναι από κάτι απλό μέχρι κάτι πολύ περίπλοκο. Στην απλούστερη των περιπτώσεων το αποτέλεσμα μπορεί να είναι μία απόφαση ναι/όχι καταδεικνύοντας αν έχει βρεθεί ή όχι η ψηφιακή υπογραφή του νόμιμου κατόχου της εικόνας. Τα πιο σύνθετα συστήματα επιστρέφουν την πληροφορία (συνήθως το λογότυπο) που έχει εμφυτευτεί στην αρχική εικόνα.



Εικόνα 24: Στάδιο Απόφασης

3.3 Σύγκριση Κρυπτογράφησης – Υδατογράφησης

Όπως είναι κατανοητό οι διαφορές μεταξύ κρυπτογράφησης και υδατογράφησης είναι φανερές και παρουσιάζονται στον παρακάτω πίνακα.

Κρυπτογράφηση	**Υδατογράφηση**
Σύγκριση	
Κρύβει το περιεχόμενο του μηνύματος από τον εισβολέα αλλά όχι την ύπαρξη του μηνύματος	Κρύβονται τόσο το περιεχόμενο όσο και η ύπαρξη του μηνύματος
Τα μεταδιδόμενα δεδομένα-πληροφορίες κωδικοποιούνται με τέτοιο τρόπο, ώστε ακόμα και αν πέσουν στα χέρια μη εξουσιοδοτημένων χρηστών, να είναι ακατανόητα και άχρηστα	Συνδυάζει δυο κομμάτια πληροφορίας, την πρωτότυπη και την προστιθέμενη (υδατογράφημα), με τέτοιο τρόπο ώστε να μπορεί κανείς να τα επεξεργαστεί ανεξάρτητα
Προστατεύει ένα προϊόν υπό μεταφορά, αλλά μόλις αποκρυπτογραφηθεί, το περιεχόμενο είναι ευάλωτο	Προστατεύει το περιεχόμενο και μετά την αποκρυπτογράφηση του, τοποθετώντας την πληροφορία μέσα στο περιεχόμενο, απ’ όπου δεν αφαιρείται ποτέ κατά την κανονική χρήση

Πίνακας 1: Σύγκριση κρυπτογράφησης - υδατογράφησης

Κεφάλαιο 4

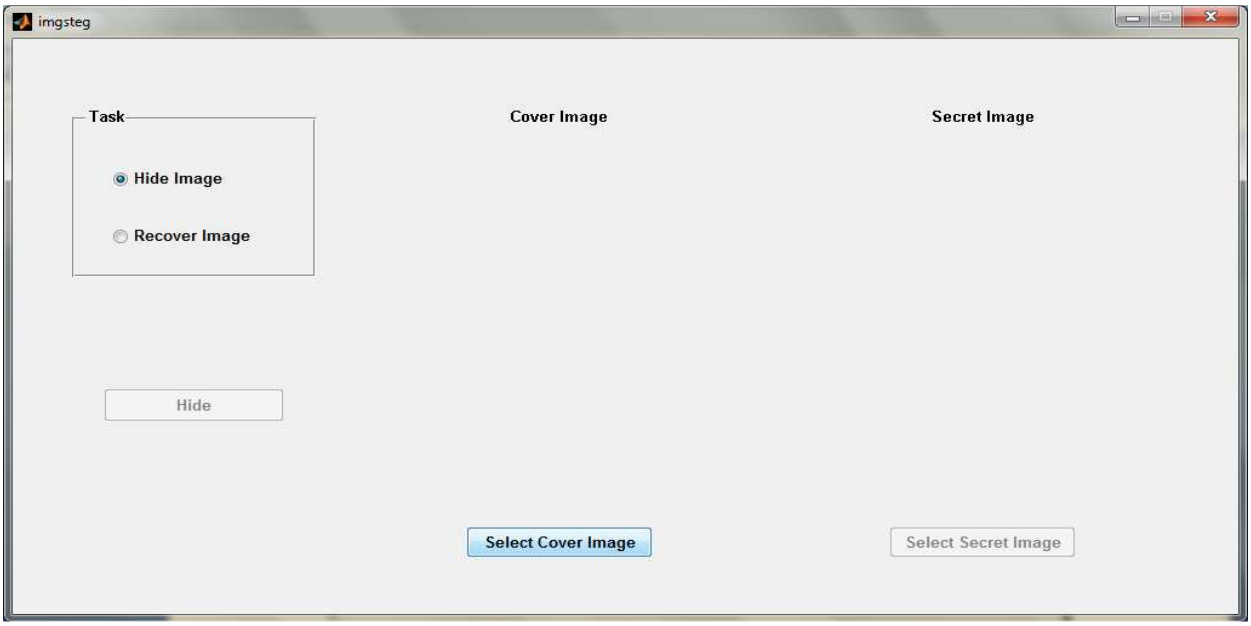
Τεχνικές Κρυπτογράφησης και Υδατογράφησης

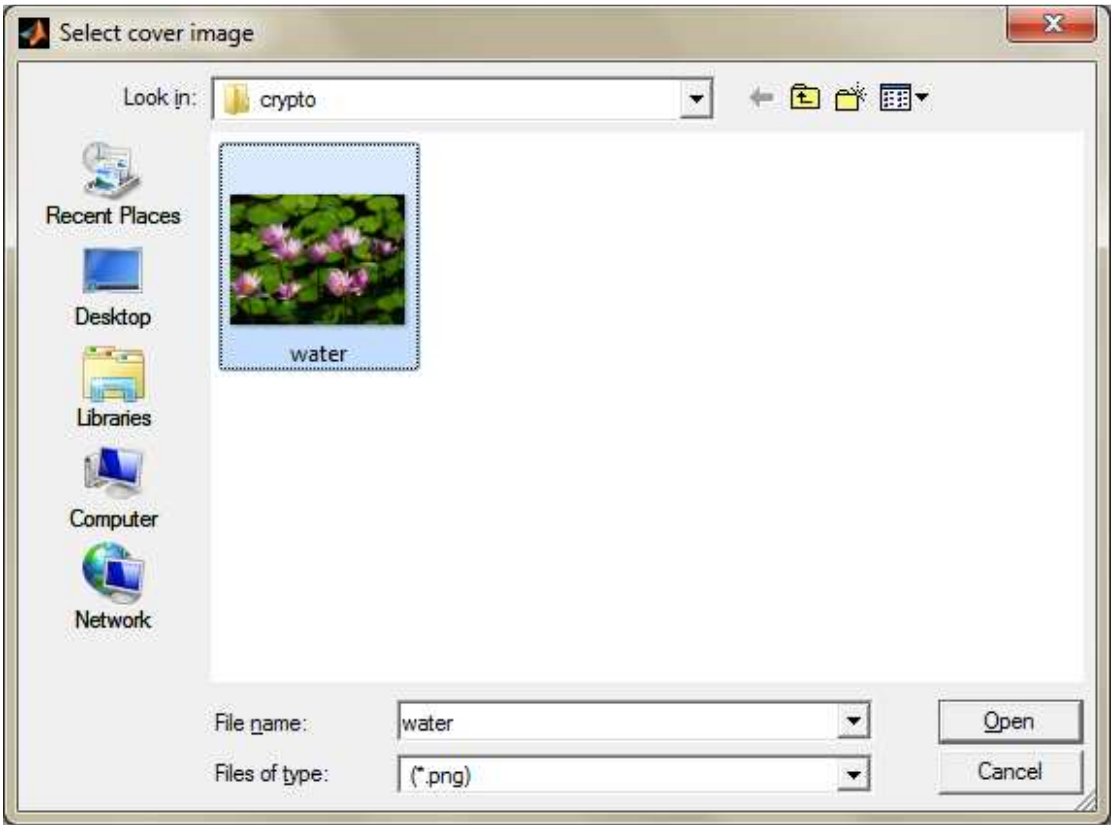
4.1 Τεχνική Κρυπτογράφησης

Υπάρχουν πολλές μέθοδοι που χρησιμοποιούνται για την απόκρυψη πληροφοριών στο εσωτερικό της εικόνας. Οι τεχνικές αυτές μπορούν να χρησιμοποιηθούν με ποικίλους βαθμούς επιτυχίας για διαφορετικούς τύπους αρχείων εικόνας. Η πιο κοινή μέθοδος είναι η **LSB με πρόγραμμα GUI.**

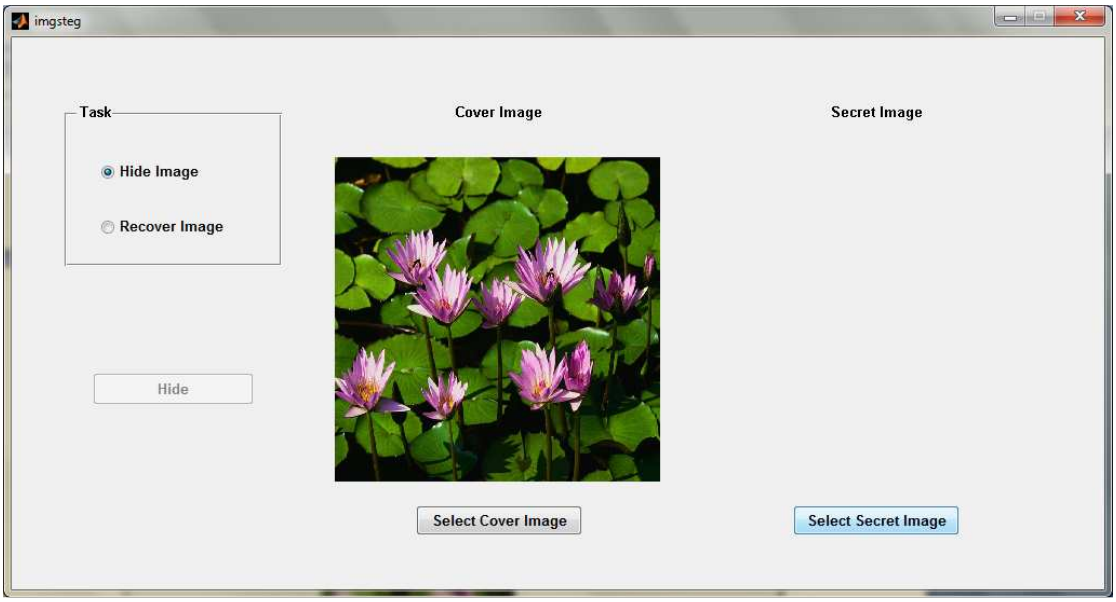
4.1.1 Κρυπτογράφηση εικόνας με μέθοδο LSB

Χρησιμοποιώντας το πρόγραμμα διεπαφής GUI, διαλέγουμε από το πινακάκι task το hide image και πατάμε το Select Cover Image για να ανοίξουμε το φάκελο με τις εικόνες.

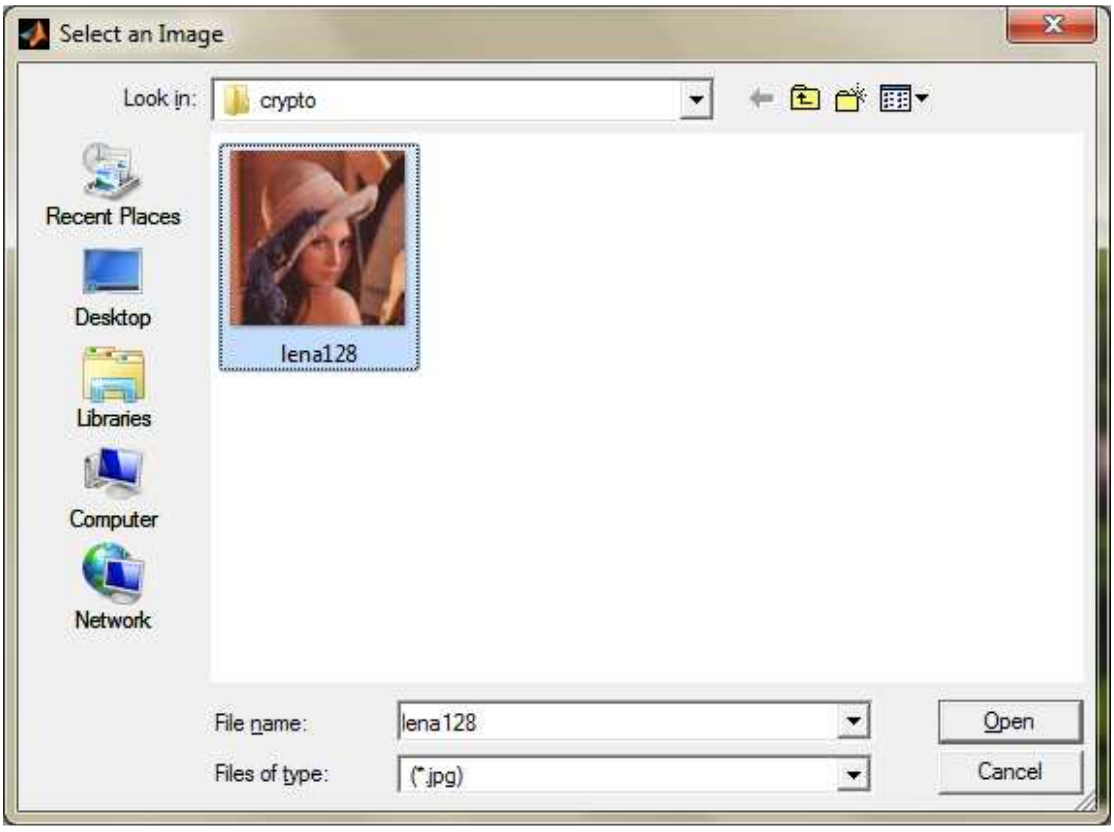




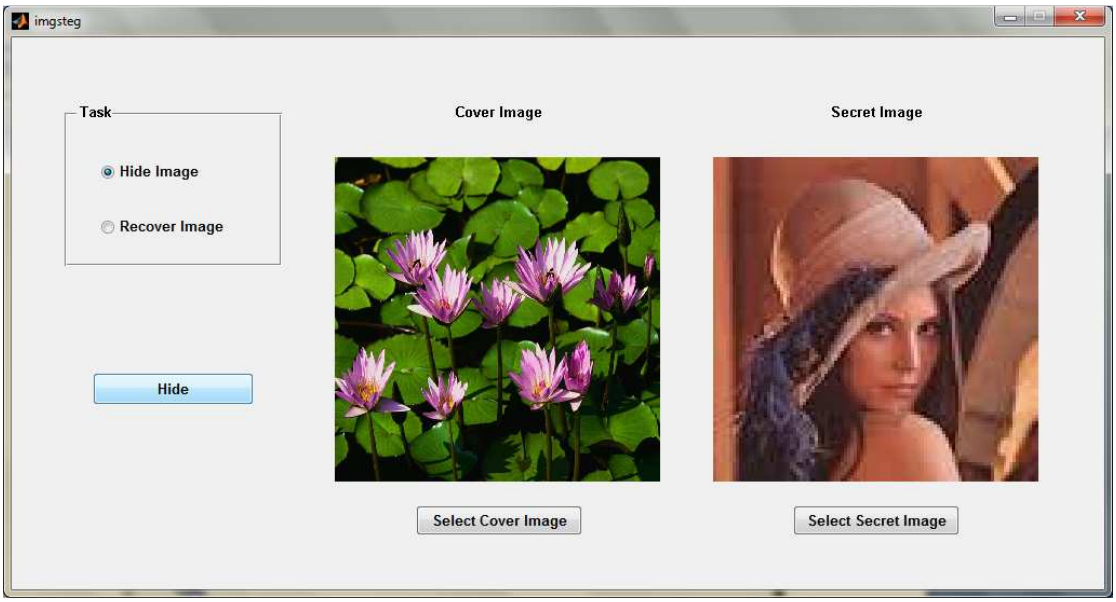
Η εικόνα που επιλέξαμε εμφανίζεται στη θέση Cover Image. Έπειτα πατάμε το κουμπί Select Secret Image, με σκοπό να επιλέξουμε την εικόνα που θέλουμε να κρύψουμε μέσα στην εικόνα water.



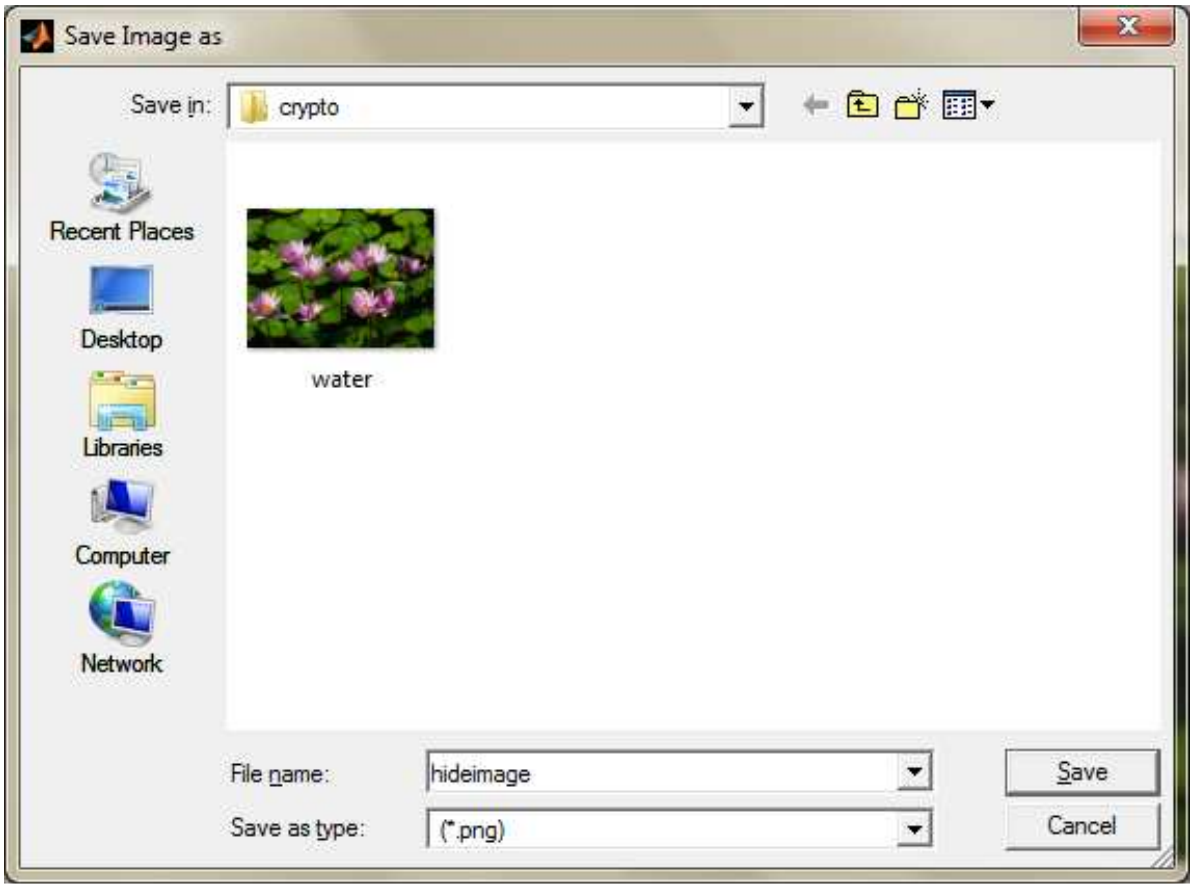
Διαλέγουμε την εικόνα lena128, μικρότερου μεγέθους 102x102 και τύπου jpg,



και έτσι εμφανίζεται στη θέση Secret Image. Πατώντας το κουμπί Hide κρύβουμε την μία εικόνα μέσα στην άλλη.



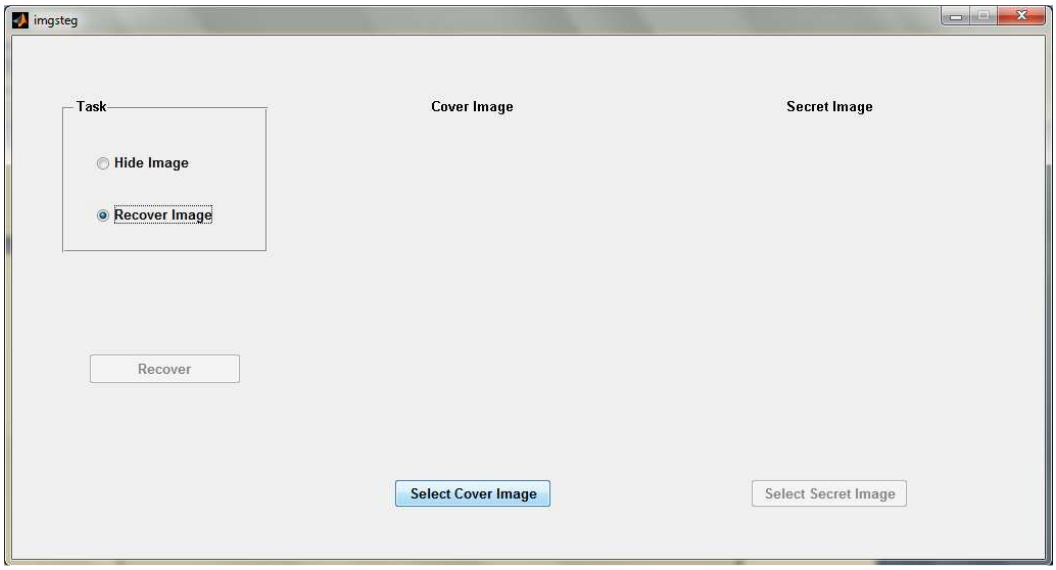
Τέλος, σώζουμε την κρυπτογραφημένη εικόνα μέσα στον φάκελο, με το όνομα hideimage. Σημειώνεται ότι η τελική μας εικόνα είναι τύπου png.



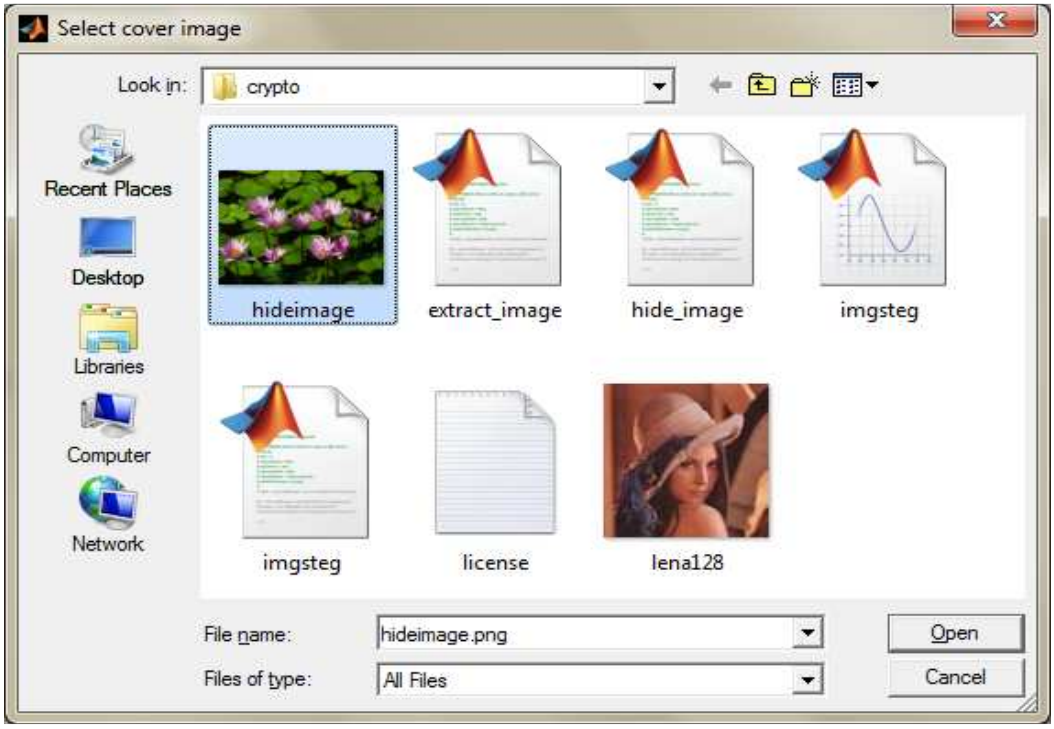
Έτσι εμφανίζεται στο παράθυρο μας το παρακάτω μήνυμα που μας εξηγεί ότι εικόνα που κρύψαμε βρίσκεται στην εικόνα με όνομα hideimage.png

4.1.2 Αποκρυπτογράφηση εικόνας

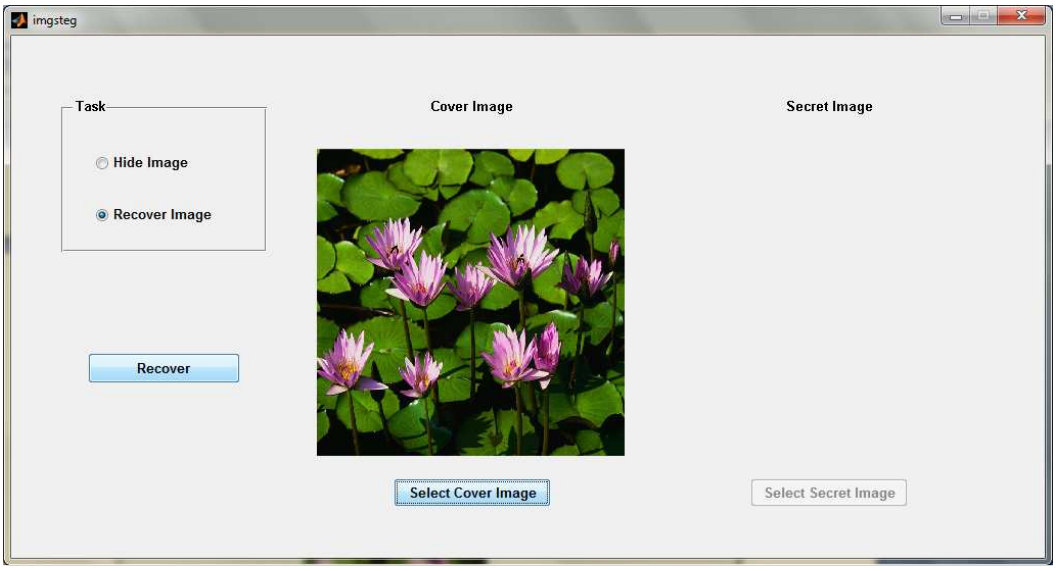
Για την διαδικασία της αποκρυπτογράφησης, διαλέγουμε από τον πίνακα task το Recover Image και πατάμε το κουμπί Select Cover Image.



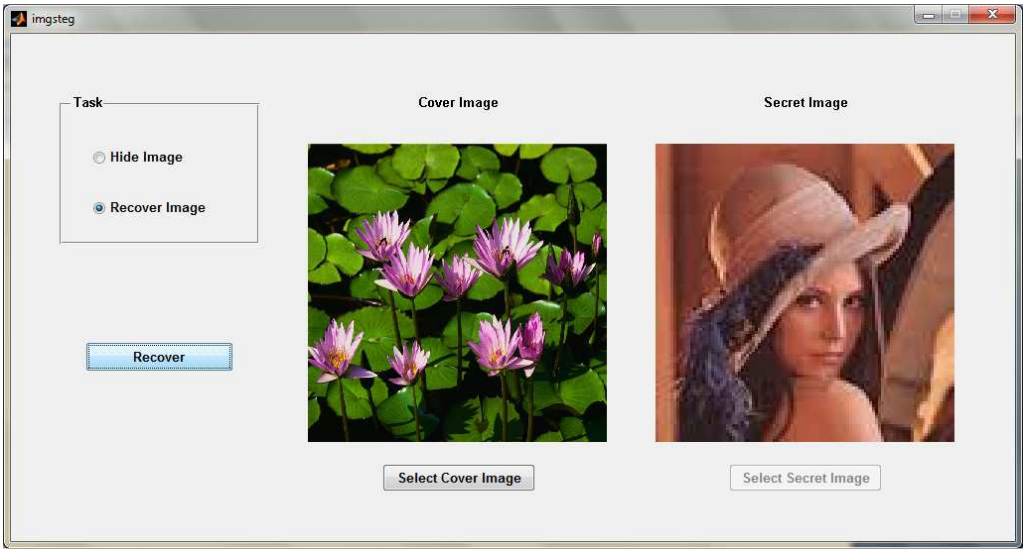
Επιλέγουμε από τον φάκελο και ανοίγουμε την κρυπτογραφημένη εικόνα (στην περίπτωση μας είναι η εικόνα που κρυπτογραφήσαμε πριν hideimage.png)



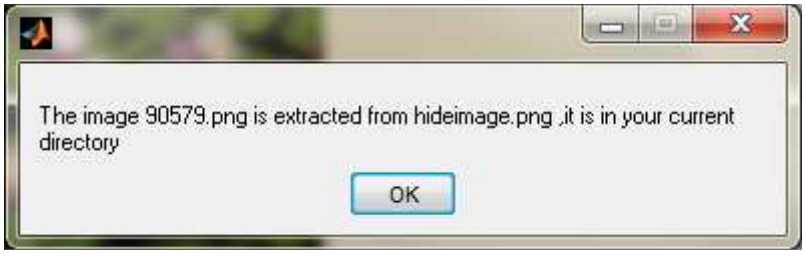
η οποία εμφανίζεται στη θέση Cover Image.



Με το πάτημα του κουμπιού Recover Image εμφανίζεται στο παράθυρο η κρυμμένη εικόνα στη θέση Secret Image



Καθώς και το μήνυμα ότι η κρυμμένη είναι πλέον διαθέσιμη.



4.2 Τεχνικές Ψηφιακής Υδατογράφησης

Οι τεχνικές ψηφιακής υδατογράφησης (digital watermarking techniques) ενθέτουν μοναδικά σημάδια (υδατογραφήματα) σε πολυμέσα, ήχους, βίντεο, εικόνες και κείμενο. Σκοπός τους είναι η επιβεβαίωση της γνησιότητας του περιεχομένου και η παροχή προστασίας πνευματικών δικαιωμάτων χωρίς τον υποβιβασμό της ποιότητας τους. Οι τεχνικές υδατογράφησης διαφέρουν από τις κρυπτογραφικές τεχνικές, λόγω του ότι στις υδατογραφικές τεχνικές γίνετε ένθεση ενός σημαδιού μέσα στα δεδομένα που μεταδίδονται ενώ στις κρυπτογραφικές τεχνικές αλλάζουν εντελώς τα δεδομένα από την αρχική τους μορφή πριν την μετάδοση τους.

Οι τεχνικές υδατογράφησης εφαρμόζονται σε εικόνες και ανάλογα με το είδος της εφαρμογής υπάρχουν συγκεκριμένες διαδικασίες από τις οποίες το υδατογράφημα θα πρέπει να παραμείνει ακέραιο. Αυτές είναι:

- Οι εφαρμογές προστασίας του περιεχομένου (content protection applications)
- Οι τεχνικές πιστοποίησης της αυθεντικότητας των δεδομένων (data authentication)
- Οι τεχνικές ετικετοποίησης (labeling)

Μερικά από τα χαρακτηριστικά που απαιτούνται στην υδατογράφηση εικόνας είναι:

- Η μη αντιληπτικότητα (imperceptibility) του υδατογραφήματος.
- Η ανθεκτικότητα (robustness).
- Η χωρητικότητα (capacity).

Επίσης το υδατογράφημα θα πρέπει να παραμένει ανεπηρέαστο από διεργασίες όπως είναι η συμπίεση, η αλλαγή του μεγέθους της εικόνας, η αποκοπή της, η συμπίεση, η μετατροπή από αναλογικό σε ψηφιακό σήμα, ο θόρυβος κλπ.

Η ενσωμάτωση του υδατογραφήματος μπορεί να εφαρμοστεί απευθείας στις τιμές των pixels στο χωρικό πεδίο (spatial domain) ή σε τροποποιημένους συντελεστές στο πεδίο μετασχηματισμού (transform domain) όπως το διακριτό μετασχηματισμό συνημίτονου (Discrete Cosine Transform-DCT) ή στο διακριτό μετασχηματισμό κυματιδίου (Discrete Wavelet Transform-DWT).

4.2.1 Least Significant Bit Modification (LSB)

Μια από τις πιο γνωστές μεθόδους υδατογραφίας ψηφιακών εικόνων στο χωρικό πεδίο (spatial domain) εφαρμόζει την ενσωμάτωση του υδατογραφήματος στο λιγότερο σημαντικό ψηφίο -bit του αντικειμένου κάλυψης. Δεδομένης της εξαιρετικά υψηλής χωρητικότητας του καναλιού χρησιμοποιώντας την αρχική μας εικόνα, ένα μικρότερο αντικείμενο μπορεί να ενσωματωθεί πολλές φορές. Η εύκολη υλοποίηση καθώς επίσης και το μικρό υπολογιστικό κόστος αποτελούν δύο επιπλέον πλεονεκτήματα.

Κάποια από τα μειονεκτήματα είναι η περιορισμένη ευρωστία στην περίπτωση απωλεστικής συμπίεσης ή προσθήκης θορύβου, οι στατιστικές εξαρτήσεις (statistics dependencies) που εντοπίζονται, αλλά και ορισμένα σημεία στα οποία το υδατογράφημα είναι οπτικά αισθητό. Υπάρχουν όμως και περιπτώσεις εφαρμογών όπου τα μειονεκτήματα μετατρέπονται σε πλεονεκτήματα, όπως η περιορισμένη ευρωστία.

Αποτελέσματα ενσωμάτωσης και ανάκτησης υδατογραφήματος

original image

watermark

watermarked image

recovered watermark

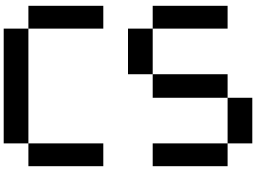
Τα αποτελέσματα από την τεχνική LSB ήταν τα αναμενόμενα. Όπως παρατηρούμε στις εικόνες, η υδατογραφημένη εικόνα δεν παρουσιάζει αισθητές μεταβολές στην ποιότητά της και το υδατογράφημα ανακτάται τέλεια. Η συγκεκριμένη περίπτωση όμως θεωρείται ιδανική καθώς η εικόνα δεν έχει υποστεί καμία επεξεργασία.

4.2.2 CDMA Spread – Spectrum

Σε περιπτώσεις υψηλού επιπέδου συμπίεσης JPEG και προσθήκης θορύβου οι εφαρμογές με το CDMA παρουσιάζουν εξαιρετική ευρωστία στο υδατογράφημα, με άψογη ανάκτηση του υδατογραφήματος από την υδατογραφημένη εικόνα. Το CDMA στο χωρικό πεδίο δεν παύει όμως να έχει αρκετά προβλήματα που περιορίζουν τη χρησιμότητά του. Το κύριο μειονέκτημα του CDMA είναι πως έχει περιορισμένη χωρητικότητα σε σχέση με παρόμοιες correlation-based τεχνικές. Ένας από τους λόγους είναι πως η ποιότητα της ανίχνευσης του υδατογραφήματος μειώνεται αρκετά σε μεγαλύτερα μεγέθη εικόνας. Σε αντίθεση με τα αποτελέσματα του υδατογραφήματος κανονικού μεγέθους που είναι απογοητευτικά, με τη χρήση μικρού υδατογραφήματος τα αποτελέσματα είναι αρκετά ικανοποιητικά.

Επίσης, ο χρόνος επεξεργασίας για το CDMA χωρικού πεδίου αυξάνει εκθετικά με την αύξηση του μεγέθους του μηνύματος. Στις εφαρμογές, το CDMA για ένα κανονικό μέγεθος μηνύματος παρουσίασε τον μεγαλύτερο χρόνο επεξεργασίας από όλες τις τεχνικές που εξετάζονται. Το CDMA εκτελέστηκε πολύ ικανοποιητικά με ένα μικρό υδατογράφημα. Μετά από πειραματισμούς, ο συντελεστής ενίσχυσης k=2 παρουσίασε καλή ισορροπία μεταξύ ποιότητας της εικόνας και ευρωστίας του υδατογραφήματος.

<u>Για k=2</u>



watermark

watermarked image

recovered watermark

Συνεπώς, οι βασικοί περιορισμοί του CMDA στο χωρικό πεδίο αποτελούν η περιορισμένη χωρητικότητα και οι υψηλές απαιτήσεις επεξεργασίας. Η ενσωμάτωση μεγάλων υδατογραφημάτων απαιτεί τη μείωση του συντελεστή k για να διατηρηθεί η οπτική ποιότητα της εικόνας. Δεδομένου ότι

περισσότερες PN ακολουθίες προστίθενται στην αρχική εικόνα, απαιτούνται μεγαλύτεροι συντελεστές k για τη διατήρηση της συσχέτισης μεταξύ των ακολουθιών. Αυτή η αντίθεση είναι ο λόγος που το CDMA στο χωρικό πεδίο θα παραμένει περιορισμένο όσον αφορά τη χωρητικότητα σε σύγκριση με τις άλλες τεχνικές.

4.2.3 Τεχνικές βασισμένες στη συσχέτιση (Correlation-based Techniques)

Άλλη μια τεχνική ενσωμάτωσης υδατογραφήματος είναι η αξιοποίηση των μοντέλων συσχέτισης προσθετικών ψευδοτυχαίων υποδειγμάτων θορύβου (additive pseudo-random noise patterns), όπως εφαρμόζονται σε μια εικόνα. Ένα υπόδειγμα W(x,y) ψευδοτυχαίου θορύβου (PN) προστίθεται στην εικόνα I(x,y) σύμφωνα με την παρακάτω εξίσωση:

$$I_w(x,y) = I(x,y) + k * W(x,y)$$

όπου k συντελεστής ενίσχυσης (gain factor) και I_w υδατογραφημένη εικόνα. Όσο αυξάνεται το k αυξάνεται η ευρωστία του υδατογραφήματος αλλά μειώνεται η ποιότητα της υδατογραφημένης εικόνας.

Για την ανάκτηση του υδατογραφήματος, χρησιμοποιείται ο ίδιος αλγόριθμος γεννήτριας ψευδοτυχαίου θορύβου με το ίδιο κλειδί και έτσι υπολογίζεται ο συσχετισμός ανάμεσα στο υπόδειγμα θορύβου και της εικόνας που πιθανόν έχει υδατογραφηθεί. Αν η συσχέτιση υπερβαίνει ένα συγκεκριμένο κατώτατο όριο T (threshold), ανιχνεύεται το υδατογράφημα και ορίζεται ένα bit. Η μέθοδος αυτή μπορεί να επεκταθεί σε υδατογράφημα πολλών bit, διαιρώντας την εικόνα σε blocks και εκτελώντας την διαδικασία ανεξάρτητα σε κάθε block.

Αυτός ο αλγόριθμος μπορεί να βελτιωθεί με διάφορους τρόπους. Πρώτον, το κατώτατο όριο T που χρησιμοποιείται για τον προσδιορισμό μιας λογικής “1” ή “0”, μπορεί να εξαλειφθεί με τη χρήση δύο ξεχωριστών υποδειγμάτων ψευδοτυχαίου θορύβου. Το πρώτο υπόδειγμα καθορίζει ένα λογικό “1” και το δεύτερο υπόδειγμα ένα “0”. Η παραπάνω διαδικασία εκτελείται μία φορά για κάθε υπόδειγμα και χρησιμοποιείται το υπόδειγμα με την μεγαλύτερη συσχέτιση. Αυτό αυξάνει την πιθανότητα μιας σωστής ανίχνευσης ακόμα και αν η εικόνα έχει υποστεί μεταβολή από επιθέσεις.

Αυτή η μέθοδος μπορεί να βελτιωθεί περεταίρω με το προ-φιλτράρισμα της εικόνας πριν την εφαρμογή του υδατογραφήματος. Αν μπορεί να μειωθεί η συσχέτιση μεταξύ της εικόνας και της ακολουθίας ψευδοτυχαίου θορύβου PN, τότε μπορεί να αυξηθεί η ανθεκτικότητα του υδατογραφήματος με την προσθήκη επιπλέον θορύβου. Με την εφαρμογή του φίλτρου edge enhancement που φαίνεται στην παρακάτω εικόνα, η ευρωστία του υδατογραφήματος μπορεί να βελτιωθεί χωρίς την απώλεια χωρητικότητας και με μικρή μείωση της ποιότητας της εικόνας.

$$F_{edge} = \frac{1}{2}\begin{bmatrix} -1 & -1 & -1 \\ -1 & 10 & -1 \\ -1 & -1 & -1 \end{bmatrix}$$

Εικόνα 25: Ενίσχυση του FIR Edge Προ-Φίλτρο

Χρησιμοποιώντας CDMA τεχνικές εκτεταμένου φάσματος (Spread spectrum techniques) για τη διασπορά του κάθε bit τυχαία στην αρχική εικόνα, μπορούμε να αποφύγουμε να καθορίσουμε τις τιμές του υδατογραφήματος από τα blocks στο χωρικό πεδίο, και έτσι αυξάνουμε τη χωρητικότητα και

βελτιώνουμε την ανθεκτικότητα στις περικοπές της εικόνας (cropping). Το υδατογράφημα πρώτα διαμορφώνεται σαν ένα long string παρά σαν μία δισδιάστατη εικόνα. Για κάθε τιμή του υδατογραφήματος δημιουργείται μία ακολουθία PN με τη χρήση ενός ανεξάρτητου seed. Η σύνοψη όλων αυτών των ακολουθιών PN αναπαριστά το υδατογράφημα, το οποίο έπειτα μετασχηματίζεται και ενσωματώνεται στην εικόνα.

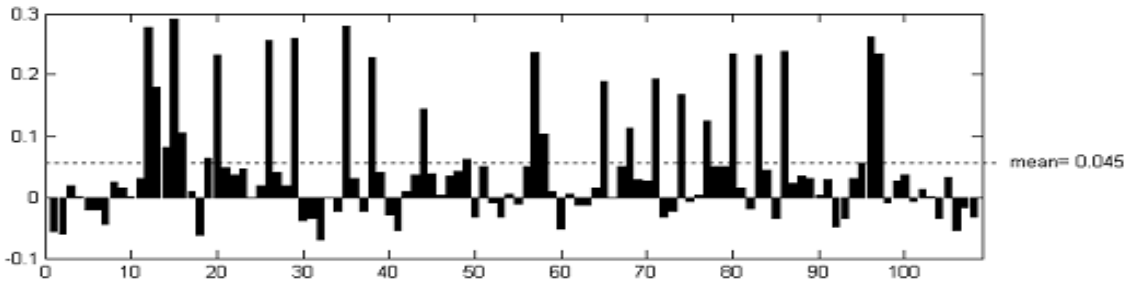
Για να ανιχνεύσουμε το υδατογράφημα κάθε seed χρησιμοποιείται για την παραγωγή της PN ακολουθίας, η οποία έπειτα συσχετίζεται με ολόκληρη την εικόνα. Εάν η συσχέτιση είναι υψηλή το bit στο υδατογράφημα τίθεται σε “1”, ενώ εάν είναι χαμηλή σε “0”. Η διαδικασία αυτή επαναλαμβάνεται έπειτα για όλες τις τιμές του υδατογραφήματος. Η τεχνική CDMA βελτιώνει σημαντικά την ευρωστία του υδατογραφήματος, αλλά απαιτεί περισσότερο υπολογιστικό χρόνο.

Αποτελέσματα Συσχέτισης βασισμένη σε κάποιο κατώτατο όριο (Threshold-Based Correlation)

Τα αποτελέσματα της Threshold-Based Correlation παρουσίασαν τεράστια βελτίωση σε σχέση με τις τεχνικές LSB όσο αφορά την ευρωστία του υδατογραφήματος. Παρόλα αυτά αρκετοί ακόμη παράγοντες παίζουν ρόλο στη συγκεκριμένη εφαρμογή.

Ένας από τους παράγοντες αυτούς αποτελεί ο συντελεστής ενίσχυσης k (gain factor). Όσο μεγαλύτερος είναι ο συντελεστής k, τόσο περισσότερο αυξάνεται η ευρωστία αλλά ταυτόχρονα μειώνεται η ποιότητα της εικόνας, όπως φαίνεται και από τις παρακάτω δοκιμές με διάφορες τιμές του k.

Ένας άλλος παράγοντας αποτελεί η επιλογή ενός κατάλληλου κατώτατου ορίου (Threshold) για την ανίχνευση. Μία μέθοδος για την επιλογή αυτή είναι η αποθήκευση της συσχέτισης κάθε PN ακολουθίας και έπειτα η χρήση της μέσης τιμής των συσχετίσεων έως το κατώτατο όριο T. Για υδατογραφήματα με σχετικά ίσο πλήθος από “0” και “1”, η τεχνική αυτή θα πρέπει να προσαρμόζεται σε μία σειρά τύπων εικόνας και σε διάφορα επίπεδα θορύβου.



Εικόνα 26: Επιλογή των κατώτατων ορίων από Μέση Τιμή

Ένας τελευταίος παράγοντας που παίζει ρόλο αποτελεί το μέγεθος του υδατογραφήματος που πρόκειται να ενσωματωθεί. Η χρήση ενός μικρότερου υδατογραφήματος επιτρέπει να χρησιμοποιηθούν μεγαλύτερα block, αυξάνοντας έτσι την ένταση της συσχέτισης και παράλληλα την ευρωστία. Χρησιμοποιώντας υδατογραφήματα κανονικού μεγέθους, όπως είναι το υδατογράφημα του παρακάτω παραδείγματος, το μεγαλύτερο δυνατό μέγεθος του block από το

πεδίο {8, 16, 32, …} καθορίζεται από το: $1000 \leq \frac{512*512}{16^2}$,από όπου υπολογίζεται πως το μέγιστο μέγεθος block είναι 16.

Για k=5 blocksize=16

watermark

watermarked image

recovered watermark

Για k=40 blocksize=16

watermarked image

watermark

recovered watermark

Αν και με την αύξηση του συντελεστή ενίσχυσης σε 5 το υδατογράφημα μπορεί να αναγνωστεί, τα αποτελέσματα δεν είναι θεαματικά. Η αύξηση του κέρδους δεν βελτιώνει την ανάκτηση του υδατογραφήματος, όμως με τιμές του k πάνω από 5, η ύπαρξη υδατογραφήματος στην εικόνα γίνεται αισθητή όπως φαίνεται παραπάνω. Επίσης σημειώνεται έντονη διαφορά μεταξύ

των PSNR των δύο υδατογραφημένων εικόνων. Για k=5 το PSNR ισούται με 4.7599e+004 ενώ για k=40 το PSNR ισούται με 743.7288, το οποίο δηλώνει την αύξηση του θορύβου.
Παρόλο που το υδατογράφημα ανακτήθηκε με ατέλειες, παρατηρούμε πολύ μεγάλη βελτίωση με την αύξηση του συντελεστή k.

Χρησιμοποιώντας έναν συντελεστή k=5, το υδατογράφημα είναι ευδιάκριτο μετά από κάποια επίπεδα θορύβου και συμπίεσης. Αν αυξήσουμε όμως, τον συντελεστή ενίσχυσης σε 40 βελτιώνεται η ευρωστία του υδατογραφήματος σε σημαντικό βαθμό.

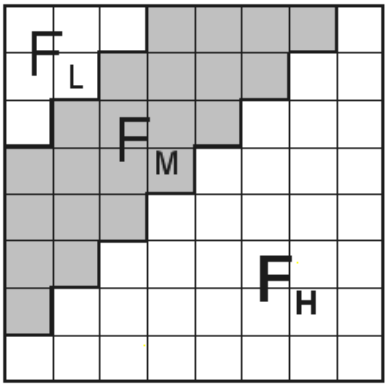
4.2.4 Τεχνικές στο πεδίο συχνότητας (Frequency Domain Techniques)

Ένα πλεονέκτημα των τεχνικών χωρικού πεδίου είναι πως μπορούν εύκολα να εφαρμοστούν σε κάθε εικόνα, ανεξάρτητα από τη μετέπειτα επεξεργασία (το αν θα επηρεαστούν ή όχι από την επεξεργασία αυτή είναι ένα εντελώς διαφορετικό θέμα). Ένα πιθανό μειονέκτημα των τεχνικών χωρικού πεδίου είναι πως δεν εκμεταλλεύονται την εν λόγω επεξεργασία που υφίσταται η εικόνα ώστε να αυξηθεί η ευρωστία του υδατογραφήματος.

Οι προσαρμοστικές τεχνικές υδατογράφησης (adaptive watermarking techniques) είναι πιο δύσκολες στην εφαρμογή τους στο χωρικό πεδίο. Τόσο η ευρωστία και η ποιότητα του υδατογραφήματος μπορούν να βελτιωθούν, εάν μπορούν να αξιοποιηθούν και οι ιδιότητες της αρχικής εικόνας. Για παράδειγμα, είναι προτιμότερο να κρύψουμε την πληροφορία του υδατογραφήματος σε θορυβώδεις περιοχές και στα άκρα των εικόνων, παρά στις πιο ομαλές περιοχές. Έτσι έχουμε διπλό όφελος δηλαδή την μείωση σε ομαλότερες περιοχές της εικόνας, που είναι περισσότερο αισθητή στο ανθρώπινο οπτικό σύστημα (Human Visual System-HVS) και γίνεται πρωταρχικός στόχος για τα σχήματα με απώλειες συμπίεσης.

Το πιο κλασικό και ακόμα πιο δημοφιλές πεδίο για επεξεργασία εικόνας είναι το πεδίο Διακριτού Μετασχηματισμού Συνημίτονου (Discrete Cosine Transform-DCT). Το DCT επιτρέπει το χωρισμό μίας εικόνας σε διαφορετικές ζώνες συχνοτήτων και έτσι καθιστά πιο εύκολη την ενσωμάτωση της υδατογραφημένης πληροφορίας στις μεσαίες ζώνες συχνοτήτων της εικόνας. Οι μεσαίες ζώνες συχνότητας επιλέγονται πρώτον, για να αποφευχθούν τα περισσότερο ορατά τμήματα της εικόνας που βρίσκονται στις χαμηλές συχνότητες, και δεύτερον, για να μην υπάρξει έκθεση της πληροφορίας σε επεξεργασίες που πραγματοποιούνται στις υψηλές ζώνες συχνοτήτων, όπως η αφαίρεση λόγω συμπίεσης ή προσθήκης θορύβου.

Αυτή η τεχνική χρησιμοποιεί τη σύγκριση των συντελεστών DCT μεσαίας ζώνης για να κωδικοποιήσουμε ένα bit σε ένα block DCT. Αρχικά ορίζονται οι μεσαίες συχνότητες FM ενός 8x8 block DCT, όπως φαίνεται παρακάτω στην εικόνα,



Εικόνα 27: Ορισμός του DCT Περιφερειών

όπου $\mathbf{F}_{L}$: Στοιχεία χαμηλών συχνοτήτων του block, $\mathbf{F}_{M}$: Στοιχεία μεσαίων συχνοτήτων του block, $\mathbf{F}_{H}$: Στοιχεία υψηλών συχνοτήτων του block

Το F_{M} επιλέγεται ως το πεδίο ενσωμάτωσης για να προσθέσει επιπλέον ανθεκτικότητα ενάντια σε τεχνικές με απώλειες συμπίεσης, αποφεύγοντας παράλληλα τις παραποιήσεις στην αρχική εικόνα.

Έπειτα επιλέγονται οι παρακάτω δύο θέσεις Bi (u1, v1) και Bi (u2, v2) από την περιοχή F_{M} για να γίνει σύγκριση. Αντίθετα,, επιλέγοντας αυθαίρετα τις θέσεις αυτές, μπορούμε να έχουμε

επιπλέον ευρωστία εάν η επιλογή των συντελεστών βασιστεί στον πίνακα κβαντοποίησης JPEG που παρουσιάζονται στον παρακάτω πίνακα. Εάν οι δύο θέσεις επιλεχθούν έτσι ώστε να έχουν τις ίδιες τιμές κβαντοποίησης, τότε κάποια αν τροποποιηθεί το μέγεθος ενός συντελεστή θα προκαλέσει την ίδια αλλαγή και στον άλλο συντελεστή διατηρώντας την αναλογία τους.

16	11	10	26	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Πίνακας 2: Τιμές κβάντισης που χρησιμοποιούνται στο πλαίσιο του καθεστώτος συμπίεσης JPEG

Με βάση τον πίνακα, μπορούμε να παρατηρήσουμε ότι οι συντελεστές (4,1) και (3,2) ή (1,2) και (3,0) θα είναι κατάλληλοι υποψήφιοι για σύγκριση, καθώς οι τιμές κβαντοποίησης τους είναι ίσες. Το μπλοκ DCT θα κωδικοποιήσει " 1" αν η λειτουργία Bi (u1, v1) > Bi (u2, v2) αλλιώς θα κωδικοποιήσει " 0". Οι συντελεστές στη συνέχεια αντιμετατίθενται αν το σχετικό μέγεθος του κάθε

συντελεστή δεν συμφωνεί με το bit που πρόκειται να κωδικοποιηθεί. Η εναλλαγή των εν λόγω συντελεστών δεν μεταβάλλει την υδατογραφημένη εικόνα σημαντικά, καθώς οι συντελεστές DCT των μεσαίων συχνοτήτων έχουν παρόμοιο μέγεθος.

Η ευρωστία του υδατογραφήματος μπορεί να βελτιωθεί με την εισαγωγή μίας σταθεράς k, τέτοια ώστε Bi (u1, v1) - Bi (u2, v2) > k. Οι συντελεστές που δεν πληρούν αυτό το κριτήριο δέχονται τροποποίηση με τη χρήση τυχαίου θορύβου έτσι ώστε να ικανοποιήσουν τη σχέση. Με την αύξηση του k μειώνεται η πιθανότητα ανίχνευσης σφαλμάτων σε βάρος μείωσης της ποιότητας της εικόνας. Μια άλλη πιθανή τεχνική είναι η ενσωμάτωση μιας PN (pseudonoise) ακολουθίας W στις μεσαίες συχνότητες του block DCT. Μπορούμε να διαμορφώσουμε ένα block DCT(x, y) χρησιμοποιώντας την εξίσωση που φαίνεται στην παρακάτω εικόνα.

$$I_{Wx,y}(u,v) = \begin{cases} I_{x,y}(u,v) + k * W_{x,y}(u,v), & u,v \in F_M \\ Ix,y(u,v), & u,v \notin F_M \end{cases}$$

Εικόνα 28: Ενσωμάτωση ενός CDMA υδατογραφήματος στις μεσαίες συχνότητες

Αρχικά υπολογίζουμε το DCT για το κάθε block 8x8 της εικόνας. Σε αυτό το block τα στοιχεία F_M των μεσαίων συχνοτήτων προστίθενται στην ακολουθία W, πολλαπλασιαζόμενη με έναν συντελεστή ενίσχυσης k. Έπειτα, κάθε block μετασχηματίζεται αντίστροφα για να δώσει την τελική υδατογραφημένη εικόνα I_W. Η διαδικασία αυτή μπορεί να γίνει κάπως πιο προσαρμοστική μεταβάλλοντας ελαφρώς τη διαδικασία ενσωμάτωσης που φαίνεται στην εικόνα.

$$I_{Wx,y}(u,v) = \begin{cases} I_{x,y}(u,v) * (1 + k * W_{x,y}(u,v)), & u,v \in F_M \\ Ix,y(u,v), & u,v \notin F_M \end{cases}$$

Εικόνα 29: Εξαρτώμενο από την εικόνα DCT CDMA υδατογράφημα

Με αυτή την ελαφρά τροποποίηση μεταβάλλουμε την ένταση της υδατογραφίας βασιζόμενη στο μέγεθος των συντελεστών που χρησιμοποιούνται. Με αυτό τον τρόπο μπορούμε να χρησιμοποιήσουμε μεγαλύτερα k για συντελεστές μεγαλύτερου μεγέθους, δίνοντας επομένως ένταση στο υδατογράφημα σε περιοχές που είναι εφικτό, και ελαττώνοντας την ένταση σε περιοχές που δεν είναι.

Κατά την διαδικασία της ανίχνευσης, η εικόνα χωρίζεται στα ίδια 8x8 blocks και εκτελείται το DCT. Έπειτα, η ίδια ακολουθία PN συγκρίνεται με τις τιμές μεσαίας συχνότητας των μετασχηματισμένων block. Εάν η συσχέτιση μεταξύ των ακολουθιών υπερβεί κάποιο κατώτατο όριο T, ανιχνεύεται το “1” για το συγκεκριμένο block, διαφορετικά ανιχνεύεται το “0”. Το k δηλώνει την ένταση του υδατογραφήματος, και η αύξησή του αυξάνει την ευρωστία του υδατογραφήματος με ταυτόχρονη μείωση της ποιότητας της εικόνας.

Αποτελέσματα συσχέτισης
Βασισμένη στη σύγκριση (Comparison-Based Correlation)

Μία πιθανή βελτίωση στο κατώτατο όριο με βάση την τεχνική που περιγράφηκε παραπάνω αποτελούν οι δύο διαφορετικές PN ακολουθίες κατά την ενσωμάτωση, μία για την κωδικοποίηση του “1” και μία για την κωδικοποίηση του “0”. Η προσέγγιση αυτή έχει το πλεονέκτημα ότι δεν απαιτείται κάποια αυθαίρετη επιλογή του ορίου, καθώς επιλέγεται το σχήμα με την υψηλότερη συσχέτιση. Επιπλέον, με προσεκτική επιλογή των δύο αυτών υποδειγμάτων ώστε να υπάρχει όσο το δυνατό λιγότερο συσχέτιση μεταξύ τους, μπορεί να μειωθεί σημαντικά η πιθανότητα λανθασμένης ανίχνευσης.

Ένα ακόμη πλεονέκτημα είναι πως η προσέγγιση αυτή κάνει καλύτερη χρήση του HVS (Human Visual System) διαδίδοντας το θόρυβο μέσα σε ολόκληρη την εικόνα. Το ανθρώπινο μάτι είναι πιο ευαίσθητο στις απότομες αλλαγές της ποιότητας, με αποτέλεσμα τα blocks του θορύβου να τείνουν να ενοχλούν τους θεατές περισσότερο απ’ ότι ένα σταθερό επίπεδο θορύβου σε ολόκληρη την εικόνα. Παρακάτω βλέπουμε πως η εικόνα παραμένει σχεδόν ανέπαφη, παρόλο που το PSNR είναι ίσο με 5,0823e + 003.

Για k=5 blocksize=16

watermark

watermarked image

recovered image

Μια ακόμη παρατήρηση είναι πως στην τεχνική comparison-based το υδατογράφημα με συντελεστή k=5 ενσωματώνεται καλύτερα από την τεχνική threshold-based με k=40. Ο λόγος είναι ότι επηρεάζεται λιγότερο η ποιότητα της εικόνας, καθώς επίσης βελτιώνεται η ευρωστία του

υδατογραφήματος. Επομένως, comparison-based προσέγγιση με k=5 ανταγωνίζεται επιτυχώς την threshold-based με k=40.

4.2.5 Σύγκριση συντελεστών DCT μεσαίων συχνοτήτων

Τα αποτελέσματα της σύγκρισης των συντελεστών DCT μεσαίων συχνοτήτων είναι ενθαρρυντικά. Το k στην περίπτωση αυτή δεν είναι κάποιος συντελεστής ενίσχυσης όπως στην τεχνική correlation-based, αλλά ένα κατώτατο όριο (threshold). Οι συντελεστές τροποποιούνται ώστε οι διαφορές στο μέγεθος μεταξύ των δύο συντελεστών που συγκρίνονται να μην υπερβαίνουν το k. Αν και οι μεγαλύτερες τιμές του k θα έχουν ως αποτέλεσμα την αύξηση της ευρωστίας επιλέξαμε να είναι ίσο με 50, αλλά σε βάρος της ποιότητας της εικόνας.

Για k=50

watermark

watermarked image

recovered watermark

Στην παραπάνω εικόνα παρατηρούμε πως η τεχνική έχει πολύ καλά αποτελέσματα ανάκτησης για εικόνες που δεν έχουν υποστεί τροποποιήσεις με καλή ποιότητα της υδατογραφημένης εικόνας, στην οποία εμφανίζεται ένα χαμηλό επίπεδο θορύβου. Το μέγεθος του block διατηρήθηκε σταθερό στο 8x8. Αν αυξηθεί το μέγεθος των block αλλά ταυτόχρονα να μειωθεί η χωρητικότητα του μηνύματος μπορούν να επιτευχθούν καλύτερα αποτελέσματα.

4.2.6 Συσχέτιση βασισμένη στη σύγκριση στις μεσαίες ζώνες DCT

Τα αποτελέσματα από τις correlation-based DCT τεχνικές είναι παρόμοια. Το correlation-based DTC φαίνεται να είναι βελτιωμένο στα υψηλότερα επίπεδα επεξεργασίας της εικόνας αλλά μη ικανοποιητικό στα χαμηλότερα επίπεδα.

Για k=15

watermark

watermarked image

recovered watermarked

Αν και στην αρχική εικόνα δεν υπάρχουν ορατές παραποιήσεις, μπορούμε να παρατηρήσουμε μια σειρά από σφάλματα στην ανίχνευση του υδατογραφήματος, χωρίς όμως αυτό να καθίσταται μη αναγνώσιμο. Τα αποτελέσματα της τεχνικής αυτής με υψηλό συντελεστή k αποσπούν περισσότερο τον θεατή σε σύγκριση με τον θόρυβο που εμφανίστηκε στην υδατογραφημένη εικόνα, όπως παρουσιάστηκε με τη χρήση του συντελεστή σύγκρισης στην προηγούμενη εφαρμογή. Τα σφάλματα που παρατηρούνται στην ανάκτηση μπορούν να απαλειφθούν, εάν επιλεχθούν ξεχωριστές ακολουθίες PN για το κάθε block. Παρόλα αυτά η

διαδικασία αυτή απαιτεί μία αλλαγή στην threshold-based ανίχνευση και έτσι πολύ πιθανόν να παρουσιαστεί πρόβλημα στην εκτέλεση της τεχνικής.

Κεφάλαιο 5

Επιθέσεις και Παραμορφώσεις

Η ασφάλεια ενός υδατογραφήματος βασίζεται στην ικανότητα του να αντιστέκεται σε κακόβουλες επιθέσεις. Κακόβουλη επίθεση είναι κάθε διαδικασία που έχει στόχο την παρεμπόδιση του σκοπού του υδατογραφήματος. Παρακάτω αναφέρουμε τα διάφορα είδη επιθέσεων:

Απλές επιθέσεις: Είναι γενικά επιθέσεις χαμηλής πολυπλοκότητας που ως στόχο έχουν να καταστρέψουν το υδατογράφημα μέσω μετασχηματισμών στο σύνολο των δεδομένων (ψηφιακό υλικό και υδατογράφημα), χωρίς να στοχεύουν στην αναγνώριση και απομόνωση του

υδατογραφήματος. Είναι γνωστές και ως επιθέσεις θορύβου (noise attacks). Σαν παράδειγμα μπορούμε να αναφέρουμε την εφαρμογή φίλτρων (γραμμικών ή μη γραμμικών), τη συμπίεση με απώλειες (JPEG, MPEG), την προσθήκη θορύβου, την αφαίρεση κομματιών της εικόνας (cropping), την κβάντιση στο πεδίο του χώρου, τη μετατροπή της εικόνας σε αναλογική κλπ. Ο απλούστερος τρόπος άμυνας απέναντι στις επιθέσεις θορύβου είναι η αύξηση του πλάτους του υδατογραφήματος, γι' αυτό είναι πολλές φορές απαραίτητη και η χρήση των οπτικών μοντέλων. Άλλος ένας τρόπος είναι η ένθεση με πλεονασμό (redundant embedding), η οποία πραγματοποιείται με την ένθεση του υδατογραφήματος πολλές φορές (σε διαφορετικά μέρη της εικόνας ή της εικονοσειράς).

Επιθέσεις συγχρονισμού: Είναι οι επιθέσεις που ως σκοπό έχουν είτε να καταστήσουν το υδατογράφημα μη ανιχνεύσιμο, είτε να κάνουν την ανίχνευση χρονοβόρα και τελικά ασύμφορη διαδικασία. Αυτό επιτυγχάνεται πολύ εύκολα με απλούς γεωμετρικούς μετασχηματισμούς, όπως με μεγέθυνση ή σμίκρυνση της εικόνας, περιστροφή, αποκοπή δεδομένων (cropping), υποδειγματοληψία, εισαγωγή ή αφαίρεση pixel και γενικά με κάθε είδους γεωμετρικό μετασχηματισμό. Μία τυπική ιδιότητα αυτού του είδους επίθεσης είναι ότι το υδατογράφημα στην πραγματικότητα παραμένει στα δεδομένα και μπορεί να ανακτηθεί με κάποια επέκταση της μεθόδου ανάκτησής του.

Επιθέσεις αντιστροφής: Οι επιθέσεις αυτές είναι γνωστές και ως «επιθέσεις ψευδών υδατογραφημάτων». Σκοπός τους είναι να καταστήσουν τα υδατογραφήματα «αμφιβόλου γνησιότητας», κυρίως με την εισαγωγή πολλών επιπλέον υδατογραφημάτων, έτσι ώστε να μην είναι δυνατό να γνωρίζει κανείς ποιο ήταν το αρχικό.

Επιθέσεις αφαίρεσης του υδατογραφήματος: Όπως δηλώνει το όνομά τους, ο σκοπός τέτοιων επιθέσεων είναι να απομακρύνουν το υδατογράφημα. Έτσι επιχειρείται εκτενής ανάλυση των υδατογραφημένων δεδομένων, γίνεται εκτίμηση του υδατογραφήματος διαχωρίζονται τα αρχικά δεδομένα από το υδατογράφημα το οποίο τελικά απορρίπτεται. Ως παραδείγματα μπορούμε να αναφέρουμε την αποθορυβοποίηση, τη χρήση συγκεκριμένων μεθόδων εφαρμογής μη γραμμικών φίλτρων κλπ. Στην ίδια επίσης κατηγορία ανήκουν και οι επιθέσεις που αναφέρονται σε μία συγκεκριμένη μέθοδο υδατογράφησης και επιχειρούν να εκμεταλλευτούν τις ενδεχόμενες αδυναμίες του συστήματος. Επίσης, στην κατηγορία αυτή ανήκει και η λεγόμενη collusion attack, η οποία προσπαθεί να αναλύσει τον τρόπο που επιδρά το σύστημα υδατογράφησης στην εικόνα, εξετάζοντας αναλυτικά πολλά αντίγραφα της ίδιας εικόνας που έχουν υδατογραφηθεί με το σύστημα αυτό, αλλά περιέχουν διαφορετικά υδατογραφήματα

Πρέπει να σημειωθεί ότι δεν μπορεί πάντοτε να γίνει σαφής διαχωρισμός μεταξύ των διαφόρων ειδών επιθέσεων που αναφέρθηκαν παραπάνω. Κάποιες επιθέσεις μπορεί να ανήκουν σε περισσότερες από μία κατηγορίες, όπως για παράδειγμα η αποκοπή δεδομένων (cropping) μπορεί να θεωρηθεί ότι ανήκει τόσο στις απλές όσο και στις επιθέσεις συγχρονισμού, όπως επίσης και η αποθορυβοποίηση αλλά και η εφαρμογή μη γραμμικών φίλτρων μπορεί να καταταχθεί είτε στις απλές είτα στις επιθέσεις αφαίρεσης. Επίσης οι collusion attacks θα μπορούσαν να αποτελέσουν ανεξάρτητη ομάδα, καθώς, αντίθετα από άλλες επιθέσεις, απαιτούν περισσότερα από ένα, διαφορετικά υδατογραφημένα αντίγραφα.

Επομένως ένα υδατογραφημένο αντικείμενο μπορεί τυχαία και μη να τροποποιηθεί. Έτσι το σύστημα ανίχνευσης και εξαγωγής του υδατογραφήματος θα πρέπει να είναι σε θέση να ανταπεξέλθει στις όποιες τροποποιήσεις της εικόνας.

Ένα είδος επιθέσεων είναι και οι παραμορφώσεις οι οποίες πρέπει να είναι περιορισμένες στην υπερβολική υποβάθμιση έτσι ώστε το μετασχηματισμένο αντικείμενο να είναι κατάλληλο προς χρήση. Εφόσον ο επιτιθέμενος δεν γνωρίζει το μυστικό κλειδί που χρησιμοποιείται κατά τη

διαδικασία εισαγωγής του υδατογραφήματος, στόχος του είναι η απώλεια του υδατογραφήματος να είναι η μέγιστη δυνατή, για να μειώσει όσο το δυνατό περισσότερο την παραμόρφωση που παράγεται στο αντικείμενο.

Παρακάτω αναφέρονται ονομαστικά μερικές από τις πιο γνωστές επιθέσεις όπως:

- Προσθετικός θόρυβος
- Φιλτράρισμα
- Εξισορρόπηση ιστογράμματος
- Περιστροφή
- Κλιμάκωση
- Κοπή
- Συμπίεση

5.1 Προσθετικός θόρυβος

Υπάρχουν διάφορα είδη θορύβου στις ψηφιακές εικόνες που σχετίζονται άμεσα με τον τρόπο δημιουργίας/ λήψης των εικόνων. Μια γενική κατηγοριοποίηση τους είναι ο προσθετικός και ο πολλαπλασιαστικός θόρυβος. Ένα παράδειγμα πολλαπλασιαστικού θορύβου είναι ο μεταβλητός φωτισμός. Αυτός είναι ίσος ο συνηθέστερος τύπος θορύβου στην εικόνα. Ο πρόσθετος θόρυβος συχνά είναι κρουστικός θόρυβος (impulse noise) ή **θόρυβος Gauss.**

Ο προσθετικός θόρυβος έχει συνήθως μηδενική μέση τιμή (zero-mean) και μπορεί να χαρακτηριστεί από την μεταβλητότητα του σ_n^2. Η επίπτωση του θορύβου στις εικόνες μπορεί να περιγραφεί από το **λόγο σήματος προς το όριο (SNR-signal to noise ratio)**. Ένας ορισμός με το SNR είναι ο ακόλουθος:

$$SNR = \frac{\sigma_s}{\sigma_n} = \sqrt{\frac{\sigma_f^2}{\sigma_n^2} - 1}$$

όπου σ_n^2 και σ_f^2 είναι οι μεταβλητότητες τις αρχικής εικόνας και της εικόνας με θόρυβο, αντίστοιχα.

Ένας διαφορετικός δείκτης είναι ο **PSNR (peak to noise ratio)** ο οποίος μας δίνει σε decibels, το λόγο του μέγιστου σήματος προς θόρυβο μεταξύ δύο εικόνων. Όσο υψηλότερο είναι το PSNR, τόσο λιγότερο θόρυβο έχουμε στην εικόνα το PSNR ορίζεται ως εξής:

$$PSNR = 10 \cdot \log_{10}\left(\frac{D^2}{MSE}\right)$$

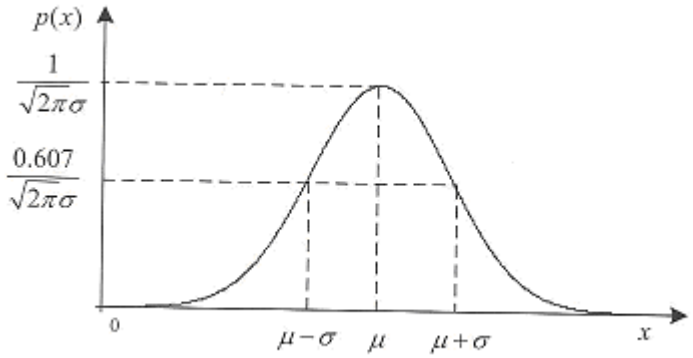
Στην εξίσωση αυτή, το **D** ισούται με την μέγιστη διακύμανση της αρχικής εικόνας.

5.1.1 Θόρυβος Gauss

Ο θόρυβος Gauss χρησιμοποιείται συνήθως για να περιγράψει αθροιστικό θόρυβο στις εικόνες. Αν και αντιστοιχίζεται σε ορισμένα είδη θορύβου, όπως ο θόρυβος κουκίδας και ο θερμικός θόρυβος, πολλές φορές γίνεται κατάχρηση της χρήσης του λόγω της απλότητας στην περιγραφή του.
Ο θόρυβος Gauss, για μια τυχαία μεταβλητή x, ικανοποιεί την ακόλουθη συνάρτηση πυκνότητας πιθανότητας

$$p(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

όπου **μ** η μέση τιμή και **σ** η τυπική απόκλιση.



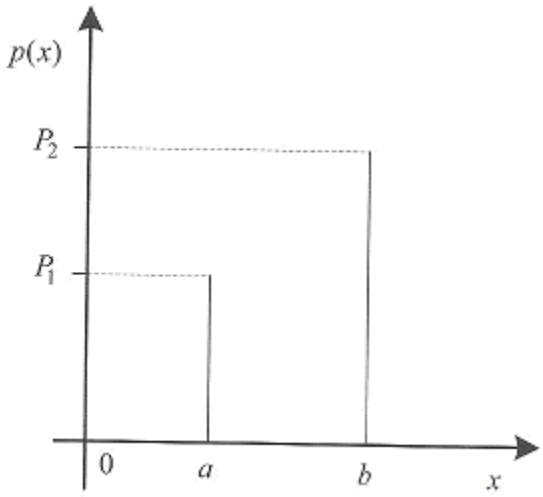
Εικόνα 30: Συνάρτηση πυκνότητας πιθανότητας της κατανομής Gauss

Με το matlab μπορούμε να προσθέσουμε θόρυβο Gauss σε μια εικόνα με τη βοήθεια της συνάρτησης *J=imnoise(I,'gaussian',m,s).* Οι τιμές προεπιλογής είναι m=0 και s=0.1.

5.1.2 Κρουστικός θόρυβος

Ο κρουστικός θόρυβος (impulse noise) καλείται συνήθως και θόρυβος αλάτι και πιπέρι (salt and pepper). Είναι μία μορφή θορύβου που φαίνεται χαρακτηριστικά στις εικόνες και εμφανίζεται ως τυχαία άσπρα και μαύρα εικονοστοιχεία. Είναι σαν να ρίχνουμε αλάτι και πιπέρι σε ένα γκρι φύλλο χαρτιού. Ο θόρυβος αυτός μπορεί να δημιουργηθεί από τους αισθητήρες χρώματος. Ένα λάθος στην απόδοση της καθαρότητας του χρώματος (saturation) ή μία αποτυχία απόκρισης του αισθητήρα μπορεί να οδηγήσουν σε λευκά και μαύρα εικονοστοιχεία, αντίστοιχα. Γενικά θα λέγαμε ότι ο κρουστικός θόρυβος έχει σαν αποτέλεσμα ορισμένα εικονοστοιχεία της εικόνας να έχουν «ανώμαλα» επίπεδα φωτεινότητας έναντι των γειτονικών τους. Τα «αλατισμένα» εικονοστοιχεία έχουν υψηλά επίπεδα φωτεινότητας, ενώ τα εικονοστοιχεία με θόρυβο «πιπεριού» έχουν πολύ χαμηλά.

Όπως φαίνεται στην εικόνα 31 η μοντελοποίηση του κρουστικού θορύβου γίνεται συνήθως με τη θεώρηση δύο σταθμών φωτεινότητας, έστω a και b με b > > a. Συνήθως για μια εικόνα αποχρώσεων του γκρι θεωρούμε ότι a=0 και b=255. Οι πιθανότητες P1=p(a) και P2=p(b) πρέπει να είναι μικρότερες από 0.1 ώστε να μην υπάρχει υπερίσχυση του θορύβου έναντι της εικόνας. Σύμφωνα με τα παραπάνω, η συνάρτηση πυκνότητας του κρουστικού θορύβου έχει τη μορφή:



Εικόνα 31: Συνάρτηση πυκνότητας πιθανότητας του κρουστικού θορύβου

Στο matlab μπορούμε να προσθέσουμε κρουστικό θόρυβο με τη βοήθεια της συνάρτησης J=imnoise(I,'salt & pepper',D) όπου το D εκφράζει την πυκνότητα του θορύβου. Οι τιμή προεπιλογής για το D είναι 0.05.

5.2 Φιλτράρισμα

Το φιλτράρισμα της εικόνας έχει ως σκοπό την οπτική βελτίωση της εικόνας, σχετικά με την χωρική διαχωριστική της ικανότητα (spatial scale information).

Οι μέθοδοι φιλτραρίσματος εικόνων είναι οι δύο βασικών τύπων:

- Χωρικό φιλτράρισμα (Spatial domain filtering)
- Φιλτράρισμα συχνοτήτων (Frequency domain filtering) ή φίλτρα Fourier

5.2.1 Χωρικά Φίλτρα

Το χωρικό φιλτράρισμα είναι μια συνηθισμένη λειτουργία που εφαρμόζεται στα δεδομένα ψηφιακής εικόνας για να ενισχύσει ή να υποβαθμίσει τη χωρική λεπτομέρεια και για να βελτιωθεί η οπτική ερμηνεία. Τυπικά παραδείγματα είναι η εφαρμογή φίλτρων για να ενισχυθεί η λεπτομέρεια των ακμών στις εικόνες, ή για να αφαιρεθούν ή να μειωθούν μορφές θορύβου σε μία εικόνα. Στην επεξεργασία εικόνας, το χωρικό φιλτράρισμα καλείται "τοπική λειτουργία", επειδή τροποποιεί την τιμή κάθε εικονοστοιχείου στην εικόνα ανάλογα με τις τιμές των εικονοστοιχείων που το περιβάλλουν. Τα φίλτρα δουλεύουν με την αφαίρεση ορισμένων φασματικών ή χωρικών συχνοτήτων για να βελτιωθούν τα χαρακτηριστικά στην υπόλοιπη εικόνα.

Ένα χαρακτηριστικό κοινό σε όλους τους τύπους ψηφιογραφικών δεδομένων, είναι η χωρική συχνότητα (spatial frequency), η οποία καθορίζει το μέγεθος των μεταβολών στις τιμές των δεδομένων ανά μονάδα απόστασης για κάθε συγκεκριμένο τμήμα μίας εικόνας. Περιοχές της εικόνας με μικρές μεταβολές ή βαθμιαίες αλλαγές των τιμών δεδομένων σε ένα δεδομένο τμήμα ονομάζονται περιοχές χαμηλής συχνότητας (low frequency). Περιοχές σε μεγάλες μεταβολές ή γρήγορες αλλαγές ονομάζονται περιοχές υψηλής συχνότητας (high frequency).

Τα χωρικά φίλτρα μπορούν να χωριστούν σε τρεις γενικές κατηγορίες:

- Τα φίλτρα χαμηλής συχνότητας (χαμηλοδιαβατά φίλτρα) σχεδιάζονται για να τονίσουν τα χαρακτηριστικά χαμηλών συχνοτήτων (μεταβολές φωτεινότητας μεγάλων περιοχών) και να αποδυναμώσουν τις υψηλές συχνότητες μίας εικόνας (τοπικές λεπτομέρειες). Δεδομένου ότι υποβαθμίζουν τη λεπτομέρεια σε μία εικόνα, τα φίλτρα χαμηλών συχνοτήτων μερικές φορές καλούνται φίλτρα εξομάλυνσης ή φίλτρα μέσης τιμής. Τα φίλτρα αυτά τονίζουν την λεπτομέρεια χαμηλής συχνότητας για να εξομαλύνουν το θόρυβο εικόνας ή να μειώσουν τα ακραία δεδομένα.
- Τα φίλτρα υψηλών συχνοτήτων (υψηπερατά φίλτρα) κάνουν ακριβώς το αντίθετο, δηλαδή, τονίζουν τις χωρικές λεπτομέρειες που σχετίζονται με τις υψηλές συχνότητες μίας εικόνας, και αποδυναμώνουν τις πλέον γενικές πληροφορίες, οι οποίες συνδέονται με τις χαμηλές συχνότητες. Τα φίλτρα υψηλών συχνοτήτων καλούνται μερικές φορές φίλτρα όξυνσης επειδή γενικά χρησιμοποιούνται για να ενισχύσουν τη λεπτομέρεια χωρίς να επηρεάζονται τα τμήματα χαμηλής συχνότητας της εικόνας. Τα φίλτρα αυτά τονίζουν τη λεπτομέρεια υψηλής συχνότητας για να ενισχύσουν ή να οξύνουν γραμμικά χαρακτηριστικά όπως δρόμοι, ρήγματα και όρια εδάφους / νερού.
- Τα φίλτρα ανίχνευσης ακμών (edge detection filters) τονίζουν τις ακμές που περιβάλλουν αντικείμενα ή χαρακτηριστικά σε μία εικόνα για να καταστήσει ευκολότερη την ανάλυση τους. Τα φίλτρα ανίχνευσης ακμών δημιουργούν συνήθως μία εικόνα με γκρίζο φόντο και μαύρες και άσπρες γραμμές που περικλείουν τις ακμές των αντικειμένων και των χαρακτηριστικών στην εικόνα.

5.2.1.1 Φίλτρα μέσης τιμής (mean filter)

Το φίλτρο μέσης τιμής χρησιμοποιείται για την εξομάλυνση των εικόνων και την μείωση του θορύβου σε αυτές. Η λειτουργία του συνίσταται στην αντικατάσταση της φωτεινότητας σε κάθε εικονοστοιχείο, με την μέση φωτεινότητα σε μία γειτονιά του. Αυτό έχει ως αποτέλεσμα την μείωση της μεταβλητότητας τοπικά σε κάθε εικονοστοιχείο και συνεπώς το θάμπωμα της εικόνας.

Συγκεκριμένα, αν N είναι η γειτονιά του εικονοστοιχείου (i, j) μιας εικόνας I, τότε η τιμή του εικονοστοιχείου (i,j) αντικαθίσταται με την βοήθεια της σχέσης: $\mathrm{I}(\mathrm{i},\mathrm{j}) = \frac{1}{\mathrm{M}}\sum_{(\mathrm{x},\mathrm{y})\in\mathrm{N}} \mathrm{I}(\mathrm{x},\mathrm{y})$
όπου M το πλήθος των εικονοστοιχείων της γειτονιάς N.

Η γειτονιά N είναι συνήθως καθορισμένη για κάθε επεξεργασία και συνήθως αντιστοιχεί σε τετράγωνες μάσκες που καθορίζονται με βάση την απόσταση (ακτίνα) από το εικονοστοιχείο αναφοράς. Έτσι, για ακτίνα ίση με ένα έχουμε ουσιαστικά μια γειτονιά διαστάσεων 3x3 η οποία όμως προσαρμόζεται κατάλληλα στις περιοχές των ορίων της εικόνας. Πρακτικά, ένα 3x3 φίλτρο μέσης τιμής μπορεί να υλοποιηθεί με μια μάσκα της μορφής: $\frac{1}{9}\begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix}$

Όσο μεγαλύτερων διαστάσεων είναι η γειτονιά, τόσο μεγαλύτερη εξομάλυνση επιτυγχάνεται και τόσο περισσότερες λεπτομέρειες της εικόνας εξαφανίζονται. Το φίλτρο μέσης τιμής μπορεί να θεωρηθεί ως ένα κατωδιαβατό φίλτρο το οποίο έχει ως αποτέλεσμα την απαλοιφή των στοιχείων της εικόνας που αντιστοιχούν σε υψηλές συχνότητες και οι οποίες ουσιαστικά αφορούν λεπτομέρειες της εικόνας. Αν θέλουμε να τονίσουμε περισσότερο τη συνεισφορά των εικονοστοιχείων ανάλογα με την απόσταση τους, τότε μπορούμε να χρησιμοποιήσουμε μάσκες εξομάλυνσης όπως $\frac{1}{16}\begin{bmatrix}1 & 2 & 1\\ 2 & 4 & 2\\ 1 & 2 & 1\end{bmatrix}$

5.2.1.2 Φίλτρα μεσαίας τιμής (median filter)

Το φιλτράρισμα με ένα φίλτρο μεσαίας τιμής είναι μια τεχνική που αρχικά αναπτύχθηκε για τη μείωση του θορύβου σε ψηφιακές εικόνες. Η τιμή median ενός συνόλου Α είναι ίση με τη μεσαία τιμή του συνόλου. Σε ένα σύνολο το οποίο έχει περιττό αριθμό στοιχείων, ταξινομούμε τα στοιχεία του συνόλου κατ' αύξουσα τιμή, οπότε το median του συνόλου ισούται με το μεσαίο στοιχείο αν έχουμε περιττό αριθμό στοιχείων ή με τη μέση τιμή των δύο γειτονικών μεσαίων στοιχείων στην περίπτωση άρτιου αριθμού στοιχείων.

Το φίλτρο μεσαίας τιμής χρησιμοποιείται για την εξομάλυνση (smoothing) των ακμών και τη μείωση του θορύβου μιας εικόνας.

Στο matlab εκτελείται το μεσαίο φιλτράρισμα στην εικόνα Α σε δύο διαστάσεις. Συγκεκριμένα, η εντολή *B= medfilt2(A,[m n])* εκτελεί φίλτρο μεσαίας τιμής με γειτονιά m x n γύρω από το αντίστοιχο εικονοστοιχείο Α(x,y). Αν δεν υπάρχει ο καθορισμός της γειτονιάς τότε νοείται μια γειτονιά διαστάσεων 3x3. Στην περίπτωση αυτή η εντολή έχει τη μορφή *B= medfilt2(A).*

Το κυριότερο μειονέκτημα της εφαρμογής του φίλτρου median με ορθογωνική γειτονιά είναι η καταστροφή που επιφέρει σε λεπτές γραμμές και σαφείς γωνίες. Το πρόβλημα αυτό μπορεί να αντιμετωπιστεί με την χρησιμοποίηση γειτονιάς κατάλληλης μορφής.

Τα φίλτρα median μπορούν να θεωρηθούν ως ειδική περίπτωση των φίλτρων rank, τα οποία βασίζονται στην κατάταξη των δεδομένων μιας γειτονιάς σε μια ακολουθία σύμφωνα με κάποιους κανόνες. Παρόμοια φίλτρα είναι τα φίλτρα που ονομάζονται order statistics (OS) σύμφωνα με τα οποία οι τιμές της γειτονιάς ταξινομούνται σε μια ακολουθία και η τιμή που σε κάθε γειτονιά προκύπτει από το γραμμικό συνδυασμό των τιμών αυτών.

5.2.1.3 Φίλτρα min/max

Τα φίλτρα min/max (ελαχίστου/ μεγίστου) είναι μη γραμμικά φίλτρα τάξης, μπορούν να υλοποιηθούν με τη βοήθεια μασκών και προσομοιάζουν με τις μορφολογικές λειτουργίες της διαστολής (dilation) και συστολής (erosion). Το φίλτρο ελαχίστου έχει ως αποτέλεσμα να απλώνει μαύρες περιοχές και να συρρικνώνει λευκές. Μπορεί να χρησιμοποιηθεί για την αφαίρεση λευκών κουκίδων θορύβου. Αντίθετα, το φίλτρο μεγίστου απλώνει λευκές περιοχές και συρρικνώνει μαύρες. Έτσι, χρησιμοποιείται και για την απαλοιφή μαύρων κουκίδων θορύβου. Επιπλέον, τα φίλτρα min/max μπορούν να χρησιμοποιηθούν για να κάνουν πιο ευδιάκριτα ασαφή περιγράμματα και να τονίσουν ασαφή γκρι αντικείμενα.

Τα φίλτρα min/max δεν έχουν την ικανότητα να αφαιρέσουν μικτό κρουστικό θόρυβο. Η υλοποίηση τους με μάσκες γίνεται με τον καθορισμό της μορφής της περιοχής και την αντικατάσταση του κεντρικού εικονοστοιχείου με τη μέγιστη ή την ελάχιστη τιμή.

Στο matlab, η υλοποίηση των φίλτρων min/max γίνεται με την παρακάτω εντολή:
Y= ordfilt2(X, k, M) όπου

- Χ ο πίνακας της εικόνας,
- k=1 για φίλτρο ελαχίστου και k=9 για φίλτρο μεγίστου, και
- Μ πίνακας που περιγράφει μια 3x3 γειτονιά

5.2.1.4 Φίλτρα Gauss

Τα φίλτρα Gauss είναι κατωδιαβατά (low-pass) φίλτρα και συνεπώς εκτός της ικανότητας φιλτραρίσματος θορύβου επιφέρουν θάμπωση στην εικόνα. Για τον προσεγγιστικό σχεδιασμό των φίλτρων Gauss μπορούμε να χρησιμοποιήσουμε τους συντελεστές του διωνυμικού αναπτύγματος: $(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n$.

Με άλλα λόγια, χρησιμοποιούμε τη γραμμή n από το τρίγωνο του Pascal ως μια διάστασης προσέγγιση του φίλτρου Gauss. Ένα φίλτρο Gauss δύο διαστάσεων μπορεί να υλοποιηθεί με διαδοχικές συνελίξεις δύο μονοδιάστατων φίλτρων Gauss, το ένα στην οριζόντια διεύθυνση και το άλλο στην κάθετη διεύθυνση. Επίσης, μπορεί να υλοποιηθεί χρησιμοποιώντας μόνο την μία μονοδιάστατη μάσκα μετασχηματίζοντας την εικόνα ανάμεσα στις συνελίξεις και μετά την τελική συνέλιξη.

Αυτή η τεχνική λειτουργεί καλά για τάξης φίλτρων μέχρι περίπου n=10. Για μεγαλύτερα φίλτρα, οι συντελεστές στο διωνυμικό ανάπτυγμα είναι πολύ μεγάλοι για τους περισσότερους υπολογιστές, ωστόσο, αυθαίρετα μεγάλα φίλτρα Gauss μπορούν να υλοποιηθούν εφαρμόζοντας επανειλημμένα ένα μικρότερο φίλτρο Gauss.

5.2.1.5 Υψηπερατά Φίλτρα

Η ανάδειξη και ο τονισμός των λεπτομερειών μιας εικόνας μπορεί να γίνει με τη χρήση υψηπερατών φίλτρων. Αυτό μπορεί να επιτευχθεί εύκολα αν από την αρχική εικόνα αφαιρέσουμε μια εξομαλυμένη έκδοση της (για παράδειγμα μετά από την εφαρμογή μιας μάσκας μέσης τιμής ή καλύτερα ενός φίλτρου Gauss). Το υψηπερατό φιλτράρισμα (high pass filtering) στο πεδίο του χώρου μπορεί να γίνει με την χρησιμοποίηση μασκών που αποτελούνται από ένα μείγμα θετικών και αρνητικών συντελεστών.

Όπως είναι φανερό, τα υψηπερατά φίλτρα τονίζουν τις λεπτομέρειες της εικόνας, όπως είναι οι ακμές. Ένα υψηπερατό φίλτρο πρέπει να έχει παρόμοια απόκριση ανεξάρτητα από την διεύθυνση μεταβολής της φωτεινότητας. Για το σκοπό αυτό, οι συντελεστές κατανέμονται συμμετρικά ως προς το κέντρο της μάσκας. Επίσης, πρέπει να έχει θετικούς συντελεστές στο κέντρο της μάσκας και αρνητικούς στην περιφέρεια. Η κλασική υλοποίηση ενός 3x3 υψηπερατού φίλτρου είναι η ακόλουθη: $\begin{bmatrix} -1 & -1 & -1 \\ -1 & 8 & -1 \\ -1 & -1 & -1 \end{bmatrix}$.

Παρατηρούμε ότι το άθροισμα των συντελεστών σε αυτή τη μάσκα είναι ίσο με μηδέν. Αυτό σημαίνει ότι, όταν η μάσκα εφαρμόζεται σε μια περιοχή σταθερής ή αργά μεταβαλλόμενης φωτεινότητας, το αποτέλεσμα θα είναι μηδέν ή κοντά στο μηδέν. Όμως, όταν έχουμε περιοχές με γρήγορα μεταβαλλόμενες φωτεινότητες και επειδή η μάσκα περιέχει θετικούς και αρνητικούς συντελεστές, το αποτέλεσμα της εφαρμογής της μάσκας θα είναι ένας μεγάλος θετικός ή αρνητικός αριθμός. Επομένως, πρέπει να απεικονίσουμε τις τιμές που προκύπτουν στην περιοχή [0,255]. Αν και αυτό μπορεί να γίνει εύκολα με κατάλληλη κλιμάκωση των αριθμών, συνήθως η απόκριση 0 της μάσκας τίθεται στο μέσο της κλίμακας. Έτσι, η αρνητική απόκριση του φίλτρου αντιστοιχίζεται σε σκοτεινούς τόνους ενώ η θετική απόκριση δίνει φωτεινούς τόνους.

5.1.2.6 Φίλτρα Ευκρίνειας (Sharpening filter)

Όπως είδαμε παραπάνω, ένα υψηπερατό φίλτρο μπορεί να καταλήξει σε μια μάσκα της μορφής: $\begin{bmatrix}-1 & -1 & -1\\ -1 & 8 & -1\\ -1 & -1 & -1\end{bmatrix}$ με μηδενικό άθροισμα συντελεστών. Προκειμένου να διατηρήσουμε και στοιχεία της εικόνας που αντιστοιχούν σε χαμηλές συχνότητες, μπορούμε να αυξήσουμε κατάλληλα την τιμή του κεντρικού στοιχείου της μάσκας και παράλληλα να διαιρέσουμε όλα τα στοιχεία της μάσκας με ένα αριθμό ώστε το τελικό άθροισμα να ισούται με μονάδα. Συγκεκριμένα, αν S είναι το άθροισμα των συντελεστών της μάσκας εξαιρουμένης της κεντρικής τιμής, τότε μπορούμε να θέσουμε ως κεντρική τιμή της μάσκας μία ποσότητα ίση με S+K και να διαιρέσουμε ταυτόχρονα με K. Ορισμένες μάσκες αυτής της κατηγορίας είναι οι ακόλουθες:

$$\begin{bmatrix}0 & -1 & 0\\ -1 & 5 & 1\\ 0 & 1 & 0\end{bmatrix} \quad \begin{bmatrix}1 & -2 & 1\\ -2 & 5 & -2\\ 1 & 2 & 1\end{bmatrix} \quad \frac{1}{7}\begin{bmatrix}1 & -2 & -1\\ -2 & 19 & 2\\ -1 & 2 & -1\end{bmatrix}$$

$$\frac{1}{14}\begin{bmatrix}0 & -1 & -1 & -1 & 0\\ -1 & -2 & -4 & -2 & 1\\ -1 & -4 & 50 & -4 & -1\\ -1 & -2 & 4 & -2 & -1\\ 0 & -1 & 1 & -1 & 0\end{bmatrix} \quad \frac{1}{10}\begin{bmatrix}1 & -1 & -1 & -1 & -1\\ -1 & -2 & -2 & -2 & 1\\ -1 & 2 & 42 & -2 & -1\\ -1 & -2 & 2 & -2 & -1\\ -1 & -1 & 1 & -1 & -1\end{bmatrix}$$

Πρέπει να σημειώσουμε ότι πριν την εφαρμογή ενός φίλτρου ευκρίνειας πρέπει, κατά το δυνατόν, να προηγείται φιλτράρισμα της εικόνας για την μείωση του θορύβου.

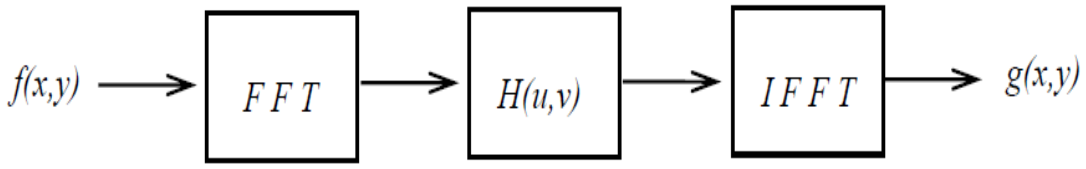
5.2.2 Επεξεργασίες στο πεδίο των χωρικών συχνοτήτων

Η ανάπτυξη τεχνικών βελτίωσης στο πεδίο των χωρικών συχνοτήτων στηρίχτηκε στα ισχυρά μαθηματικά εργαλεία της Θεωρίας Σημάτων και Συστημάτων δύο διαστάσεων. Στην πλειοψηφία των περιπτώσεων, απαραίτητο συστατικό στοιχείο στην υλοποίηση των τεχνικών αυτών είναι ο πασίγνωστος αλγόριθμος **FFT (Fast Fourier Transform)** ο οποίος υπολογίζει τον **DFT (Discrete Fourier Transform)** με θεαματικά χαμηλή υπολογιστική πολυπλοκότητα. Παρακάτω θα δούμε δύο γενικά σχήματα που καλύπτουν την πλειοψηφία των επεξεργασιών αυτού του τύπου.

5.2.2.1 Γραμμικά Φίλτρα στο Πεδίο Συχνοτήτων

Όπως και στην περίπτωση των χωρικών φίλτρων έτσι κι εδώ έχουμε δύο βασικές κατηγορίες φίλτρων, τα χαμηλοπερατά και τα υψηπερατά με χρήσεις αντίστοιχες με αυτές που έχουν ήδη περιγραφεί. Μια κατηγορία φίλτρων που χρησιμοποιούνται ευρέως στο πεδίο συχνοτήτων είναι τα λεγόμενα φίλτρα **Butterworth** τα οποία λόγω της ελεγχόμενα ομαλής μετάβασής τους από τη ζώνη διέλευσης στη ζώνη αποκοπής υλοποιούν το απαιτούμενο φιλτράρισμα χωρίς τα προβλήματα που θα δημιουργούσε η απότομη μετάβαση (φαινόμενο δακτυλίων, πλήρης απώλεια πληροφορίας από ορισμένες περιοχές συχνοτήτων κλπ). Δοθέντος ενός γραμμικού φίλτρου στο πεδίο των *u, v,* η διαδικασία υλοποίησής του είναι πολύ απλή και φαίνεται στην Εικόνα 32. Πρώτα εφαρμόζουμε τον FFT στην αρχική εικόνα f(x,y) και λαμβάνουμε την F(u,v) (διαστάσεων επίσης N x N). Στη συνέχεια

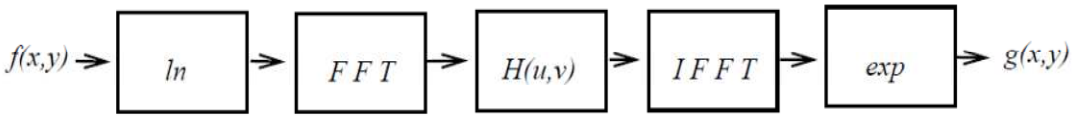
πολλαπλασιάζουμε σημείο-προς-σημείο την F(u,v) με την απόκριση συχνότητας H(u,v) του φίλτρου και, τέλος, στο αποτέλεσμα εφαρμόζουμε τον αντίστροφο FFT (IFFT).



Εικόνα 32: Διαδικασία υλοποίησης γραμμικού φίλτρου

5.2.2.2 Ομοιομορφικά Φίλτρα

Σύμφωνα με ένα γενικά παραδεκτό μοντέλο, η εικόνα μπορεί να γραφεί ως f(x,y)=i(x,y)r(x,y), δηλαδή ως γινόμενο δύο δισδιάστατων συναρτήσεων εκ των οποίων η i(x,y) είναι η συνάρτηση φωτεινής έντασης και η r(x,y) είναι η συνάρτηση αντίθεσης. Στη συντριπτική πλειονότητα των περιπτώσεων η i(x,y) είναι μία αργά μεταβαλλόμενη (στο χώρο) συνάρτηση, ενώ η r(x,y) είναι γρήγορα μεταβαλλόμενη. Εάν μπορούσε κανείς να επιδράσει ξεχωριστά πάνω στην κάθε μία συνάρτηση με κάποιο φίλτρο, τότε θα μπορούσε να επιτύχει ταυτόχρονα τη μείωση της δυναμικής περιοχής τιμών φωτεινής έντασης και την αύξηση της αντίθεσης. Αυτή ακριβώς την ιδέα υλοποιούν τα ομοιομορφικά φίλτρα. Η διαδικασία περιγράφεται σχηματικά στην Εικόνα 33. Όπως βλέπουμε, το κεντρικό μέρος της διαδικασίας είναι ίδιο με αυτό του προηγουμένου σχήματος. Η βασική διαφορά έγκειται στην εφαρμογή της συνάρτησης του λογαρίθμου στο πρώτο στάδιο (για τη μετατροπή του γινομένου των συναρτήσεων i(x,y) και r(x,y) σε άθροισμα). Στο τελευταίο στάδιο έχουμε εφαρμογή της αντίστροφης συνάρτησης exp(+).



Εικόνα 33: Διαδικασία υλοποίησης ομοιομορφικού φίλτρου

5.3 Εξισορρόπηση ιστογράμματος

Το ιστόγραμμα μιας εικόνας αποχρώσεων του γκρι περιέχει σημαντικές πληροφορίες για την εικόνα και για τον λόγο αυτό είναι ένα από τα σημαντικότερα εργαλεία στην επεξεργασία ψηφιακών εικόνων. Μπορεί να χρησιμοποιηθεί για την βελτιστοποίηση της εικόνας, την τροποποίηση των χαρακτηριστικών της, την μετατροπή της σε εικόνα με λιγότερες αποχρώσεις, την εξαγωγή χαρακτηριστικών της εικόνας κ.α.

Η βελτιστοποίηση μιας εικόνας που προκύπτει από την τροποποίηση του ιστογράμματος της είναι επιθυμητή σε πολλές εφαρμογές. Μια υποβιβασμένη εικόνα μπορεί να βελτιωθεί μειώνοντας τον υποβιβασμό της. Παραδείγματα υποβιβασμού είναι το θόλωμα, ο τυχαίος θόρυβος βάθους, ο θόρυβος στίγματος και ο θόρυβος κβάντωσης (quantization noise).

Εκφράζει την κατανομή των αποχρώσεων του γκρι στην εικόνα και στις περισσότερες περιπτώσεις καθαρίζει απόλυτα την εικόνα. Ένα ιστόγραμμα είναι ένα γράφημα που στον οριζόντιο άξονα έχει τις φωτεινότητες από 0-255 και στον κατακόρυφο άξονα το πλήθος των εικονοστοιχείων που έχουν κάθε φωτεινότητα. Οι τεχνικές τροποποίησης ιστογράμματος μετασχηματίζουν την αρχική ζώνη φωτεινότητας με την βοήθεια μιας γραμμικής ή μη γραμμικής συνάρτησης μετασχηματισμού T(.).

Η τεχνική εξισορρόπησης ιστογράμματος (histogram equalization) μετασχηματίζει τις γκρι φωτεινότητες μιας εικόνας έτσι ώστε αυτές να κατανέμονται ομοιόμορφα σε όλη την κλίμακα φωτεινοτήτων. Η εικόνα που προκύπτει με τον τρόπο αυτό είναι αυξημένης αντίθεσης σε σχέση με την αρχική.

Για την ανάπτυξη της μεθόδου ας υποθέσουμε ότι έχουμε μια γκρι εικόνα A(k,m), διαστάσεων N x M έτσι ώστε A(k,m) □ {0,….,L- 1}. Έστω, h(g), g=0,….,L- 1, το ιστόγραμμα της εικόνας I. Υπολογίζουμε την συνάρτηση αθροιστικής πιθανότητας από τη σχέση

$$P(g) = \frac{1}{N \times M} \sum_{i=0}^{g} h(i), \;\; g = 0,\ldots,L-1$$

Η συνάρτηση T(g)=int[L· P(g)] είναι συνάρτηση μετασχηματισμού των φωτεινοτήτων. Σύμφωνα με τη σχέση αυτή, κάθε φωτεινότητα A(k,m) της αρχικής εικόνας A μετασχηματίζεται στη φωτεινότητα B(k.m) της νέας εικόνας με την βοήθεια της σχέσης
B(k, m)=T(A(k, m)), k=0,…,N – 1 και m=0,…,M – 1. Με την διαδικασία αυτή οι φωτεινότητες της αρχικής εικόνας κατανέμονται ομοιόμορφα στην περιοχή [0,L - 1] αυξάνοντας έτσι την απόσταση μεταξύ τους και συνεπώς την αντίθεση της εικόνας

Η διαδικασία εξισορρόπησης ιστογράμματος που περιγράψαμε αναφέρεται ως “ολική εξισορρόπηση ιστογράμματος” (global histogram equalization) σε αντίθεση με τεχνικές τοπικής εξισορρόπησης ιστογράμματος(local histogram equalization) όπου η εξισορρόπηση ιστογράμματος εφαρμόζεται τοπικά σε περιοχές που καθορίζονται από το κινούμενο παράθυρο.

5.4 Περιστροφή και Κλιμάκωση

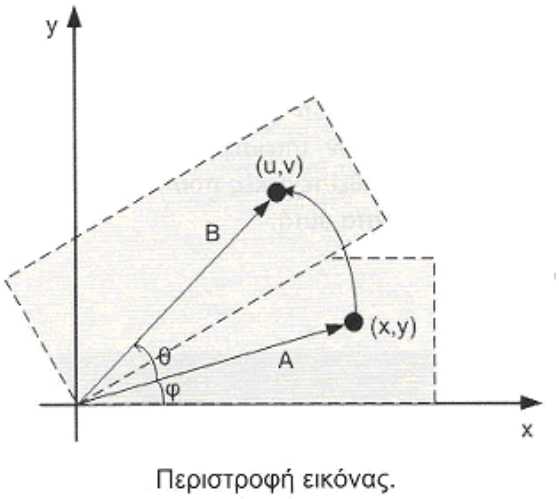
Η ανίχνευση και η εξαγωγή του υδατογραφήματος που είναι βασισμένο σε συσχέτιση (Correlation-Based) αποτυγχάνουν όταν εκτελείται η περιστροφή ή το Scaling στην υδατογραφημένη εικόνα επειδή το ενσωματωμένο υδατογράφημα και η τοπικά παραγμένη έκδοση του δεν μοιράζονται πλέον το ίδιο χωρικό πρότυπο (spatial pattern).

5.4.1 Περιστροφή (Rotation)

Σε πολλές εφαρμογές είναι αναγκαία η περιστροφή των εικόνων. Το βασικό πρόβλημα της περιστροφής αποτυπώνεται στο παρακάτω σχήμα, όπου το εικονοστοιχείο A=(x,y) περιστρέφεται κατά γωνία θ και πηγαίνει στη θέση B=(u,v). Τα διανύσματα έχουν το ίδιο μέτρο και το διάνυσμα A έχει γωνία φ ως προς τον άξονα x.

Ισχύουν οι σχέσεις:

- $u=|B|\cos(\vartheta + \varphi)=|B|(\cos\vartheta\cos\varphi-\sin\vartheta\sin\varphi)$
- $v=|B|\sin(\vartheta + \varphi)=|B|(\sin\vartheta\cos\varphi+\cos\vartheta\sin\varphi)$



Αν κάνουμε τις αντικαταστάσεις

$$\cos\phi = \frac{x}{|A|} = \frac{x}{|B|} \quad \text{και} \quad \sin\phi = \frac{y}{|A|} = \frac{y}{|B|}$$

Εικόνα 34: Περιστροφή εικόνας

Θα έχουμε:

u= (cos θ)x – (sin θ)y

v=(sin θ)x +(cos θ)y

$$\begin{pmatrix} u \\ v \end{pmatrix} = P \begin{pmatrix} x \\ y \end{pmatrix} \qquad P = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

ή όπου το καλείται τελεστής περιστροφής. Το P είναι ένας ορθογωνικός πίνακας διότι PT P=I. Αυτό σημαίνει ότι

$$\begin{pmatrix} x \\ y \end{pmatrix} = P^T \begin{pmatrix} u \\ v \end{pmatrix}$$

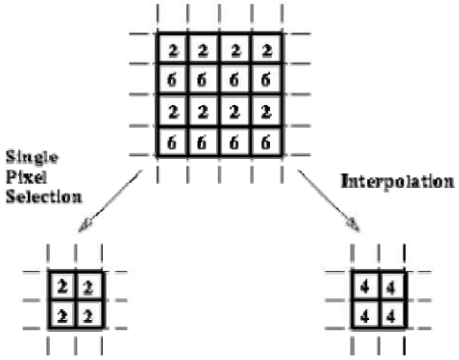
Συνεπώς το PT είναι και αυτός ένας τελεστής περιστροφής που επιτελεί την αντίστροφη μ' αυτή του P, δηλαδή περιστρέφει την εικόνα κατά γωνία – θ.

5.4.2 Κλιμάκωση (Scaling)

Η διαδικασία της κλιμάκωσης εκτελεί έναν γεωμετρικό μετασχηματισμό που μπορεί να χρησιμοποιηθεί για την σμίκρυνση ή τη μεγέθυνση του μεγέθους μιας εικόνας (ή μέρος μιας εικόνας). Η μείωση εικόνας, γνωστή συνήθως ως subsampling, εκτελείται από την αντικατάσταση (μιας ομάδας τιμών εικονοστοιχείου από μια αυθαίρετα επιλεγμένη τιμή εικονοστοιχείου μέσα από αυτήν την ομάδα) ή με την παρεμβολή μεταξύ των τιμών εικονοστοιχείων των τοπικών γειτονιών. Η μεγέθυνση της εικόνας επιτυγχάνεται από την επανάληψη εικονοστοιχείων ή από την παρεμβολή τους. Χρησιμοποιούμε τη κλιμάκωση για να αλλάξουμε την εμφάνιση μιας εικόνας και για να αλλάξουμε την ποσότητα πληροφοριών που περιέχεται σε μια εικόνα.

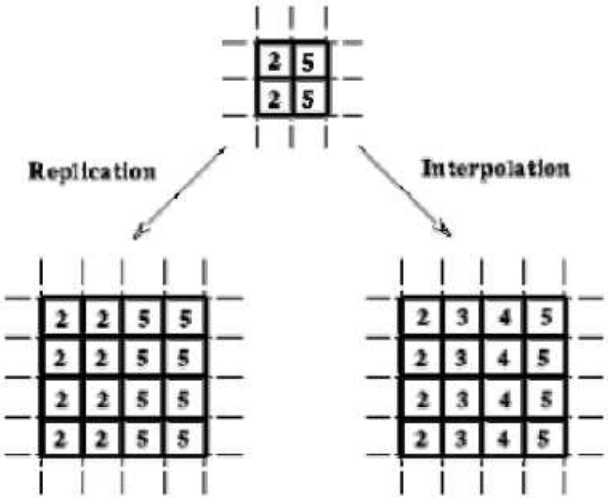
Η κλιμάκωση μπορεί να συμπιέσει ή να επεκτείνει μια εικόνα κατά μήκος των συντεταγμένων κατευθύνσεων. Διαφορετικές τεχνικές μπορούν να χρησιμοποιηθούν στην υποδειγματοληψία και το ζουμ.

Το παρακάτω σχήμα επεξηγεί τις δύο μεθόδους υπο-δειγματοληψίας. Στον πρώτο, επιλέγουμε(ίσως τυχαία) μια τιμή εικονοστοιχείου μέσα σε μια τοπική γειτονιά για να είναι αντιπροσωπεύει τα περίχωρα της. (Αυτή η μέθοδος είναι υπολογιστικά απλή, αλλά μπορεί να οδηγήσει σε πάρα πολύ φτωχά αποτελέσματα εάν οι διαφορές στις γειτονικές τιμές δειγματοληψίας είναι επίσης μεγάλες.) Η δεύτερη μέθοδος παρεμβάλλει μεταξύ των τιμών εικονοστοιχείου μέσα σε μια γειτονιά από τη λήψη ενός στατιστικού δείγματος (όπως ο μέσος) των τοπικών τιμών έντασης.



Εικόνα 35: α) Αντικατάσταση με το ανώτερο αριστερό εικονοστοιχείο, β) Παρεμβολή (interpolation) που χρησιμοποιεί τη μέση τιμή

Μια εικόνα (ή περιοχές μιας εικόνας) μπορεί να μεγεθυνθεί είτε μέσω της επανάληψης είτε της παρεμβολής εικονοστοιχείων. Το παρακάτω σχήμα εμφανίζει πώς η επανάληψη εικονοστοιχείων αντικαθιστά κάθε αρχικό εικονοστοιχείο εικόνας από μια ομάδα εικονοστοιχείων με την ίδια τιμή (όπου το μέγεθος ομάδας καθορίζεται από τον παράγοντα κλιμάκωσης). Εναλλακτικά, η παρεμβολή των τιμών των γειτονικών εικονοστοιχείων στην αρχική εικόνα μπορεί να εκτελεσθεί προκειμένου να αντικαταστήσει κάθε εικονοστοιχείο με μια επεκταμένη ομάδα εικονοστοιχείων.



Εικόνα 36: α) Επανάληψη μιας ενιαίας τιμής εικονοστοιχείου**.** β) Παρεμβολή (interpolation)

5.5 Κοπή (Cropping)

Αυτό είναι μια πολύ κοινή επίθεση δεδομένου ότι σε πολλές περιπτώσεις τον επιτιθέμενο τον ενδιαφέρει ένα μικρό τμήμα του υδατογραφημένου αντικειμένου, όπως τα μέρη μιας ορισμένης εικόνας ή των πλαισίων (frames) ενός βίντεο. Έτσι προκειμένου να επιζήσει το υδατογράφημα χρειάζεται να διαδοθεί σε όλες τις διαστάσεις όπου αυτή η επίθεση μπορεί να πραγματοποιηθεί

Στο matlab μπορούμε να περικόψουμε την εικόνα με την βοήθεια της συνάρτησης *J=imcrop(I,[x y w h])* όπου το x εκφράζει τον άξονα x, το y εκφράζει τον άξονα y, το w εκφράζει το πλάτος και το h το ύψος, δηλαδή τις διαστάσεις της εικόνας I που θέλουμε.

5.6 Συμπίεση (Compression)

Ο όρος συμπίεση ψηφιακής εικόνας αναφέρεται σε ένα σύνολο τεχνικών και αλγορίθμων που έχουν σαν βασικό σκοπό την εξοικονόμηση της απαιτούμενης μνήμης για την αναπαράσταση και αποθήκευση ψηφιακών εικόνων. Η αποθήκευση μιας ψηφιοποιημένης εικόνας η οποία προέρχεται από μία απλή δειγματοληψία αναλογικού σήματος οδηγεί σε κατασπατάληση της μνήμης. Έτσι, σε τομείς όπου έχουμε μετάδοση και αποθήκευση μεγάλου πλήθους εικόνων, το μεγάλο μέγεθος της μνήμης που απαιτείται δημιουργεί σοβαρά προβλήματα. Για αυτόν το λόγο αναζητήθηκαν γρήγοροι αλγόριθμοι συμπίεσης και αποσυμπίεσης εικόνας .

Οι τεχνικές συμπίεσης ψηφιακής εικόνας μπορούν να χωριστούν σε δυο μεγάλες κατηγορίες: σε αυτές όπου έχουμε απώλεια πληροφορίας (lossy compression) και σε αυτές όπου δεν έχουμε (lossless compression). Οι τεχνικές στις οποίες δεν έχουμε απώλεια πληροφορίας

χρησιμοποιούνται στις περιπτώσεις όπου η αρχική εικόνα είναι δύσκολο να αποκτηθεί ή περιέχει πληροφορία ζωτικής σημασίας. Από την άλλη μεριά, οι τεχνικές συμπίεσης με απώλειες χρησιμοποιούνται όταν η αρχική εικόνα μπορεί να ανακατασκευαστεί εύκολα ή όταν είναι ανεκτή, ανάλογα με την εφαρμογή, με απώλεια ενός μέρους της πληροφορίας του δέκτη.

Όλες οι τεχνικές συμπίεσης βασίζονται στην απόρριψη της πλεονάζουσας πληροφορίας που υπάρχει στις περισσότερες ψηφιακές εικόνες. Η πλεονάζουσα πληροφορία προέρχεται από τα στατιστικά χαρακτηριστικά της εικόνας (π.χ μεγάλη χωρική συσχέτιση) και μπορεί να περιγράφει διάφορους τρόπους. Για αυτό τον λόγο εμφανίστηκαν και διάφορες τεχνικές συμπίεσης. Η ύπαρξη πλεονάζουσας πληροφορίας σχετίζεται άμεσα με την κατανομή πιθανότητας που ακολουθεί η εικόνα και, επομένως, μπορεί να αντιμετωπιστεί με τεχνικές της Θεωρίας Πληροφοριών που κάνουν χρήση της έννοιας της εντροπίας της εικόνας. Η απόρριψη της πλεονάζουσας πληροφορίας με αυτό τον τρόπο οδηγεί σε τεχνικές συμπίεσης χωρίς απώλειες, όπως η κωδικοποίηση Huffman και η κωδικοποίηση μήκους διαδρομών (Run-Length Coding). Τέλος, συμπίεση μπορεί να επιτευχθεί μέσω μετασχηματισμών της εικόνας. Αυτό επιτυγχάνεται λόγω της ιδιότητας ορισμένων ορθογώνιων μετασχηματισμών (π.χ Διακριτός Μετασχηματισμός Συνημίτονου, Διακριτός Μετασχηματισμός Ημίτονου) να συγκεντρώνουν την ενέργεια του σήματος σε ένα σχετικά μικρό πλήθος συντελεστών του μετασχηματισμού.

Έτσι, κωδικοποιώντας τους συντελεστές του μετασχηματισμού με διάφορες τεχνικές μπορούμε να πετύχουμε αρκετά μεγάλη συμπίεση. Η χρήση των μετασχηματισμών είναι μια από τις

καλύτερες τεχνικές συμπίεσης ψηφιακής εικόνας και εφαρμόζεται κυρίως στις περιπτώσεις όπου είναι ανεκτή μια μικρή απώλεια πληροφορίας.

5.6.1 Κωδικοποίηση Εντροπίας

Η κωδικοποίηση εντροπίας αναφέρεται σε τεχνικές, οι οποίες δεν λαμβάνουν υπ' όψη τους το είδος της πληροφορίας που πρόκειται να συμπιεστεί. Με άλλα λόγια, αυτές οι τεχνικές αντιμετωπίζουν την πληροφορία ως μια απλή ακολουθία bits. Γι΄ αυτό το λόγο, η κωδικοποίηση εντροπίας μπορεί να εφαρμοσθεί ανεξάρτητα από το είδος της πληροφορίας. Επιπλέον, οι τεχνικές κωδικοποίησης εντροπίας προσφέρουν κωδικοποίηση χωρίς απώλειες.

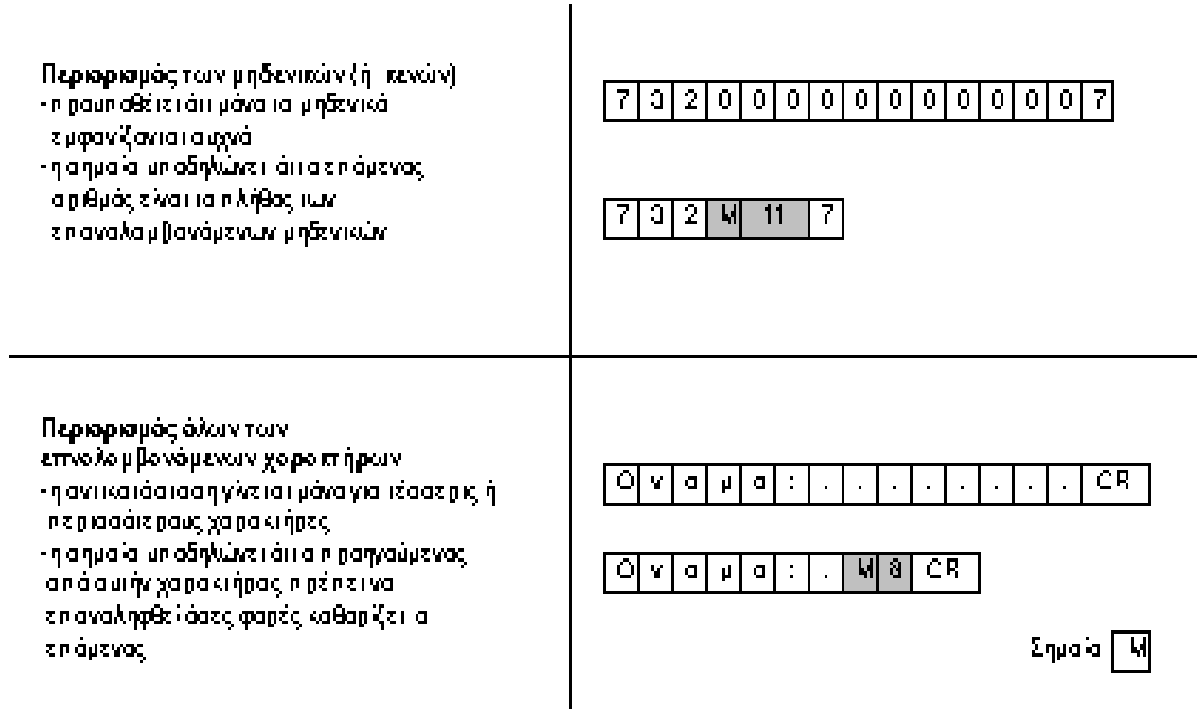
Ας δούμε ένα παράδειγμα. Μπορούμε να αντικαθιστούμε κάθε ακολουθία 10 διαδοχικών μηδενικών που βρίσκουμε με ένα ειδικό χαρακτήρα ακολουθούμενο από τον αριθμό 10. Με αυτόν τον τρόπο, μειώνουμε το μήκος της ακολουθίας χωρίς να κάνουμε καμία υπόθεση για την σημασία των μηδενικών, αλλά και χωρίς να αλλοιώνεται το σήμα.

Οι τεχνικές κωδικοποίησης εντροπίας διαχωρίζονται σε δύο βασικές κατηγορίες:

- Περιορισμός των επαναλαμβανόμενων ακολουθιών (Suppression of repetitive sequences)
- Στατιστική Κωδικοποίηση (Statistical encoding)

5.6.1.1 Περιορισμός των επαναλαμβανόμενων ακολουθιών

Αυτή η μέθοδος κωδικοποίησης εντροπίας είναι από τις παλαιότερες και πιο απλές που χρησιμοποιούνται. Η ιδέα είναι ότι σε μια τυχαία ακολουθία από bits είναι να πιθανό να εμφανιστούν κάποια τμήματα που αποτελούνται από κάποιο επαναλαμβανόμενο χαρακτήρα (υποθέτουμε ότι η ακολουθία από bits που αποτελεί την πληροφορία ομαδοποιείται σε χαρακτήρες ή οκτάδες από bits και οι χαρακτήρες αποτελούν το ελάχιστο ποσό πληροφορίας). Αυτά τα τμήματα μπορούν να αντικατασταθούν από το χαρακτήρα, ένα ειδικό χαρακτήρα, που ονομάζεται σημαία, και το πλήθος των επαναλήψεων του χαρακτήρα σε αυτά. Η κωδικοποίηση αυτή έχει την παρακάτω σημασία: Κάθε φορά που συναντάται η σημαία, ο χαρακτήρας που προηγείται αυτής πρέπει να επαναληφθεί όσες φορές υποδεικνύει ο αριθμός που ακολουθεί τη σημαία.



Αυτή η μορφή που περιγράψαμε μπορεί να γίνει πιο αποδοτική, αν έχουμε συχνά εμφανιζόμενες ακολουθίες μηδενικών. Σ' αυτές τις περιπτώσεις απαιτείται απλώς μια σημαία (που θα σημαίνει "επαναλαμβανόμενα μηδενικά") και ο αριθμός των επαναλήψεων. Και στις δύο περιπτώσεις, το μήκος των ακολουθιών πρέπει να είναι τέτοιο, ώστε να υπάρχει ουσιαστικό όφελος από αυτήν την αντικατάσταση.

5.6.1.2 Στατιστική Κωδικοποίηση

Η στατιστική κωδικοποίηση προσπαθεί να εντοπίσει τις περισσότερο συχνά εμφανιζόμενες σειρές χαρακτήρων μέσα στο "κείμενο" των συμβόλων και να τις αντιστοιχίσει σε κωδικούς με τα λιγότερα bits. Έτσι προκύπτει ένα "λεξικό" κωδικών όπου οι πιο συχνές ακολουθίες συμβόλων έχουν μικρότερους κωδικούς, ενώ οι πιο σπάνιες μεγαλύτερους. Κατά την αποσυμπίεση της πληροφορίας ο αποκωδικοποιητής χρησιμοποιεί το "λεξικό" ώστε να μετατρέψει και πάλι τους κωδικούς σε ακολουθίες συμβόλων.

Η στατιστική κωδικοποίηση παίρνει δύο μορφές: αντικατάσταση προτύπων (pattern substitution) και κωδικοποίηση Huffman (Huffman encoding).

5.6.1.2.1 Αντικατάσταση Προτύπων

Η μέθοδος της αντικατάστασης προτύπων χρησιμοποιείται αποκλειστικά για κείμενα. Συχνά εμφανιζόμενα πρότυπα (ακολουθίες χαρακτήρων, λέξεις) αντικαθιστώνται με λίγους χαρακτήρες. Για παράδειγμα, θα μπορούσαμε να κωδικοποιήσουμε αυτές τις σημειώσεις αντικαθιστώντας τη λέξη "πολυμέσα" με τους χαρακτήρες "*π". Σε μια τέτοια περίπτωση, το λεξικό προκύπτει από ανάλυση του κειμένου, ενώ κάποιες λέξεις είναι εκ των προτέρων γνωστό ότι θα εμφανιστούν σίγουρα.

5.6.1.2.2 Κωδικοποίηση Huffman

Η κωδικοποίηση Huffman (Huffman encoding) χρησιμοποιείται και στη συμπίεση ακίνητης και κινούμενης εικόνας. Συνήθως για κάθε εικόνα δημιουργείται ένα νέο λεξικό κωδικών ενώ στην περίπτωση της κινούμενης εικόνας το λεξικό μπορεί να δημιουργείται και για κάθε πλαίσιο ή σειρά πλαισίου(frames). Το λεξικό πρέπει βέβαια να αποθηκεύεται ώστε να είναι δυνατή αργότερα η αποσυμπίεση.

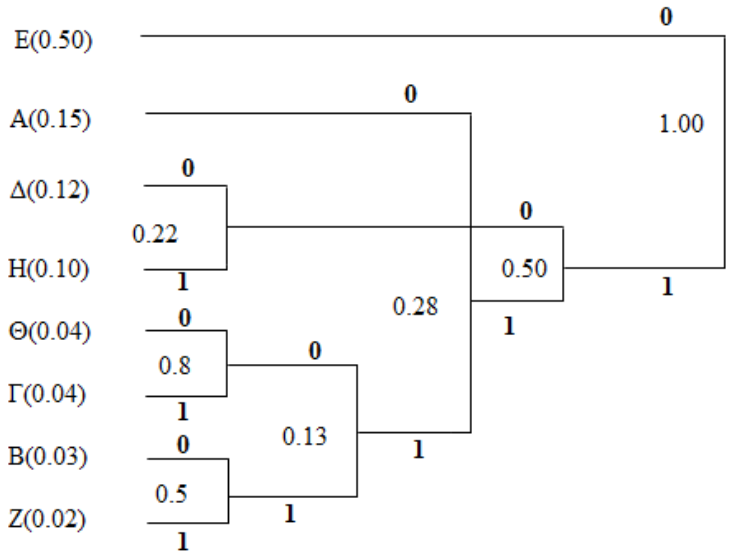
Στην πράξη ο κώδικας Huffman δημιουργείται συνδυάζοντας κάθε φορά τα δύο λιγότερα πιθανά σύμβολα της πηγής και προσθέτοντας τις πιθανότητες εμφάνισης τους μέχρι να συμπεριληφθούν όλα.

Για την καλύτερη κατανόηση της μεθόδου ακολουθεί ένα παράδειγμα: Υποθέτουμε πως η πηγή εκπέμπει ένα αλφάβητο 8 συμβόλων, N={Α, Β, Γ, Δ, Ε, Ζ, Η, Θ}. Έστω ότι τα σύμβολα εκπέμπονται με τις πιθανότητες που εμφανίζονται στον πίνακα 2.

Σύμβολο	Πιθανότητα
Ε	0.50
Α	0.15
Δ	0.12
Η	0.10
Θ	0.04
Γ	0.04
Β	0.03
Ζ	0.02

Πίνακας 3: Πίνακας Huffman

Για να δημιουργήσουμε των κώδικα Huffman συνδυάζουμε κάθε φορά τα δύο λιγότερο πιθανά σύμβολα και προσθέτουμε τις πιθανότητες εμφάνισης τους, δημιουργώντας το γράφημα της επόμενης εικόνας.



Εικόνα 37: Η διαδικασία δημιουργίας του κώδικα Huffman

Τα βήματα κατασκευής του κώδικα Huffman είναι:

1. Ταξινομούμε τα σύμβολα κατά φθίνουσα τάξη πιθανότητας εμφάνισης.
2. Ενώνουμε τα δύο σύμβολα με τις χαμηλότερες πιθανότητες και δημιουργούμε ένα νέο κλάδο με πιθανότητα το άθροισμα των δύο συμβόλων.
3. Επαναλαμβάνουμε το βήμα 2 μέχρις ότου ενώσουμε όλα τα σύμβολα σε ένα κλάδο με πιθανότητα εμφάνισης τη μονάδα.
4. Περνάμε από όλους τους κλάδους που περιέχει το γράφημα μας και εκχωρούμε σε κάθε κατώτερο κλάδο το σύμβολο "1" και σε κάθε ανώτερο το "0".

Ο κωδικός του κάθε συμβόλου στο "λεξικό" του κώδικα Huffman προκύπτει δημιουργώντας την ακολουθία των "0"και "1" που το προσδιορίζει.

Έτσι οι κωδικοί που προκύπτουν για τα 8 σύμβολα είναι:

Σύμβολο	Πιθανότητα εμφάνισης p	Δυαδικός κωδικός Huffman	Πλήθος ψηφίων στον κωδικό, N	N*p
Ε	0.50	0	1	0.50
Α	0.15	110	3	0.45
Δ	0.12	100	3	0.36
Η	0.10	101	3	0.30
Θ	0.04	11100	5	0.20
Γ	0.04	11101	5	0.20
Β	0.03	11110	5	0.15
Ζ	0.02	11111	5	0.10
				2.26

Πίνακας 4: Κωδικοί που προκύπτουν

Στην τελευταία στήλη το γινόμενο N*p δίνει την πιθανότητα εμφάνισης των δυαδικών ψηφίων που κωδικοποιούν το συγκεκριμένο σύμβολο σε ένα μεγάλο μήνυμα της πηγής. Προσθέτοντας για όλα τα σύμβολα παίρνουμε το μέσο πλήθος bits/σύμβολο που χρειάζονται τώρα για να μεταδοθεί το μήνυμα. Στο συγκεκριμένο παράδειγμα η τιμή αυτή είναι 2.26, δηλαδή σημαντικά μικρότερη από τα 3 bits/σύμβολο που θα έπρεπε να χρησιμοποιήσουμε χωρίς κωδικοποίηση.

Το αποτέλεσμα είναι ότι τελικά χρειάζονται στατιστικά λιγότερα bits/σύμβολο για τη μετάδοση του μηνύματος. Παρατηρούμε ακόμα ότι η κωδικοποίηση Huffman δημιουργεί τέτοιους κωδικούς ώστε να είναι σαφής η αποκωδικοποίηση κάθε αλληλουχίας δυαδικών συμβόλων. Άρα η αλληλουχία "01110011110100" στο παράδειγμα μας αποκωδικοποιείται με μοναδικό τρόπο ως "ΕΘΒΔ".

5.6.2 Κωδικοποίηση Πηγής

Στην κωδικοποίηση πηγής προσδιορίζονται τα χαρακτηριστικά εκείνα της πηγής του σήματος που μπορούν να οδηγήσουν στην αφαίρεση τμημάτων της πληροφορίας χωρίς όμως μείωση της συνολικής ποιότητας του σήματος.

Για παράδειγμα, κατά την κωδικοποίηση στοιχείων πολυμέσων (ήχος, εικόνα, βίντεο) όπου τα σήματα αντιπροσωπεύουν ανθρώπινα αισθητηριακά δεδομένα λαμβάνεται υπόψη πως υπάρχουν συχνότητες των ακουστικών και οπτικών σημάτων που δεν γίνονται αντιληπτές από τον άνθρωπο

και μπορούν να εξαλειφθούν από την αρχική πληροφορία με προφανές αποτέλεσμα ένα σημαντικό βαθμό συμπίεσης.

Γενικά, αυτές οι τεχνικές μπορούν να παράγουν μεγαλύτερα ποσοστά συμπίεσης σε σχέση με την κωδικοποίηση εντροπίας. Μειονεκτούν όμως στη σταθερότητα, γιατί το ποσοστό συμπίεσης που επιτυγχάνουν διαφοροποιείται ανάλογα με το αντικείμενο που συμπιέζεται. Πάντως, η κωδικοποίηση πηγής μπορεί να λειτουργήσει και με απώλειες και χωρίς απώλειες.

Οι τεχνικές κωδικοποίησης πηγής διακρίνονται σε τρεις τύπους:

- Κωδικοποίηση Μετασχηματισμού (transform encoding)
- Διαφορική ή προβλεπτική κωδικοποίηση (differential or predictive encoding) η οποία αφορά ήχο
- Διανυσματική κβαντοποίηση (vector quantization) η οποία αφορά

Να σημειωθεί ότι οι δυο παραπάνω κατηγορίες κωδικοποίησης δεν αποκλείουν η μια την άλλη. Υπάρχουν αλγόριθμοι που συνδυάζουν τεχνικές και των δυο κατηγοριών για να επιτύχουν καλύτερα αποτελέσματα. Παρακάτω θα αναπτύξουμε την κωδικοποίηση μετασχηματισμού.

5.6.2.1 Κωδικοποίηση Μετασχηματισμού

Στην κωδικοποίηση μετασχηματισμού (Transform encoding) όπου το αρχικό σχήμα υφίσταται ένα κατάλληλο μετασχηματισμό ώστε να είναι ευκολότερη η επεξεργασία του με απώτερο στόχο βέβαια τον εντοπισμό των τμημάτων εκείνων που μπορούν να αφαιρεθούν.

Η ψηφιακή καταγραφή ηχητικών και οπτικών πληροφοριών περιλαμβάνει πληροφορίες που είτε δεν γίνονται αντιληπτές από τα ανθρώπινα αισθητήρια όργανα λόγω των περιορισμών τους είτε έχουν τόσο μικρή συμμετοχή στη συνολική αντίληψη ώστε η απώλεια τους δεν θα αλλοίωνε σημαντικά την ποιότητα της πληροφορίας.

Στη κωδικοποίηση μετασχηματισμού, το σήμα υφίσταται ένα μαθηματικό μετασχηματισμό από το αρχικό πεδίο του χρόνου ή του χώρου σε ένα αφηρημένο πεδίο το οποίο είναι πιο κατάλληλο για συμπίεση. Αυτή η διαδικασία είναι αντιστρεπτή, δηλαδή υπάρχει ο αντίστροφος μετασχηματισμός που θα επαναφέρει το σήμα στην αρχική του μορφή.

Ένας τέτοιος μετασχηματισμός είναι ο μετασχηματισμός Fourier, ο οποίος μετασχηματίζει μια συνάρτηση f(t) από το πεδίο του χρόνου σε μια συνάρτηση g(λ) στο πεδίο ων συχνοτήτων και προσδιορίζουν το πλάτος g καθεμίας συχνότητας λ στις οποίες αναλύεται η αρχική f(t). Στην περίπτωση των εικόνων χρησιμοποιείται μια ειδική μορφή του μετασχηματισμού Fourier, ο διακριτός μετασχηματισμός Fourier (DFT), και το σημαντικό σημείο που εκμεταλλευόμαστε είναι το εξής: στη φασματική (στο πεδίο των συχνοτήτων) αναπαράσταση των εικόνων, οι συχνότητες περιγράφουν πόσο γρήγορα μεταβάλλονται τα χρώματα και η απόλυτη φωτεινότητα.

Ο DFT και ο Διακριτός Μετασχηματισμός Συνημίτονου (DCT) συναντώνται στα συστήματα υδατογράφησης και θα αναλυθούν εκτενέστερα στη συνέχεια .

5.6.2.1.1 Βασικοί Δισδιάστατοι Μετασχηματισμοί

Στην κωδικοποίηση μέσω μετασχηματισμών επιδιώκεται η συμπίεση της ενέργειας μιας εικόνας με σχετικά λίγους συντελεστές του μετασχηματισμού. Η ενέργεια των υπολοίπων συντελεστών είναι αμελητέα και έτσι αυτοί μπορούν να απορριφθούν. Οι υπόλοιποι μπορούν να κωδικοποιηθούν χρησιμοποιώντας κωδικές λέξεις μεταβλητού μήκους. Με αυτό τον τρόπο μπορεί να επιτευχθεί πολύ σημαντική συμπίεση. Η κωδικοποίηση με την σχέση:

$$\mathbf{F=Af}$$

όπου f το διάνυσμα που αναπαριστά μια εικόνα μεγέθους L=N x M και A ο πίνακας μετασχηματισμού. Ο αντίστροφος μετασχηματισμός με τον οποίο γίνεται η αποκωδικοποίηση, ορίζεται ως εξής:

$$\mathbf{f=A^{-1}F}$$

Ένας μετασχηματισμός ονομάζεται ορθομοναδιαίος εάν ικανοποιεί τη σχέση:

$$\mathbf{AA^{*T}=A^{T}A^{*}=I}$$

Επίσης ικανοποιεί τη συνθήκη διατήρησης της ενέργειας:

$$||f||^2 = \sum_{k=1}^{L} |f(k)|^2 = \sum_{k=1}^{L} |F(k)|^2 = ||F||^2$$

Στις περισσότερες περιπτώσεις, οι ενέργεια του σήματος κατά την εφαρμογή του μετασχηματισμού κατανέμεται ανομοιόμορφα στους συντελεστές του μετασχηματισμού. Η περισσότερη ενέργεια συγκεντρώνεται στο DC όρο και σε μερικούς όρους "χαμηλής συχνότητας" F(k), 1 ≤ k ≤ K << L. Έτσι πολλοί συντελεστές του μετασχηματισμού μπορούν να απορριφθούν χωρίς σημαντική απώλεια πληροφορίας.

5.6.2.1.2 Δισδιάστατος Διακριτός Μετασχηματισμός Fourier (2D-DFT)

Στα δισδιάστατα σήματα,(εικόνες), υπάρχει ακριβώς η ίδια δυνατότητα μετασχηματισμού Fourier. Το διακριτό μετασχηματισμό Fourier (DFT) τον υλοποιούμε γρήγορα με τον αλγόριθμο που καλείται FFT. Φυσικά, αφού η εικόνα αποτελεί σήμα που περιγράφει τον τρόπο μεταβολής της αμαύρωσης (ή του χρώματος) στο χώρο και όχι στο χρόνο, ο διακριτός μετασχηματισμός Fourier θα μας μεταφέρει στην περιοχή των χωρικών συχνοτήτων. Ο δισδιάστατος μετασχηματισμός Fourier p(k1,k2), μιας εικόνας q(n1,n2) μεγέθους N×N εικονοστοιχείων, ορίζεται ως:

$$p(k_1,k_2) = \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} q(n_1,n_2)\ W_N^{k_1 n_1}\ W_N^{k_2 n_2} \qquad 0 \le k_1,k_2 \le N-1$$

ενώ ο αντίστροφος μετασχηματισμός είναι ο εξής:

$$q(n_1,n_2) = \frac{1}{N^2} \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{N-1} p(k_1,k_2)\ W_N^{-k_1 n_1}\ W_N^{-k_2 n_2} \qquad 0 \le n_1,n_2 \le N-1$$

Η διαχωρισιμότητα της πρώτης σχέσης απορρέει από το γεγονός ότι μπορεί να γραφεί και ως:

$$p(k_1,k_2) = \sum_{n_1=0}^{N-1} W_N^{k_1 n_1} \sum_{n_2=0}^{N-1} q(n_1,n_2)\ W_N^{k_2 n_2} \qquad 0 \le k_1,k_2 \le N-1$$

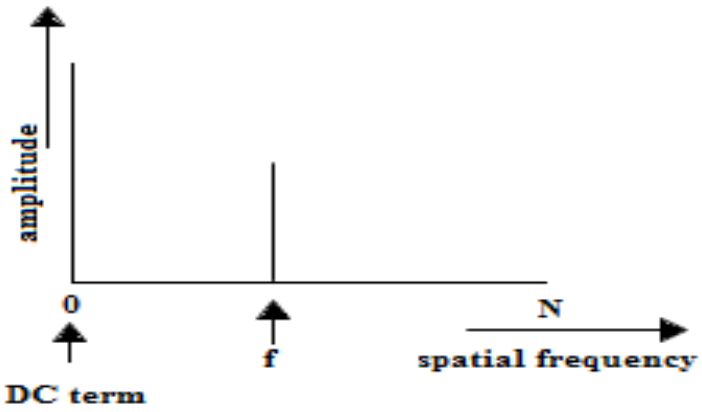
που σημαίνει ότι μπορούμε να υπολογίσουμε πρώτα το εσωτερικό άθροισμα της σχέσης. Η πράξη αυτή ισοδυναμεί με το να υπολογίσουμε τον DFT κάθε μιας γραμμής της εικόνας και στο αποτέλεσμα που προκύπτει να υπολογίσουμε τον DFT της κάθε στήλης. Η χρησιμοποίηση του FFT θα μειώσει τις απαιτούμενες πράξεις για τον υπολογισμό του φάσματος σε πλήθος της τάξης του 2N2log2N. Δεδομένου ότι οι όροι p(k1,k2) του φάσματος είναι μιγαδικοί αριθμοί, για να μελετήσουμε το φάσμα μιας εικόνας, συνήθως μελετούμε το μέτρο των χωρικών συνιστωσών και τη φάση τους ξεχωριστά.

Η θεωρία Fourier δηλώνει ότι οποιοδήποτε σήμα, στις οπτικές εικόνες, μπορεί να εκφραστεί ως μια ημιτονοειδής σειρά. Μία εικόνα με ημιτονοειδές πρότυπο μπορεί να αναλυθεί σε έναν ενιαίο όρο Fourier που κωδικοποιεί τη χωρική συχνότητα, το πλάτος (θετικό ή αρνητικό) και τη φάση. Αυτές οι τρεις τιμές περιέχουν όλες τις πληροφορίες στην ημιτονοειδή εικόνα. Η χωρική συχνότητα θεωρητικά είναι ανεξάρτητη από το πλάτος της εικόνας.

Το μέγεθος του πλάτους (amplitude) αντιστοιχεί στην αντίθεσή (contrast), ή τη διαφορά μεταξύ των σκοτεινότερων και φωτεινότερων τόνων της εικόνας. Ένα αρνητικό μέγεθος

αντιπροσωπεύει μια αντίθεση-αντιστροφή, δηλ. τα bright γίνονται σκοτεινά, και αντίστροφα. Η φάση αντιπροσωπεύει πώς οι ημιτονοειδείς συνιστώσες του σήματος μετατοπίζονται σε σχέση με την αρχική τους θέση. Δηλαδή, πόσο η ημιτονοειδής συνιστώσα μετατοπίζεται αριστερά ή δεξιά. Ένας μετασχηματισμός Fourier κωδικοποιεί όχι μόνο μια ημιτονοειδή συνιστώσα (single sinusoid), αλλά ολόκληρη σειρά sinusoids μέσω ενός φάσματος χωρικών συχνοτήτων από το μηδέν μέχρι τη "συχνότητα Nyquist"(η υψηλότερη χωρική συχνότητα που μπορεί να κωδικοποιηθεί στην ψηφιακή εικόνα και η οποία συσχετίζεται με το μέγεθος των pixels).

Ο μετασχηματισμός κατά Fourier κωδικοποιεί όλες τις χωρικές συχνότητες που είναι παρούσες σε μια εικόνα ταυτόχρονα ως εξής: Ένα σήμα που περιέχει μόνο μια ενιαία χωρική συχνότητα f σχεδιάζεται ως μια γραμμή στο σημείο f κατά μήκος του χωρικού άξονα συχνότητας, ύψους που αντιστοιχεί στο εύρος (amplitude), του ημιτονοειδούς σήματος ή στην αντίθεση (contrast) των τιμών της εικόνας.



Εικόνα 38: Ο μετασχηματισμός κατά Fourier μιας ημιτονοειδούς εικόνας (μία γραμμή), η οποία είναι ένα μονοδιάστατο σήμα

Ο μετασχηματισμός Fourier έχει δύο σημαντικές λειτουργίες στην ψηφιακή επεξεργασία εικόνας. Η πρώτη είναι ότι ο δισδιάστατος μετασχηματισμός Fourier είναι η γέφυρα μεταξύ της χωρικής περιοχής και της περιοχής συχνότητας. Η δεύτερη είναι ότι ο δισδιάστατος μετασχηματισμός Fourier συνδέεται πολύ με το θεώρημα συνελίξεων και δειγματοληψίας. Το πρώτο είναι η βάση της επεξεργασίας εικόνας και το δεύτερο είναι η γέφυρα μεταξύ του συνεχούς (αληθινού) κόσμου και του διακριτού κόσμου.

Για την περίπτωση των ψηφιακών εικόνων αποχρώσεων του γκρι προκύπτουν οι ακόλουθες βασικές ιδιότητες :

- Περιοδικότητα
- Γραμμικότητα

- Χωρική μετατόπιση
- Διαμόρφωση
- Συμμετρία
- Περιστροφή
- Κλιμάκωση
- Αναστροφή
- Κυκλική συνέλιξη
- Γραμμική συνέλιξη

Στο Matlab ο υπολογισμός του 2D-DFT μιας εικόνας f γίνεται με την παρακάτω εντολή F=fft2(f, M_0 ,N_0) .

5.6.2.1.3 Δισδιάστατος Διακριτός Μετασχηματισμός Συνημιτόνου (2D-DCT)

Ο 2D-DCT παρότι εννοιολογικά είναι παρόμοιος με το 2D-DFT διαφέρουν σημαντικά κυρίως ως προς τα ακόλουθα:

- Ενώ ο DFT μας δίνει συντελεστές φάσματος γενικά μιγαδικούς αριθμούς ακόμα και για πραγματικά δεδομένα όπως οι εικόνες, ο DCT είναι ένας μετασχηματισμός πραγματικών αριθμών και δίνει πάντα πραγματικούς συντελεστές.
- Ο 2D-DCT είναι ένας ξεχωριστός μετασχηματισμός και δεν αποτελεί το πραγματικό μέρος του 2D-DFT.
- Ένα πολύ σημαντικό χαρακτηριστικό του 2D-DCT είναι ότι οι πρώτοι του συντελεστές στο φάσμα έχουν τη σημαντικότερη πληροφορία. Με αυτή την έννοια, ο DCT προσφέρει σημαντικά πλεονεκτήματα στην ενεργειακή συμπίεση(energy compaction) των εικόνων.
- Αν έχουμε ένα περιοδικό σήμα, το πλάτος των συντελεστών του 2D-DFT είναι αμετάβλητο στο χώρο(λόγω χωρικής μετατόπισης), δηλαδή η φάση του σήματος δεν επηρεάζει το πλάτος των συντελεστών. Αυτό δεν ισχύει για τον 2D-DCT.
- Οι λοιπές ιδιότητες του 2D-DCT είναι παρόμοιες με αυτές του 2D-DFT, με μια σημαντική εξαίρεση: δεν έχει αποδειχθεί ακόμα ότι είναι πιθανό να εφαρμοστεί συνέλιξη με τον DCT.

Ο 2D-DCT μιας εικόνας f(m, n) διαστάσεων MxN δίνεται από τη σχέση:

$$F(u,v) = \mathrm{a(u)a(v)} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \mathrm{f(m,n)} \cos\left[\frac{\pi}{\mathrm{M}}\left(\mathrm{m}+\frac{1}{2}\right)\mathrm{u}\right] \cos\left[\frac{\pi}{\mathrm{N}}\left(\mathrm{n}+\frac{1}{2}\right)\mathrm{v}\right]$$

με u=0,1,….,M-1 και v=0,1,….,N-1 και

$$a(u) = \begin{cases} \frac{1}{\sqrt{M}} & u = 0 \\ \sqrt{\frac{2}{M}} & 1 \le u \le M-1 \end{cases} \qquad a(v) = \begin{cases} \frac{1}{\sqrt{N}} & v = 0 \\ \sqrt{\frac{2}{N}} & 1 \le v \le N-1 \end{cases}$$

Στο Matlab ο υπολογισμός του 2D-DCT γίνεται με την εντολή: b=dct2(a, mrows, ncols). Οι μεταβλητές mrows και ncols καθορίζουν τα πόσα μηδενικά πρέπει να προστεθούν πριν τον μετασχηματισμό.

5.6.3 Συμπίεση κατά JPEG

Το JPEG αποτελεί ένα εξαιρετικά διαδεδομένο σχήμα συμπίεσης (codec) για ψηφιακή εικόνα τόσο μονόχρωμη (grayscale) όσο και έγχρωμη. Μπορεί να προσφέρει σημαντικούς βαθμούς συμπίεσης κρατώντας παράλληλα σε υψηλά επίπεδα την ποιότητα της εικόνας κάτι που το κάνει ιδανικό για τη συμπίεση ψηφιογραφικών εικόνων (bitmaps) που παρουσιάζουν μεγάλη ποικιλία χρωμάτων. Λόγω αυτών των χαρακτηριστικών χρησιμοποιείται εκτεταμένα για τη συμπίεση αρχείων εικόνας που παρουσιάζονται και μεταφέρονται στο Διαδίκτυο.

5.6.3.1 Αρχή λειτουργίας

Τεχνικά το JPEG εντάσσεται στην κατηγορία των απωλεστικών συμπιεστών(lossy compressor) και βασίζεται στην μαθηματική τεχνική DCT. Η περιγραφή που ακολουθεί ισχύει για την συμπίεση μονόχρωμων εικόνων όμως τις ίδιες αρχές ακολουθεί και η συμπίεση των έγχρωμων. Το JPEG αντιμετωπίζει την εικόνα ως αποτελούμενη από τρεις μονόχρωμες που η κάθε μια αντιστοιχεί σε ένα από τα τρία πρωτεύοντα χρώματα του μοντέλου RGB.

Τα βήματα που ακολουθεί το σχήμα JPEG για τη συμπίεση ενός αρχείου εικόνας είναι τα εξής:

1. Εφαρμογή του μετασχηματισμού DCT στο ψηφιακό σήμα που αναπαριστά την αρχική εικόνα. Στη φάση αυτή καθορίζονται οι συντελεστές DCT.
2. Κβάντωση των συντελεστών DCT. Στη φάση αυτή γίνεται η ουσιαστική συμπίεση: εκείνοι από τους συντελεστές DCT που έχουνε μικρή τιμή στρογγυλοποιούνται στο μηδεν.
3. Περαιτέρω συμπίεση με εφαρμογή του αλγόριθμου συμπίεσης RLE (Run Length Encoding). Στη φάση αυτή η σειρά των συντελεστών που έχει προκύψει από τις δύο προηγούμενες διαδικασίες συμπιέζεται κατά RLE ώστε να αποθηκευτεί και να δημιουργήσει το τελικό αρχείο .jpg

5.6.3.2 Βασικά χαρακτηριστικά

Ένα εξαιρετικά χρήσιμο χαρακτηριστικό του JPEG είναι ότι επιτρέπει στον χρήστη να καθορίσει το **βαθμό συμπίεσης** σε μία εικόνα. Δηλαδή το λογισμικό επεξεργασίας της εικόνας JPEG επιτρέπει να γίνει ρύθμιση του πόσο θα συμπιεστεί η αρχική εικόνα κάτι που καθορίζει παράλληλα και το βαθμό μείωσης της ποιότητας που θα προκληθεί. Μπορεί κανείς επομένως να επιλέξει τι τον εξυπηρετεί καλύτερα:

- Μεγάλος βαθμός συμπίεσης με μειωμένη σχετικά ποιότητα εικόνας και μικρότερο μέγεθος αρχείων ή
- Μικρός βαθμός συμπίεσης με βελτιωμένη ποιότητα εικόνας και μεγαλύτερο μέγεθος αρχείων.

Το JPEG μπορεί εύκολα να προσφέρει λόγους συμπίεσης 10:1 μέχρι και 20:1 χωρίς καμιά ορατή μείωση της ποιότητας της εικόνας. Τέτοιοι λόγοι συμπίεσης προφανώς διευκολύνουν τόσο τη μεταφορά του αρχείου μέσω δικτύου όσο και την αποθήκευση του. Μεγαλύτερες συμπιέσεις (30:1

μέχρι 50:1) είναι επίσης δυνατές αλλά με κάποιες μικρές έως μεσαίες παραμορφώσεις της εικόνας. Ενώ τέλος εξαιρετικά μεγάλες συμπιέσεις (π.χ 100:1) είναι επίσης δυνατές αν δεν ενοχλεί η σημαντική πτώση της ποιότητας.

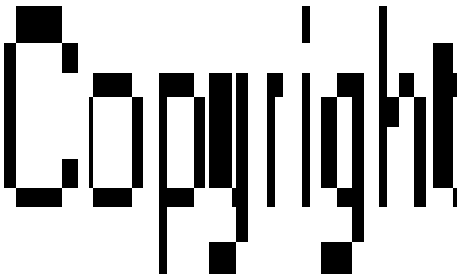
Ένα ακόμη σημαντικό χαρακτηριστικό του JPEG είναι ότι **διατηρεί τη χρωματική ποικιλία εικόνων με πραγματικό χρώμα** σε αντίθεση με το GIF που χρησιμοποιεί μόνο 256 χρώματα. Αυτό φυσικά το καθιστά καταλληλότερο από το GIF για τη συμπίεση αρχείων με πληροφορία πραγματικού χρώματος (π.χ ψηφιακές φωτογραφίες) και μεταφορά τους στο Διαδίκτυο.

Κεφάλαιο 6

Εφαρμογές και αποτελέσματα

Τα πειραματικά αποτελέσματα έγιναν χρησιμοποιώντας τη μέθοδο LSB έχοντας πάντα την αρχική εικόνα (original image) μεγέθους 512x512 εικονοστοιχείων, το υδατογράφημα (watermark) 128x128 εικονοστοιχείων, την υδατογραφημένη εικόνα(watermarked image) καθώς και το ανακτώμενο υδατογράφημα(recovered watermark). Επίσης οι επιθέσεις πραγματοποιούνται στην υδατογραφημένη εικόνα όμως τα αποτελέσματα φαίνονται και στο ανακτημένο υδατογράφημα.

Original image



Watermark

Watermarked image **Recovered watermark**

6.1 Θόρυβος

6.1.1 Θόρυβος Gauss

Για να προσθέσουμε θόρυβο "Gaussian" στην αρχική εικόνα χρησιμοποιούμε τις εντολές:

J1 = imnoise(watermarked_image,'gaussian',0,0.01);
J2 = imnoise(watermarked_image,'gaussian');
J3 = imnoise(watermarked_image,'gaussian',0,0.1);

Watermarked Image

Gaussian m=0,s=0.01

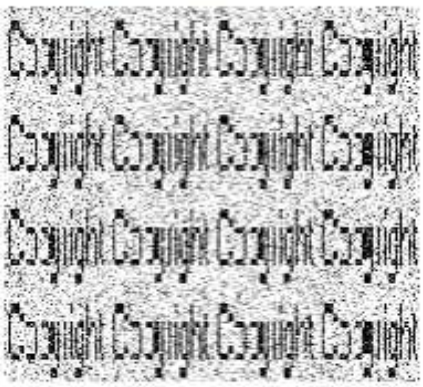
Gaussian xoris mesi timi kai typiki apoklisi

Gaussian m=0,s=0.1

και όπως βλέπουμε επηρεάζεται το ίδιο και το ανακτημένο υδατογράφημα

Recover watermark

Recover watermark with Gaussian m=0,s=0.1



6.1.2 Κρουστικός θόρυβος

Για να προσθέσουμε θόρυβο “salt & pepper” στην αρχική εικόνα χρησιμοποιούμε τις εντολές:

```
J4 = imnoise(watermarked_image,'salt & pepper');
J5 = imnoise(watermarked_image,'salt & pepper',0.05);
J6 = imnoise(watermarked_image,'salt & pepper',0.1);
```

Watermarked Image

salt&pepper

salt&pepper D=0.005

salt&pepper D=0.01

Recover watermark

Recover watermark with "salt and pepper" D=0.01

Όπως αναφέραμε και στο κεφάλαιο 4 ο κρουστικός θόρυβος έχει σαν αποτέλεσμα ορισμένα εικονοστοιχεία της εικόνας να έχουν «ανώμαλα» επίπεδα φωτεινότητας έναντι των γειτονικών τους. Τα «αλατισμένα» εικονοστοιχεία έχουν υψηλά επίπεδα φωτεινότητας, ενώ τα εικονοστοιχεία με θόρυβο «πιπεριού» έχουν πολύ χαμηλά.

6.2 Φίλτρα

6.2.1 Φίλτρα ανίχνευσης ακμών

Η διαδικασία εύρεσης των ορίων μεταξύ διαφορετικών αντικειμένων της εικόνας τα οποία συναντούμε στις περιοχές όπου έχουμε απότομη αλλαγή στις τιμές φωτεινότητας ονομάζεται ανίχνευση ακμών (edge detection). Έχει προταθεί μια ποικιλία από ανιχνευτές ακμών όπως ο Prewitt, ο Sobel και ο Canny. Για την εύρεση ακμών στο Matlab χρησιμοποιούμε τις εντολές:

```
BW1 = edge(watermarked_image,'prewitt');
BW2 = edge(watermarked_image,'sobel');
BW3 = edge(watermarked_image,'canny');
```

Watermarked Image

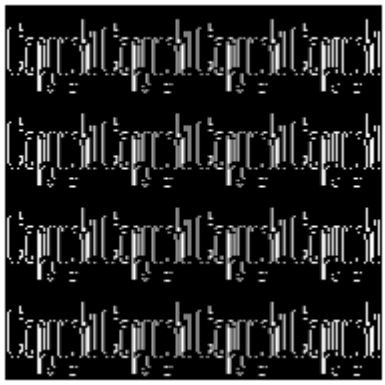
prewitt filter

sobel filter

canny filter

Recover watermark

Recover watermark with canny filter



6.2.2 Φίλτρο μέσης τιμής (mean filter)

Για να χρησιμοποιήσουμε το φίλτρο μέσης τιμής πρέπει πρώτα να προσθέσουμε θόρυβο στην εικόνα μας (π.χ salt&pepper) και έπειτα το φίλτρο. Το αποτέλεσμα είναι πολύ ικανοποιητικό όσο αφορά την απαλλαγή από τον θόρυβο αλλά ταυτόχρονα δημιουργείται μια θαμπάδα στην εικόνα. Χρησιμοποιήσαμε μάσκα εξομάλυνσης 5x5 διότι όσο μεγαλύτερη είναι η μάσκα τόσο περισσότερο εξομαλύνεται η εικόνα. Παρακάτω βλέπουμε τις εντολές που χρησιμοποιήσαμε, τα αποτελέσματα της εξομάλυνσης στην υδατογραφημένη εικόνα και στο αρχικό υδατογράφημα καθώς και τις διαφορές της υδατογραφημένης με την φιλτραρισμένη εικόνα.

```
J = imnoise(watermarked_image,'salt & pepper',0.3);
H1 = fspecial('average',[5 5]); K1 = imfilter(J,H1);
```

Watermarked Image

with salt&pepper noise

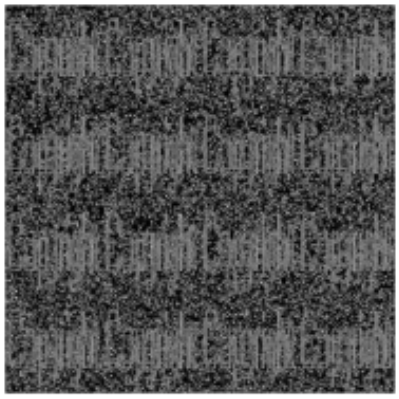
average filter

differences watermarked image+average fillter

I= imnoise(watermark,'salt & pepper',0.3);
H2 = fspecial('average',[5 5]); K2 = imfilter(I,H2);

Recover Watermark with noise

differences recover watermark+average filter



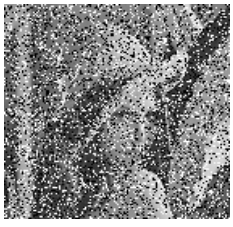
6.2.3 Φίλτρο μεσαίας τιμής (median filter)

Για να χρησιμοποιήσουμε το φίλτρο μεσαίας τιμής πρέπει πρώτα να προσθέσουμε θόρυβο στην εικόνα μας (π.χ salt&pepper) και έπειτα το φίλτρο. Με την εφαρμογή του 5x5 median φίλτρου παρατηρούμε ότι η υδατογραφημένη εικόνα είναι λιγότερο θολωμένη από την εικόνα με mean φίλτρο καθώς επίσης το υδατογράφημα έχει περισσότερα λάθη από το υδατογράφημα που εφαρμόζεται mean φίλτρο. Όσο το μέγεθος της μάσκας μεγαλώνει τόση μεγαλύτερη απώλεια πληροφορίας έχουμε στο αποτέλεσμα που τείνει να μοιάσει τεχνητά ζωγραφισμένο.

L = imnoise(watermarked_image,'salt & pepper',0.3);
L1 = medfilt2(watermarked_image,[5 5]);

Watermarked Image

with salt&pepper noise

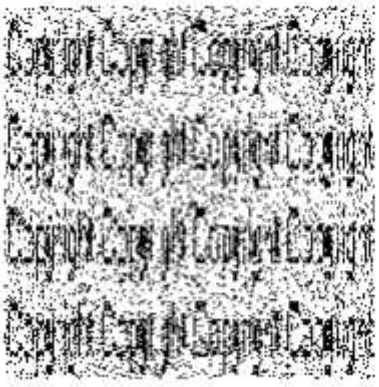


median filter

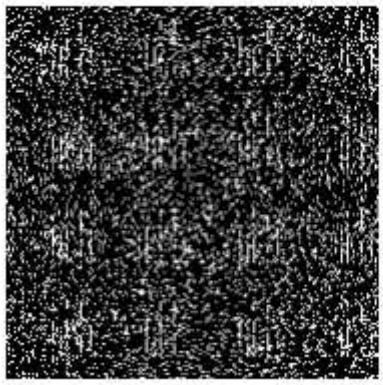
differences watermarked image+median fillter

```
M= imnoise(I,'salt & pepper',0.3);
L2 = medfilt2(M,[5 5]);
```

Recover Watermark with noise



differences Reover watermark+median filter



6.2.4 Φίλτρο min/max

Εφαρμόζοντας τις παρακάτω εντολές υλοποιούμε το φίλτρο min/max χρησιμοποιώντας μια γειτονιά εικονοστοιχείων 5x5, επιλέγοντας το 1 δηλαδή το ελάχιστο στα 25 στοιχεία άρα φίλτρο ελαχίστου (A) και αντίστοιχα επιλέγοντας το 25 δηλαδή το μέγιστο στα 25 στοιχεία άρα φίλτρο μεγίστου (B). Το φίλτρο ελαχίστου επέκτεινε τις σκούρες περιοχές της εικόνας και συρρίκνωσε τις λευκές. Αντίθετα το φίλτρο μεγίστου επέκτεινε τις λευκές περιοχές και συρρίκνωσε τις σκούρες.

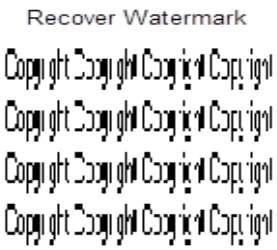
A = ordfilt2(watermarked_image,1,ones(5,5));

B = ordfilt2(watermarked_image,25,ones(5,5));

Watermarked Image

filtro elaxistou

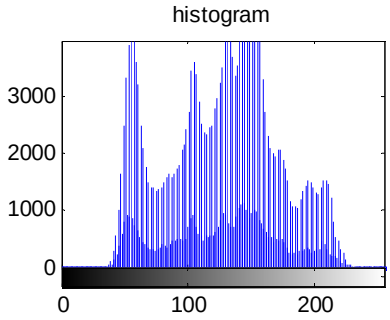
filtro megistou

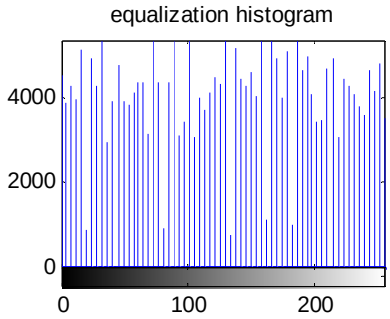


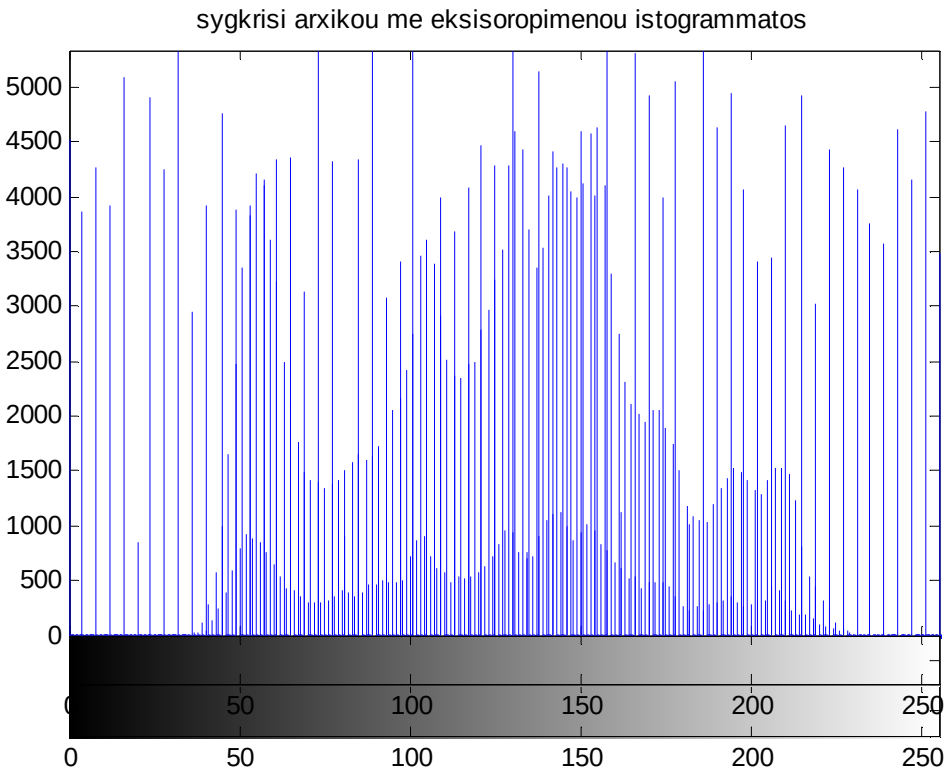
6.2.5 Εξισορρόπηση ιστογράμματος

Στο ιστόγραμμα της υδατογραφημένης εικόνας παρατηρούμε ότι οι φωτεινότητες της εικόνας κατανέμονται σε περιορισμένη ζώνη με αποτέλεσμα η αντίθεση της εικόνας να είναι μειωμένη. Με την τεχνική εξισορρόπησης ιστογράμματος παρατηρούμε ότι οι φωτεινότητες κατανέμονται σε όλο το δυνατό εύρος φωτεινοτήτων με αποτέλεσμα η εξισορροπημένη εικόνα να είναι αυξημένης αντίθεσης. Οι εντολές που χρησιμοποιήσαμε είναι οι:

imhist(watermarked_image)
C=histeq(watermarked_image);
imhist(C)







6.3 Περιστροφή

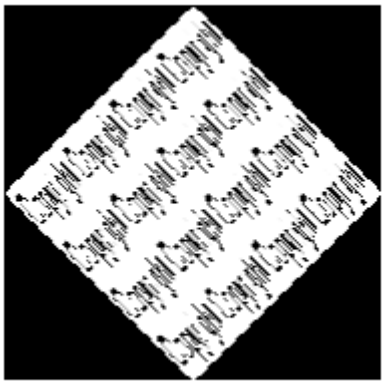
Η εντολή *D=imrotate(watermarked_image,45,'bilinear'');* που χρησιμοποιούμε παρακάτω γυρίζει την εικόνα αριστερόστροφα κατά 45 μοίρες χρησιμοποιώντας τη μέθοδο παρεμβολής bilinear. Άλλες μέθοδοι μπορεί να είναι η “nearest” και η “bicubic”. Αν θέλουμε να περιστρέψουμε την εικόνα μας δεξιόστροφα βάζουμε στην γωνία μας αρνητική τιμή.

watermarked image

rotated watermarked image

Recover Watermark

Rotated Recovered Watermark



6.4 Κλιμάκωση

Μειώνουμε την υδατογραφημένη εικόνα σε μέγεθος 256x256 και το αποτέλεσμα είναι ότι η εικόνα που προκύπτει είναι πιο θολή. Στο υδατογράφημα παρουσιάζονται περισσότερα λάθη από ότι στο αρχικό μας.

F=imresize(watermarked_image,[256 256]);

G=imresize(I,[256 256]);

watermarked Image

Resized Watermarked Image

Recovery Watermark with noise

Resized Recovery Watermark

6.5 Κοπή εικόνας

Όπως παρατηρούμε στα αποτελέσματα της τεχνικής που χρησιμοποιήσαμε για να κόψουμε κομμάτι της υδατογραφημένης εικόνας με την εντολή:

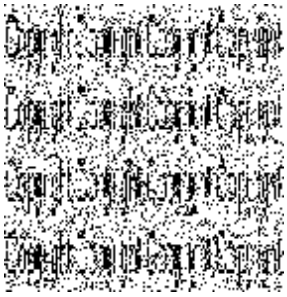
N = imcrop(watermarked_image,[60 40 225 300]);

το ανακτημένο υδατογράφημα έχει λιγότερα λάθη. Παρόλα αυτά όμως έχει επηρεαστεί στο σημείο όπου έχει κοπεί η εικόνα μας και επίσης δεν είναι σχεδόν καθόλου αναγνώσιμο.

Watermarked Image

Cropped Watermarked Image

Recovered Watermark with noise

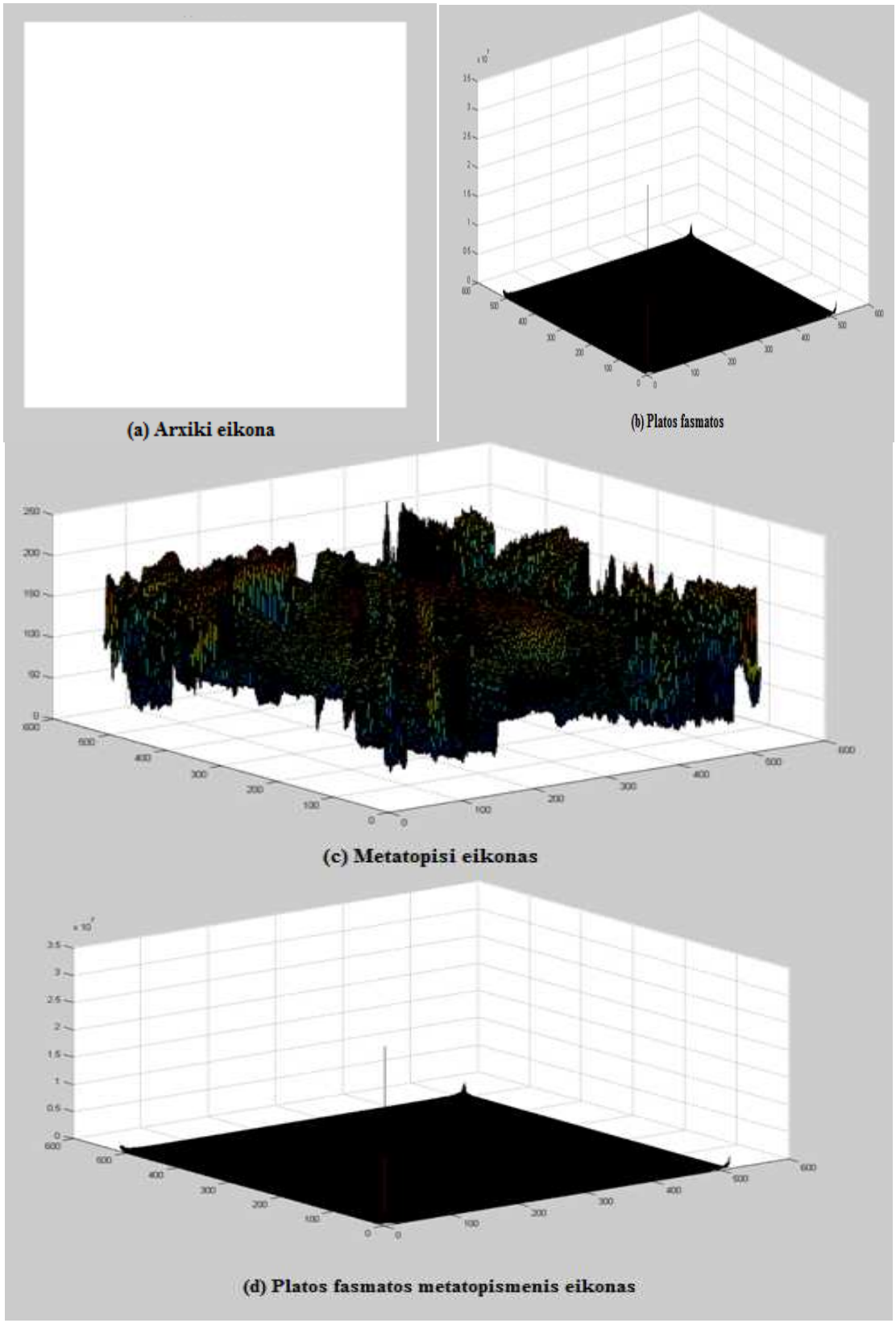


Cropped Recovered Watermark

6.6 Κωδικοποιήσεις μετασχηματισμών

6.6.1 Μετασχηματισμός 2D-DFT

Με την εντολή *image_fft=fft2(R);* προσδιορίζουμε τον 2D-DFT το πλάτος του οποίου δείχνεται στο σχήμα (b). Με την εντολή *imagefft=fft2(imageshifted);* μετατοπίζουμε την εικόνα οπότε (σε τρισδιάστατη μορφή) η εικόνα παίρνει τη μορφή της εικόνας (c). Μετασχηματίζουμε την μετατοπισμένη εικόνα με την εντολή *imagefft=fft2(imageshifted);* οπότε παίρνουμε την εικόνα (d) για το πλάτος του μετασχηματισμού όπου μπορούμε να παρατηρήσουμε ότι όπως αναμενόταν από την ιδιότητα της χωρικής μετατόπισης, το πλάτος του φάσματος παραμένει σταθερό και ίδιο με αυτό της εικόνας (b). Τέλος βρίσκουμε το τελικό κεντραρισμένο φάσμα με την εντολή *shiftedimagefft=fftshift(imagefft);*. Το πλάτος του τελικού φάσματος φαίνεται στην εικόνα (e) ενώ στην εικόνα (f) δείχνεται το φάσμα με την μορφή γκρι εικόνας.

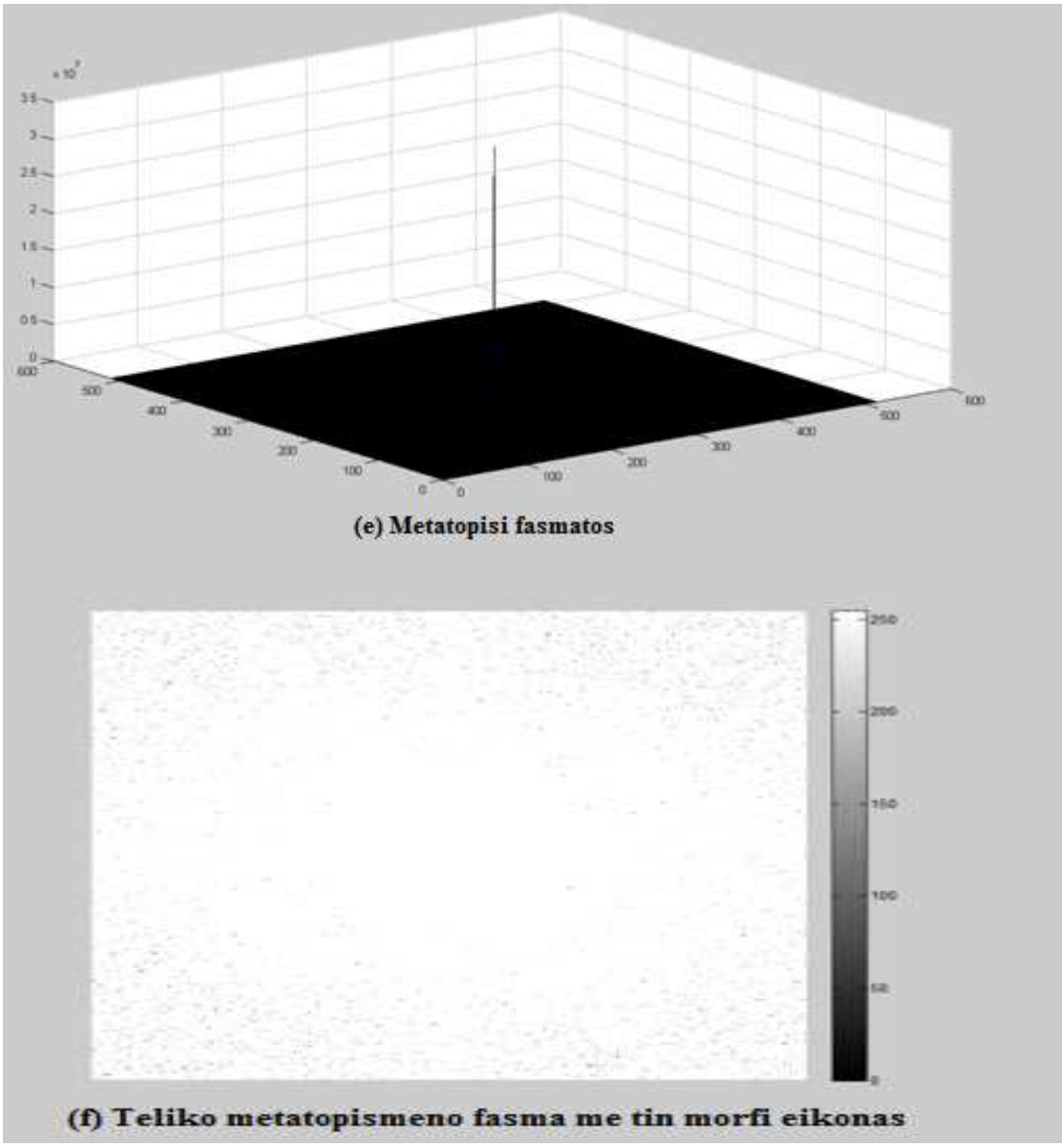


(a) Arxiki eikona

(b) Platos fasmatos

(c) Metatopisi eikonas

(d) Platos fasmatos metatopismenis eikonas



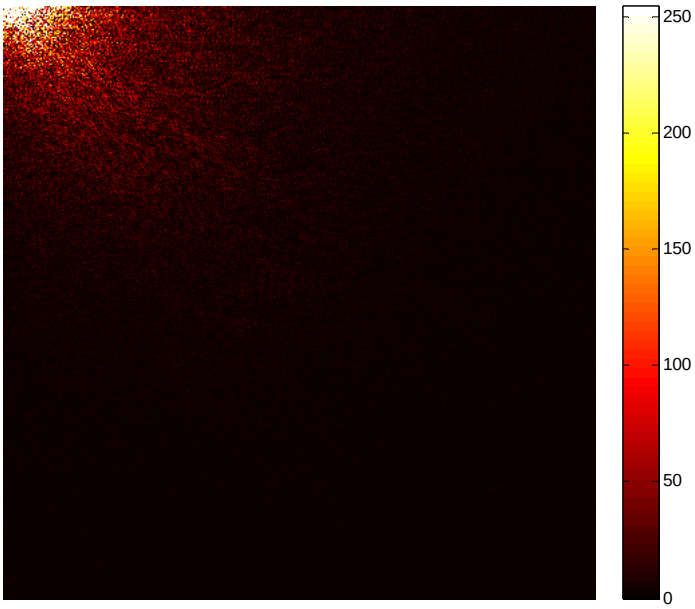
(e) Metatopisi fasmatos

(f) Teliko metatopismeno fasma me tin morfi eikonas

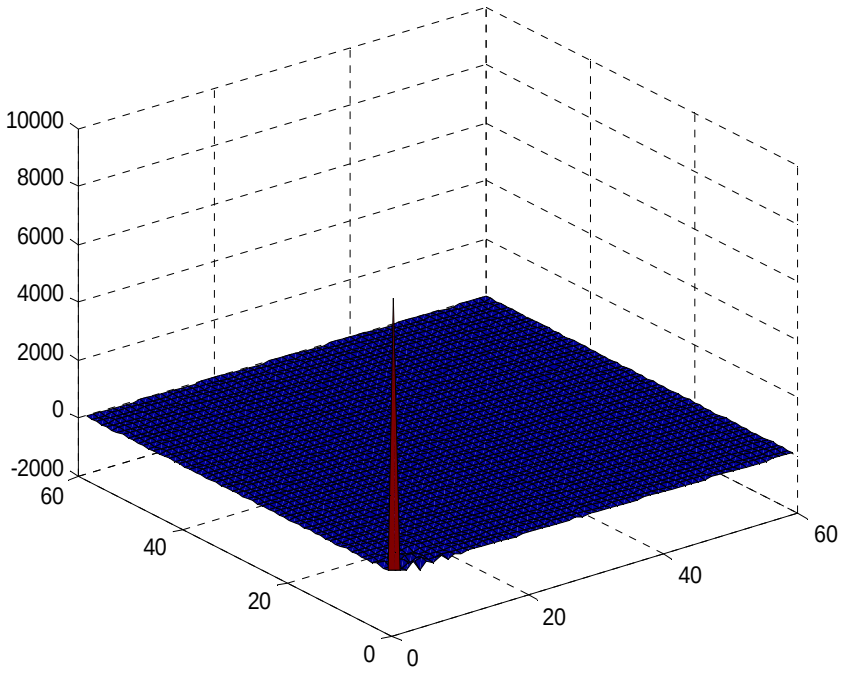
6.6.2 Μετασχηματισμός 2D-DCT

Η εφαρμογή του 2D-DCT μας δίνει το φάσμα που φαίνεται στην εικόνα (1) όπου μπορούμε να δούμε ότι κοντά στην αρχή των αξόνων συγκεντρώνονται οι σημαντικότεροι, σε πλάτος, συντελεστές. Αυτό φαίνεται καλύτερα στην 3D απεικόνιση του φάσματος της περιοχής [0:60, 0:60] εικόνα (2).

(1) Fasma tou 2D-DCT



(2)Trisdiastati apeikonisi tou fasmatos



6.7 Με απώλειες συμπίεση JPEG

JPEG με δείκτη 100

Η υδατογραφημένη εικόνα και το υδατογράφημα συμπιέστηκαν χρησιμοποιώντας με απώλειες συμπίεση JPEG με δείκτη 100. Ο δείκτης κυμαίνεται από 0 έως 100, όπου 0 είναι καλύτερη συμπίεση και 100 είναι καλύτερη ποιότητα . Το υδατογράφημα καθώς και η υδατογραφημένη εικόνα παρουσιάζουν σχεδόν άριστη ποιότητα.

JPEG με δείκτη 75

Η υδατογραφημένη εικόνα και το υδατογράφημα συμπιέστηκαν χρησιμοποιώντας με απώλειες συμπίεση JPEG με δείκτη 75. Τα αποτελέσματα είναι πολύ καλής ποιότητας και δεν έχουν ιδιαίτερες διαφορές από τα αποτελέσματα της συμπιεσμένης εικόνας με δείκτη 100.

JPEG με δείκτη 50

Η υδατογραφημένη εικόνα και το υδατογράφημα συμπιέστηκαν χρησιμοποιώντας με απώλειες συμπίεση JPEG με δείκτη 50. Το υδατογράφημα έχει αποδεκτή ποιότητα σε σύγκριση με το υδατογράφημα που έχει συμπιεστεί με δείκτη 100.

watermarked image

watermarked image JPEG 50

recover watermark

recover watermark with JPEG 50

JPEG με δείκτη 25

Η υδατογραφημένη εικόνα και το υδατογράφημα συμπιέστηκαν χρησιμοποιώντας με απώλειες συμπίεση JPEG με δείκτη 25. Τα αποτελέσματα είναι μέτριας ποιότητας σε σχέση με τον δείκτη 100.

watermarked image

watermarked image JPEG 25

recover watermark

recover watermark with JPEG 25

Κεφάλαιο 7

Συμπεράσματα

Το ψηφιακό υδατογράφημα παρέχει δυνατότητες όπως η ενσωμάτωση πληροφοριών μέσα σε ένα ψηφιακό αντικείμενο με σκοπό οι πληροφορίες αυτές να εξασφαλίζουν στον ιδιοκτήτη του ψηφιακού αντικειμένου τον έλεγχο για νόμιμη κατοχή και χρήση αντικειμένου από τρίτους, καθώς και τη δυνατότητα αναγνώρισης παράνομων τροποποιήσεων του υδατογραφημένου αντικειμένου.

Συνεπώς πρέπει να γνωρίζουμε ότι δεν υπάρχει σύστημα υδατογράφησης στο οποίο να ικανοποιούνται όλες οι απαιτήσεις. Ανάλογα με τον προορισμό της εφαρμογής, σχεδιάζεται και το κάθε σύστημα υδατογράφησης.

Η ελλιπής ανθεκτικότητα σε κάποιες επιθέσεις και το περιορισμένο ωφέλιμο φορτίο του υδατογραφήματος αποτελούν προβλήματα για την ασφάλεια των δεδομένων.

Στην παρούσα εργασία πραγματοποιήθηκε μελέτη πάνω στην υδατογράφηση. Στο Κεφάλαιο 2 αναφέρονται ιστορικά παραδείγματα κρυπτογράφησης και υδατογράφησης ανά περιόδους. Ακολουθεί το Κεφάλαιο 3 όπου αναλύονται τα είδη κρυπτοσυστημάτων, συμμετρικά και ασύμμετρα καθώς και οι δύο σημαντικές μέθοδοι ECB και CBC. Όσο αφορά την υδατογράφηση γίνεται διαχωρισμός των υδατογραφημάτων σε ορατά και αόρατα, όπως επίσης γίνεται μια εκτενής παρουσίαση των εφαρμογών και των ιδιοτήτων της υδατογράφησης. Τέλος έχουμε τη σύγκριση των δύο εφαρμογών προστασίας και ασφάλειας της εικόνας.

Κάποιες από τις τεχνικές υδατογράφησης όπως η LSB παρουσιάζονται αναλυτικά και βλέπουμε την εφαρμογή και τα αποτελέσματα της κάθε τεχνικής στο Κεφάλαιο 4. Στη συνέχεια στο Κεφάλαιο 5 παρουσιάστηκαν και αναλύθηκαν οι επιθέσεις και παραμορφώσεις που μπορούν να παρεμποδίσουν το σκοπό του υδατογραφήματος , ενώ στο Κεφάλαιο 6 είχαμε την εφαρμογή τους στο αρχικό υδατογράφημα και παρατηρήσαμε τις αλλαγές που είχε σε αυτή καθώς και στο ανακτημένο υδατογράφημα. Σε κάποια από αυτά, οι παραμορφώσεις δεν ήταν εμφανείς αφού η διαφορά της αρχικής και της υδατογραφημένης ήταν ελάχιστη. Υπήρχαν όμως και ανακτημένα υδατογραφήματα με έντονες αλλοιώσεις καθώς ίσα που διακρίναμε την ομοιότητα αρχικού και υδατογραφημένου αντικειμένου.

Τέλος, ως παράρτημα παρουσιάζουμε τον αλγόριθμο που χρησιμοποιήσαμε για τις διάφορες τεχνικές υδατογράφησης, καθώς επίσης και τις επιθέσεις και παραμορφώσεις που είχε στην υδατογραφημένη εικόνα και τις επιπτώσεις στο ανακτημένο υδατογράφημα.

Βιβλιογραφία

[1] Arnold, M., Schmucker, M., Wolthusen, D.S. (2003) Techniques and applications of digital watermarking and content protection. Artech House.

[2] H.M. Gladney, F.C. Mintzer, and F. Schiattarella, "Safeguarding Digital Library Contents and Users: Digital Images of Treasured Antiquities," D-Lib Magazine, http://www.dlib.org/dlib/july97/vatican/07gladney.html, July 1997

[3] Katzenbeisser, S., Petitcolas, A.P.F. (2000) Information hiding techniques for steganography and digital watermarking. Artech House.

[4] I.J.Cox, J. Kilian, T. Leighton, T. Shamoon,"Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans.Image Processing, vol.6, no. 12, pp.1673-1687, Dec. 1997.

[5] X.G. Xia, C. G. Boncelet, G. R. Arce, "A multiresolution watermark for digital images", Proc. IEEE Int. Conf. Image Processing, v.1, pp.548-551, Santa Barbara, CA, Oct 26-29, 1997.

[6] X.G. Xia, C. G. Boncelet, G. R. Arce, "Wavelet transform based watermark for digital images", Optics Express, vol.3, 20. 12, pp. 497-511, Dec. 1998.

[7] C.I. Podilchuk, W. Zeng, "Image-Adaptive Watermarking Using Visual Models", IEEE Trans. Selected Areas of Comm., vol.16, no.4, pp. 525-539, May 1998.

[8] C.I. Podilchuk, E.J. Delp,"Digital watermarking: algorithms and applications", IEEE Sig. Proc. Mag., vol.18, no.4, pp.33-46, July 2001.

[9] W. Bender, D. Gruhl, N. Morimoto, A.Lu, "Techniques for data hiding", IBM Systems Journal, vol.35, no. 3&4,pp. 313-336,1996`

[10] E. Koch,J. Zhao, "Towards robust and hidden image copyright labelling", Proc. IEEE Workshop Nonlinear Signal and Image Process., I. Pitas, Ed., Neos Marmaras, Greece, June 20-22, 1995,pp. 452-455

[11] J.-F. Delaigle, C.D.Vleeschouwer, B. Macq, "Digital Watermarking", Proc. SPIE, Optimal Security and Counterfeit Deterrence Techniques, vol. 2659. pp. 99-110, Feb.1996

[12] I.J. Cox, M. L. Miller, J.A.Bloom, Digital Watermarking. San Francisco, CA: Morgan Kaufamnn, 2002.

[13] E.T. Lin, E.J.Delp,"A Review of Data Hiding in Digital Images", Proc. Image Processing, Image Quality, Image Capture Systems Conference (PICS'99),Savannah, Georgia, pp.274-278, April 25-28, 1999

[14] S. Craver, N. Memon, B.Yeo, M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications", IEEE Journal of Selected Areas in Communications, vol. 16, no. 4, May 1998

[15] S. Katzenbeisser, Information Hiding Techniques for Steganography and Digital Watermarking, Norwood: Artech House Inc., 2000

[16] R. Venkatesan, S.- M. Koon, M. H Jakubowski, P. Moulin, "Robust Image Hashing", Proc. IEEE Int. Conf. Image Processing, ICIP 2000, Vancouver, Canada, Sept. 10-13,2000

[17] S. Pereira, T. Pun, "Robust template matching for affine- resistant image watermarks", IEEE Transactions on Image Processing, vol.9,no.6,pp 1123-1129,2000

[18] C.-T. Hsu, J.-L. Wu, "Hidden digital watermarks in images", IEEE Transactions on Image Processing, vol.8, no.1, pp.58-68, 1999

[19] F. Harting, M. Kutter, “Multimedia Watermarking Techniques”, Proceedings of the IEEE, vol. 87, no. 7, July 1999, pp 1079-1107.

[20] Ιωάννης Πήτας, Ψηφιακή Επεξεργασία Εικόνας, 1999

[21] Νικόλαος Η. Παπαμάρκος. Ψηφιακή Επεξεργασία & Ανάλυση Εικόνας ,έκδοση 2η,2010

[22] Σ.Ν Δημητριάδης Α.Σ Πομπόρτσης Ε.Γ Τριανταφύλλου, Τεχνολογία Πολυμέσων, Θεωρία και Πράξη, Εκδόσεις Τζιόλα

[23] Rafael C. Gonzalez, Richard E. Woods, Digital Image Processing, 2008, third edition

[24] R.J. Anderson, F. A. P. Peticolas, "On the limits of Steganography," IEEE J. Sel.
Areas Commun Special Issue on Copyright and Privacy Protection, vol. 16, no. 4, pp.474-481, May 1998

[25] G. L. Friedman, "The trustworthy camera: restoring credibility to the
photographic image",IEEE Trans. Consumer Electronics, vol. 39, no4, pp.905-910, 1993

[26] M. Charrier, D. S. Cruz, M. Larsson, "JPEG2000, the next millennium compression standard for still images," Proc. IEEE Intern. Conf. Multimedia &
Computing Systems,ICMCS'99, vol.1,pp.131-132, Florence, Italy, June 1999

[27] M. Barno, C.I. Podillchuk, F. Bartolini, E.J Delp, ''Watermark Embedding: Hiding a Signal Within a Cover Image," IEEE Communication Magazine, Special Issue on Digital Watemarking for Copyright Protection: A Communication Perspective, vol. 39, no.8, pp102-108, Aug. 2001.

[28] M. D. Swanson, B. Zhu, A. H. Tewfik, "Transparent Robust Image Watermarking," Proc. IEEE International Confence on Image Processing, vol. 3, pp. 211-214, 1996.

[29] J.F. Delaigle, C.De Vleeschouwer, B.Macq,"Watermarking algorithm based on a human visual model," Signal Processing, vol. 66, no.3, pp.319-335, 1998.

[30] M. Barni, F. Bartolini, V.Cappellini, A.Piva,"A DCT- domain system for robust image watermarking," Signal Processing, vol.66, no.3,pp357-372,1998.

[31] FRANK HARTUNG, STUDENT MEMBER, IEEE, AND MARTIN KUTTER "Multimedia Watermarking Techniques "PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999

[32]http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

[33]http://el.wikipedia.org/wiki/%CE%A3%CF%84%CE%B5%CE%B3%CE%B1%CE%BD%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

[34] http://www.filaderlis.com/ebooks/kryptografeia.pdf

[35] http://users.uom.gr/~steph/material/crypto/HAC_Ch01.pdf

[36] http://www.vis.uky.edu/~cheung/courses/ee639_fall04/readings/procieeehartungkutter.pdf

[37] http://scripts.top4download.com/steganography/esglu.html

[38] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.158.6849

[39] http://en.wikipedia.org/wiki/Digital_watermarking

[40] www.research.ibm.com/image_apps/watermark.html

[41] http://www.dlib.org/dlib/december97/ibm/12lotspiech.html

[42] http://utopia.duth.gr/~vkatos/documents/the_book/

[43] http://students.ceid.upatras.gr/~mprokala/techarticles/cryptography/AES/aes.htm

[44] http://www.vu.union.edu/~shoemakc/watermarking

[45] http://www.mathworks.com/matlabcentral/fileexchange/5195-watermarking

[46] http://www.mathworks.com/matlabcentral/fileexchange/3508-digital-image-watermarking

[47] http://www.mathworks.com/matlabcentral/fileexchange/14079-simple-watermarking-by-using-wavelets

[48] http://homepages.cae.wisc.edu/~ece533/project/f06/elliott_schuette_rpt.pdf

[49] http://pdincau.wordpress.com/2010/03/22/lsb-watermarking-using-matlab

[50] http://web.vu.union.edu/~shoemakc/watermarking/watermarking.html

[52] http://www.hackchina.com/en/r/187699/test1.m__html

[53] http://www.image.ece.ntua.gr/papers/645.pdf

[54] http://www.hackchina.com/en/r/85682/wave2.m__html

[55] http://www.mathworks.com/matlabcentral/fileexchange/8745-image-compression-using-wavelets/content/wavelet.m

[56] http://homepages.inf.ed.ac.uk/rbf/HIPR2/wksheets.htm

[57] http://portal.survey.ntua.gr/main/courses/general/sigproc/lectures/dsp2005_06.pdf

[58] ecourses.dbnet.ntua.gr/fsr/10768/askisi_3A_tutorial.pdf

[59] ecourses.dbnet.ntua.gr/fsr/10751/09_ERMapper_filters.pdf

[60] xanthippi.ceid.upatras.gr/people/psarakis/courses/.../CV_1.ppsx

[61] www.hep.upatras.gr/class/download/psi_epe_iko/kef3.pdf

[62] www.cs.ucy.ac.cy/~nicolast/courses/teds150/lectures/IP04.pdf

[63] http://www.digicamhelp.com/learn/image-editing/image-cropping.html

[64] http://www.it.uom.gr/project/MultimediaTechnologyNotes

[65] http://www.image.ntua.gr/meleti172KTP/node/12

[66] http://www.petitcolas.net/fabien/watermarking/image_database/index.html

Παράρτημα

Αλγόριθμος Κρυπτογράφησης

```
%in GUI select one of the task 'hide image'  or 'Recover image'

%select 'hide image' radiobutton to hide image and click the 'select cover image'
%button to select a cover image(jpg or png).Then 'select secret image'
%button activates, click it to select image you want to hide in
%cover image if it is too big error dialog appears,select
%a smaller image.After selecting secret image 'hide' button
%activates click it to hide secret image in cover image.
%Dialog box appears to save that image.

%select 'recover image' radiobutton to recover secret image
%image from cover image.Select a cover image (png).
%Then 'recover' button activates click it to recover image.
%Secret image appears in axes 2,and it will be saved in
%current directory with random name.

%NOTE:selecting radiobutton in between the process
%clear the axes.Then you have to restart the whole process
%from selecting the cover image and then continue.
%
%water.png has a hidden image use GUI to recover it.
gui_Singleton = 1;
```

```
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @imgsteg_OpeningFcn, ...
                   'gui_OutputFcn',  @imgsteg_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
   gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
   [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
   gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT


% --- Executes just before imgsteg is made visible.
function imgsteg_OpeningFcn(hObject, eventdata, handles, varargin)
```



```
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to imgsteg (see VARARGIN)

% Choose default command line output for imgsteg
handles.output = hObject;
handles.rad1=1;
handles.rad2=0;
handles.cfilename=' ';
handles.cpathname=' ';
handles.sfilename=' ';
handles.spathname=' ';
handles.equ=0;
set(handles.pushbutton2,'Enable','off');
set(handles.pushbutton3,'Enable','off');

axes(handles.axes1);
axis off
axes(handles.axes2);
axis off

% Update handles structure
guidata(hObject, handles);

% UIWAIT makes imgsteg wait for user response (see UIRESUME)
% uiwait(handles.figure1);
```

```
% --- Outputs from this function are returned to the command line.
function varargout = imgsteg_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;


% --- Executes on button press in pushbutton1.
function pushbutton1_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton1 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
lsb=1;
[handles.cfilename,handles.cpathname] = uigetfile(  {'*.jpg';'*.png';'*.bmp';'*.*'}, ...
       'Select cover image');
```



```
axes(handles.axes1);
I=imread([handles.cpathname handles.cfilename]);

imageinfo_cover=imfinfo([handles.cpathname handles.cfilename]);
val_red=I(:,:,1);
if handles.rad2==1
emb=zeros(3,7);
emb(1,:)=bitget(val_red(1,50:56),lsb);
emb(2,:)=bitget(val_red(1,57:63),lsb);
emb(3,:)=bitget(val_red(1,64:70),lsb);
emb_double=bi2de(emb);
emb=char(emb_double);
emb=emb';
 if ~strcmp(emb,'yes')
    axes(handles.axes1);cla
    errordlg(['No hidden image in ' handles.cfilename],'Select another Image');
 else
    image(I),axis off
    set(handles.pushbutton3,'Enable','on');
 end
else
    image(I),axis off
    image_height=imageinfo_cover.Height;
    image_width=imageinfo_cover.Width;
    handles.equ=((image_height-1)*(image_width-mod(image_width,8)))/8;
    set(handles.pushbutton2,'Enable','on');
end
guidata(hObject, handles);
```

```
% --- Executes on button press in pushbutton2.
function pushbutton2_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
if handles.rad2==1

else
   [handles.sfilename handles.spathname]=uigetfile({'*.jpg';'*.png'},'Select an Image');
   imageinfo_cover=imfinfo([handles.spathname handles.sfilename]);
   image_height=imageinfo_cover.Height;
   image_width=imageinfo_cover.Width;

   equ=image_width*image_height;

   if equ <=handles.equ
   I=imread([handles.spathname handles.sfilename]);
   set(handles.pushbutton3,'Enable','on');
   axes(handles.axes2);
   image(I);axis off
```



```
else
   errordlg('Select another Image','Image too big');
   end
   guidata(hObject, handles);
end


% --- Executes on button press in pushbutton3.
function pushbutton3_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

if handles.rad1==1
lsb=1;
I=imread([handles.cpathname handles.cfilename]);
imageinfo_cover=imfinfo([handles.cpathname handles.cfilename]);
image_height=imageinfo_cover.Height;
image_width=imageinfo_cover.Width;


val_red=I(:,:,1); %get the red color matrix

I_sec=imread([handles.spathname handles.sfilename]);
imageinfo_sec=imfinfo([handles.spathname handles.sfilename]); %get information of secret image
i_sec_height=imageinfo_sec.Height;          % secret image height
i_sec_width=imageinfo_sec.Width;            % secret image width
```

```
val_red=double(val_red);

%hide the secret image height
i_sec_height_bin=de2bi(i_sec_height,16);
val_red(1,1:16)=bitset(val_red(1,1:16),1,i_sec_height_bin);

%hide the secret image width
i_sec_width_bin=de2bi(i_sec_width,16);
val_red(1,17:32)=bitset(val_red(1,17:32),1,i_sec_width_bin);

%hide an identity, that this image has a secret image.
emb=('yes');
emb_bin=de2bi(double(emb));
val_red(1,50:56)=bitset(val_red(1,50:56),lsb,emb_bin(1,1:7));
val_red(1,57:63)=bitset(val_red(1,57:63),lsb,emb_bin(2,1:7));
val_red(1,64:70)=bitset(val_red(1,64:70),lsb,emb_bin(3,1:7));

I(:,:,1)=val_red;

i_sec_length=i_sec_height*i_sec_width;
I_sec_bin=zeros(i_sec_length*3,8);
```



```
I_sec_bin=de2bi(double(I_sec));    %convert the secret image to binary
Ipix_counter=1;                    %set a counter for the  pixels


len=mod(image_width,8);
len=image_width-len;

for count_hi=2:image_height
   count_wi=1;
   for count_wi=1:8:len-8
        val_red(count_hi,count_wi:count_wi+7)=...
            bitset(val_red(count_hi,count_wi:count_wi+7),1,I_sec_bin(Ipix_counter,:));

      Ipix_counter=Ipix_counter+1;
     if Ipix_counter>i_sec_length*3
      break;
     end


   end
     if Ipix_counter>i_sec_length*3
      break;
     end

end

I(:,:,1)=val_red;
```

```
[filename, pathname] = uiputfile('.png', 'Save Image as');
imwrite(I,[pathname filename ],'png');
set(handles.pushbutton3,'Enable','off');
set(handles.pushbutton2,'Enable','off');
axes(handles.axes1);cla
axes(handles.axes2);cla
msgbox(['The secret image ' handles.sfilename ' is in '  filename]);
else
  %case 2:Dercyption(Reocver the secret image from cover image)
lsb=1;
I=imread([handles.cpathname handles.cfilename]);

imageinfo_cover=imfinfo([handles.cpathname handles.cfilename]);%cover image information
image_height=imageinfo_cover.Height;        %cover image height
image_width=imageinfo_cover.Width;          %cover image width

val_red=I(:,:,1);                       %get the red color matrix

%extract the secret image height and width from 1st 32pixel of cover image
i_sec_height=bi2de(bitget(double(val_red(1,1:16)),1));
i_sec_width=bi2de(bitget(double(val_red(1,17:32)),1));
i_sec_length=i_sec_height*i_sec_width;
```



```
I_sec_bi=zeros(i_sec_length*3,8);%initialize a zero matrix
Ipix_counter=1;                 %counter for pixels

len=mod(image_width,8);
len=image_width-len;

for count_hi=2:image_height
   count_wi=1;
   for count_wi=1:8:len-8
      I_sec_bi(Ipix_counter,1:8)=...
      bitget(val_red(count_hi,count_wi:count_wi+7),1);

      Ipix_counter=Ipix_counter+1;
      if Ipix_counter>i_sec_length*3
        break;
      end


   end
      if Ipix_counter>i_sec_length*3
        break;
      end
end

image1=reshape(bi2de(I_sec_bi),i_sec_height,i_sec_width,3);
image1=uint8(image1);
rn=num2str(rand(1,1));
imwrite(image1,[num2str(rn(3:end)) '.png'],'png');
axes(handles.axes2);
```

```
image(image1);axis off
msgbox(['The image '  rn(3:end) '.png is extracted from ' handles.cfilename ' ,it is in your current
directory']);
end

% --------------------------------------------------------------------
function uipanel1_SelectionChangeFcn(hObject, eventdata, handles)
% hObject    handle to uipanel1 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
switch get(hObject,'Tag')   % Get Tag of selected object
   case 'radiobutton1'
      handles.rad1=1;
      handles.rad2=0;
      guidata(hObject, handles);
      % code piece when radiobutton1 is selected goes here
       axes(handles.axes1);cla
       axes(handles.axes2);cla
       set(handles.pushbutton3,'String','Hide');
       set(handles.pushbutton3,'Enable','off');
       set(handles.pushbutton2,'Enable','off');
       set(handles.pushbutton1,'Enable','on');
```



```
case 'radiobutton2'
      % code piece when radiobutton2 is selected goes here
      % ...
      handles.rad2=1;
      handles.rad1=0;
      guidata(hObject, handles);
       axes(handles.axes1);cla
       axes(handles.axes2);cla
       set(handles.pushbutton3,'String','Recover');
       set(handles.pushbutton3,'Enable','off');
       set(handles.pushbutton2,'Enable','off');
       set(handles.pushbutton1,'Enable','on');
end
```

Αλγόριθμος Υδατογράφησης

```
%Project:   Least Significant Bit Substitution


clear all;

% save start time
start_time=cputime;

% read in the cover object
file_name='_lena_std_bw.bmp';
cover_object=imread(file_name);

% read in the message image
file_name='_copyright1.bmp';
message=imread(file_name);
I= imnoise(message,'salt & pepper',0.3);
% convert to double for normalization, then back again
message=double(message);
message=round(message./256);
message=uint8(message);

% determine size of cover object
Mc=size(cover_object,1);   %Height
Nc=size(cover_object,2);   %Width

% determine size of message object
Mm=size(message,1);        %Height
Nm=size(message,2);        %Width

% title the message object out to cover object size to generate watermark
for ii = 1:Mc
   for jj = 1:Nc
      watermark(ii,jj)=message(mod(ii,Mm)+1,mod(jj,Nm)+1);
   end
end

% now we set the lsb of cover_object(ii,jj) to the value of watermark(ii,jj)
watermarked_image=cover_object;
for ii = 1:Mc
   for jj = 1:Nc
      watermarked_image(ii,jj)=bitset(watermarked_image(ii,jj),1,watermark(ii,jj));
   end
end

% write the watermarked image out to a file
imwrite(watermarked_image,'lsb_watermarked.bmp','bmp');
```

```
% display processing time
elapsed_time=cputime-start_time,

% calculate the PSNR
psnr=psnr(cover_object,watermarked_image,Mc,Nc),

% display watermarked image
figure(1)
subplot(2,2,1)
imshow(cover_object,[])
title('original  image')
subplot(2,2,2)
imshow(message,[])
title('watermark')
subplot(2,2,3)
imshow(watermarked_image,[])
title('Watermarked Image')

% read in watermarked image
file_name='lsb_watermarked.bmp';
%file_name='_lena_std_bw.bmp';
watermarked_image=imread(file_name);

% determine size of watermarked image
Mw=size(watermarked_image,1);   %Height
Nw=size(watermarked_image,2);   %Width

% use lsb of watermarked image to recover watermark
for ii = 1:Mw
   for jj = 1:Nw
      watermark(ii,jj)=bitget(watermarked_image(ii,jj),1);
   end
end

% scale the recovered watermark
watermark=2*double(watermark);

% display processing time
elapsed_time=cputime-start_time,

subplot(2,2,3)
imshow(watermarked_image,[])
title('Watermarked Image')
subplot(2,2,4)
imshow(watermark,[])
title('Recovered Watermark')
```

```
imwrite(watermark,'rec.bmp','bmp');
O=imnoise(watermark,'salt & pepper',0.3);
figure(2);imshow(O);title('recovered watermark with noise')
%-------------------------------------------------------------%
```



```
%----- add noise "gaussian" to the watermarked image------------

figure(3)
subplot(2,2,1), imshow(watermarked_image);
title('Watermarked Image')
J1 = imnoise(watermarked_image,'gaussian',0,0.01);
J2 = imnoise(watermarked_image,'gaussian');
J3 = imnoise(watermarked_image,'gaussian',0,0.1);
J11 = imnoise(watermark,'gaussian',0,0.1)

subplot(2,2,2), imshow(J1);
title('Gaussian m=0,s=0.01')
subplot(2,2,3), imshow(J2);
title('Gaussian xoris mesi timi kai typiki apoklisi')
subplot(2,2,4), imshow(J3);
title('Gaussian m=0,s=0.1')
figure(4)
subplot(1,2,1),imshow(watermark);
title('Recover watermark');
subplot(1,2,2),imshow(J11);
title('Recover watermark with Gaussian m=0,s=0.1')

%-------------------------------------------------------------%
%-------add noise "salt and pepper" to the watermarked image------
J4 = imnoise(watermarked_image,'salt & pepper');
J5 = imnoise(watermarked_image,'salt & pepper',0.05);
J6 = imnoise(watermarked_image,'salt & pepper',0.1);
J44 = imnoise(watermark,'salt & pepper',0.1)
figure(5)
subplot(2,2,1), imshow(watermarked_image);
title('Watermarked Image')
subplot(2,2,2), imshow(J4);
title('salt&pepper')
subplot(2,2,3), imshow(J5);
title('salt&pepper D=0.005')
subplot(2,2,4), imshow(J6);
title('salt&pepper D=0.01')

figure(6)
subplot(1,2,1),imshow(watermark);
title('Recover watermark');
subplot(1,2,2),imshow(J44);
title('Recover watermark with "salt and pepper" D=0.01')
```

```
%-------------------------------------------------------------%
%-----------------------add edge filtering----------------------
BW1 = edge(watermarked_image,'prewitt');            %βρίσκει τις ακμές της εικόνας
χρησιμοποιώντας το φίλτρο prewitt
```



```
BW2 = edge(watermarked_image,'sobel');              %βρίσκει τις ακμές της εικόνας χρησιμοποιώντας
το φίλτρο sobel
BW3 = edge(watermarked_image,'canny');              %βρίσκει τις ακμές της εικόνας
χρησιμοποιώντας το φίλτρο canny
BW4 = edge(watermark,'canny');

figure(7),
subplot(2,2,1), imshow(watermarked_image);
title('Watermarked Image')
subplot(2,2,2), imshow(BW1);
title('prewitt filter')
subplot(2,2,3), imshow(BW2);
title('sobel filter')
subplot(2,2,4), imshow(BW3);
title('canny filter')
figure(8)
subplot(1,2,1),imshow(watermark);
title('Recover watermark');
subplot(1,2,2),imshow(BW4);
title('Recover watermark with canny filter');
%-------------------------------------------------------------%
%-------------average filtering---------------------------------
J = imnoise(watermarked_image,'salt & pepper',0.3);
        % denoising
H1 = fspecial('average',[5 5]);
K1 = imfilter(J,H1);
H2 = fspecial('average',[5 5]);
K2 = imfilter(O,H2);
figure(9)
subplot(2,2,1), imshow(watermarked_image);
title('Watermarked Image')
subplot(2,2,2),imshow(J);
title('with salt&pepper noise')
subplot(2,2,3), imshow(K1);
title('average filter')
subplot(2,2,4), imshow(imabsdiff(watermarked_image,K1))
title('differences watermarked image+average fillter')
figure(10)
subplot(1,2,1), imshow(O);
title('Recover Watermark with noise')
```

```
subplot(1,2,2), imshow(imabsdiff(O,K2))
title('differences recover watermark+average fillter')
%-------------------------------------------------------------%
%-----------------median filtering----------------------------
L = imnoise(watermarked_image,'salt & pepper',0.3);
L1 = medfilt2(watermarked_image,[5 5]);
L2 = medfilt2(O,[5 5]);
```



```
figure(11)
subplot(2,2,1), imshow(watermarked_image);
title('Watermarked Image')
subplot(2,2,2),imshow(L);
title('with salt&pepper noise')
subplot(2,2,3), imshow(L1);
title('median filter')
subplot(2,2,4), imshow(imabsdiff(watermarked_image,L1))
title('differences watermarked image+median fillter')
figure(12)
subplot(1,2,1), imshow(O);
title('Recover Watermark with noise')
subplot(1,2,2), imshow(imabsdiff(O,L2))
title('differences Recover watermark+median fillter')
%-------------------------------------------------------------%
%----------------------min/max filtering---------------------%

A = ordfilt2(watermarked_image,1,ones(5,5));
B = ordfilt2(watermarked_image,25,ones(5,5));
AA=  ordfilt2(watermark,1,ones(5,5));
BB = ordfilt2(watermark,25,ones(5,5));
figure(13)
subplot(2,2,1),imshow(watermarked_image);
title('Watermarked Image')
subplot(2,2,2),imshow(A);
title('filtro elaxistou')
subplot(2,2,3),imshow(B);
title('filtro megistou')
figure(14)
subplot(2,2,1),imshow(watermark);
title('Recover Watermark')
subplot(2,2,2),imshow(AA);
title('filtro elaxistou')
subplot(2,2,3),imshow(BB);
title('filtro megistou')
%-------------------------------------------------------------%
%---------------histogram equalization--------------------------%
```

```
figure(15)
subplot(2,2,1),imshow(watermarked_image);
title('Watermarked Image')
subplot(2,2,2),imhist(watermarked_image);
title('histogram')
C=histeq(watermarked_image);
subplot(2,2,3),imshow(C);
title('equalization')
subplot(2,2,4), imhist(C);
title('equalization histogram')
figure(16)
imhist(watermarked_image);
hold on
```



```
imhist(C);
title('sygkrisi arxikou me eksisoropimenou istogrammatos')
%-------------------------------------------------------------%
%------------------------Rotation-----------------------------%
D=imrotate(watermarked_image,45,'bilinear');
figure(17)
subplot(1,2,1),imshow(watermarked_image);
title('Watermarked Image')
subplot(1,2,2),imshow(D);
title('Rotated Watermarked Image')
DD=imrotate(watermark,45,'bilinear');
figure(18)
subplot(1,2,1),imshow(watermark);
title('Recover Watermark')
subplot(1,2,2),imshow(DD);
title('Rotated Recovered Watermark')
%-------------------------------------------------------------%
%-------------------------scaling-----------------------------%
F=imresize(watermarked_image,[256 256]);
G=imresize(O,[256 256]);
figure(19)
subplot(2,2,1),imshow(watermarked_image);
title('Watermarked Image')
subplot(2,2,2),imshow(F);
title('Resized Watermarked Image')
subplot(2,2,3),imshow(O);
title('Recovery Watermark with noise')
subplot(2,2,4),imshow(G);
title('Resized Recovery Watermark')
%-------------------------------------------------------------%
%------------------------cropping-----------------------------%
N = imcrop(watermarked_image,[60 40 225 300]);
figure(20)
subplot(2,2,1),imshow(watermarked_image);
```

```
title('Watermarked Image')
subplot(2,2,2),imshow(N);
title('Cropped Watermarked Image')
subplot(2,2,3),imshow(O);
title('Recovered Watermark with noise')
 % determine size of watermarked image
Mw=size(N,1);   %Height
Nw=size(N,2);   %Width

% use lsb of watermarked image to recover watermark
for ii = 1:Mw
   for jj = 1:Nw
      watermark(ii,jj)=bitget(N(ii,jj),1);
   end
end
```



```
 % scale the recovered watermark
watermark=2*double(watermark);
subplot(2,2,4), imshow(imabsdiff(watermark,O))
title('Cropped Recovered Watermark')
%-----------------------------------------------------------------%
%-------------------------metasximatismoi-----------------------%
%-----------------------DFT---------------------------------%
R=double(watermarked_image);
figure(21);
subplot(2,2,1)
imshow(R,'InitialMagnification','fit');
title('(a) Arxiki eikona')
image_fft=fft2(R);
subplot(2,2,2),
surf(abs(image_fft));
title('(b) Platos fasmatos')
imageshifted=fftshift(R);
subplot(2,2,3),
surf(imageshifted)
title('(c) Metatopisi eikonas')
imagefft=fft2(imageshifted);
subplot(2,2,4),
surf(abs(imagefft))
title('(d) Platos fasmatos metatopismenis eikonas')
shiftedimagefft=fftshift(imagefft);
figure(22);surf(abs(shiftedimagefft))
title('(e) Metatopisi fasmatos');
figure(23);
imshow(abs(shiftedimagefft), [0 255],'InitialMagnification','fit');
imagefft=fftshift(imageshifted);
```

```
colormap(gray); colorbar
title('(f) Teliko metatopismeno fasma me ti morfi eikonas')
%-------------------------------------------------------------%
%-------------------------DCT---------------------------------%
T=double(watermarked_image);
[M, N]=size (T)
TT=T(1:60, 1:60);
figure(24);
subplot(2,1,1)
imshow(TT, [0, 255]);
U=dct2(TT);
U2=dct2(T);
%UU2=U2(1:193, 1:152);       %------entoli gia antistrofi----
%InvUU2=idct2(UU2);          %-------entoli gia antistrofi------
imshow(abs(U2),[0 255]);
colormap(hot(64));
title('(1) Fasma tou 2D-DCT')
colorbar;
subplot(2,1,2)
```



```
surf(U)
colormap(jet(64))
title('(2)Trisdiastati apeikonisi tou fasmatos')
%subplot(2,2,4)             %----------entoli gia antistrofi-------
%imshow(InvUU2,[0, 255]);    %-------entoli gia antistrofi----
%-------------------------------------------------------------%
%-----------------------JPEG me diaforous deiktes----------------------%

imwrite(watermarked_image,'lsb_watermarked.jpg','Quality',100);
imwrite(watermarked_image,'lsb_watermarked.jpg','Quality',75);
imwrite(watermarked_image,'lsb_watermarked.jpg','Quality',50);
imwrite(watermarked_image,'lsb_watermarked.jpg','Quality',25);

imwrite(watermark,'rec.jpg','Quality',100);
imwrite(watermark,'rec.jpg','Quality',75);
imwrite(watermark,'rec.jpg','Quality',50);
imwrite(watermark,'rec.jpg','Quality',25);

V1=imread('_lena_std_bw.jpg');
V2=imread('_lena_std_bw.jpg');
V3=imread('_lena_std_bw.jpg');
V4=imread('_lena_std_bw.jpg');

W1=imread('rec.jpg');
W2=imread('rec.jpg');
W3=imread('rec.jpg');
W4=imread('rec.jpg');
```

```
W1=imnoise(W1,'salt & pepper',0.3);
W2=imnoise(W2,'salt & pepper',0.3);
W3=imnoise(W3,'salt & pepper',0.3);
W4=imnoise(W4,'salt & pepper',0.3);

figure(25);subplot(1,2,1);imshow(watermarked_image);
title('Watermarked Image')
subplot(1,2,2);imshow(V1);title('watermarked image JPEG 100')
figure(26);subplot(1,2,1);imshow(watermarked_image);
title('Watermarked Image')
subplot(1,2,2);imshow(V2);title('watermarked image JPEG 75')
figure(27);subplot(1,2,1);imshow(watermarked_image);
title('Watermarked Image')
subplot(1,2,2);imshow(V3);title('watermarked image JPEG 50')
figure(28);subplot(1,2,1);imshow(watermarked_image);
title('Watermarked Image')
subplot(1,2,2);imshow(V4);title('watermarked image JPEG 25')

figure(29);subplot(1,2,1);imshow(watermark);title('Recover watermark')
subplot(1,2,2);imshow(W1);title('Recover Watermark with JPEG 100')
figure(30);subplot(1,2,1);imshow(watermark);title('Recover watermark')
subplot(1,2,2);imshow(W2);title('Recover Watermark with JPEG 75')
```



```
figure(31);subplot(1,2,1);imshow(watermark);title('Recover watermark')
subplot(1,2,2);imshow(W3);title('Recover Watermark with JPEG 50')
figure(32);subplot(1,2,1);imshow(watermark);title('Recover watermark')
subplot(1,2,2);imshow(W4);title('Recover Watermark with JPEG 25')
```