Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Στεγανογραφία και συμπιεσμένη αίσθηση**
Ονοματεπώνυμο Φοιτητή	**Γεώργιος Τσακαμής**
Πατρώνυμο	**Ιωάννης**
Αριθμός Μητρώου	**ΜΠΣΠ/ 09027**
Επιβλέπων	**Νικόλαος Αλεξανδρής, Καθηγητής**

Ημερομηνία Παράδοσης **Ιανουάριος 2011**

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Τριμελής Εξεταστική Επιτροπή

Νικόλαος Αλεξανδρής Καθηγητής	Γεώργιος Τσιχριντζής Καθηγητής	Παναγιώτης Κοτζανικολάου Λέκτορας

Ευχαριστώ θερμά τον Δρ. κ. Πατσάκη Κωνσταντίνο για την σημαντική βοήθεια και την καθοδήγησή του καθ' όλη την διάρκεια της συγγραφής της παρούσας μεταπτυχιακής διατριβής και την οικογένεια μου για την πολύτιμη συμπαράσταση της.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Περιεχόμενα

Λίστα Εικόνων

Λίστα Πινάκων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Περίληψη

Η στεγανογραφία είναι ένας νέος όρος που χρησιμοποιείται για την πραγματοποίηση μιας μυστικής επικοινωνίας. Κύριος σκοπός της είναι η ενσωμάτωση μηνυμάτων μέσα σε αντικείμενα χωρίς αυτό να γίνεται αντιληπτό από τρίτους. Ωστόσο παρ' όλες τις ομοιότητες που έχει με την κρυπτογραφία και την υδατογράφηση εντούτοις διαφέρει πολύ. Η στεγανογραφία σε ψηφιακά μέσα είναι μια νέα επιστήμη η οποία αναπτύσσετε ταχύτατα χωρίς βέβαια να λείπουν και τα διάφορα προβλήματα.

Η παρούσα μεταπτυχιακή διατριβή χωρίζεται σε δύο κύρια μέρη. Στο πρώτο μέρος πραγματοποιείται μια αναλυτική παρουσίαση του όρου της στεγανογραφίας και των διαφόρων κατηγοριών και τύπων που υπάρχουν γύρω από αυτή, ενώ στο δεύτερο μέρος αναπτύσσουμε μια νέα μέθοδος ανίχνευσης χρήσης στεγανογραφίας σε μια εικόνα. Η μέθοδος αυτή βασίζεται στην τεχνική της συμπιεσμένης δειγματοληψία. Σκοπός της μεθόδου αυτής είναι να βρούμε τον αριθμό των ίδιων εικονοστοιχείων μεταξύ της αρχικής εικόνας και της στεγο-εικόνας.

Λέξεις κλειδιά: Στεγανογραφία, στεγανάλυση, στεγο-εικόνα, κατηγορίες στεγανογραφίας, τύποι στεγανογραφίας, τύποι πρωτοκόλλων στεγανογραφίας, στεγανογραφικό κανάλι, συμπιεσμένη δειγματοληψίας.

Abstract

Steganography is another term for covert communication. The main goal of steganography is to hide messages in inconspicuous objects without anybody find them. Although steganography has many similarities with cryptography and watermarking however, it differs a lot. Steganography in digital media is a new science which is growing rapidly, however lots of open issues occur.

This postgraduate thesis is separated in two main parts. In the first part is realized a analytic presentation of term steganography and various categories and types that exist, while in the second part we develop a new method of detection of use steganography in a picture. This method is based on the technique compressive sampling. Aim of this method is to find the number of same pixels between the initial picture and the stego-picture.

Key words: Steganography, steganalysis, stego-picture, steganography categories, steganography types, protocol type of steganography, steganography channel, compressive sensing.

Εισαγωγή

Το 1^{ο} Κεφάλαιο παρουσιάζει την ιστορική εξέλιξη και χρήση της στεγανογραφίας από τα παλιά χρόνια μέχρι και το σήμερα ενώ παράλληλα περιέχει τον ορισμό και τις ιδιότητες της. Επιπλέον κάνει μια σύγκριση της στεγανογραφίας με την κρυπτογραφία και την υδατογράφηση, ενώ τέλος αναφέρεται στην στεγανάλυση και την ασφάλεια της στεγανογραφίας.

Το 2^{ο} Κεφάλαιο εμβαθύνει περισσότερο στην στεγανογραφία παρουσιάζοντας αναλυτικά τις τεχνικές, τις κατηγορίες, και τους τύπους πρωτοκόλλων που ισχύουν. Επίσης στο κεφάλαιο αυτό υπάρχουν αλγόριθμοι εφαρμογής της στεγανογραφίας αλλά και εικόνες για την καλύτερη κατανόηση τους.

Το 3^{ο} Κεφάλαιο κάνει μια σύντομη αναφορά στο στεγανογραφικό κανάλι παρουσιάζοντας αρχές για την δημιουργία στεγανογραφικών μεθόδων με σκοπό την καλύτερη χρησιμοποίηση του καναλιού επικοινωνίας μεταξύ του αποστολέα και του παραλήπτη του μηνύματος.

Το 4^{ο} Κεφάλαιο μπορεί να χαρακτηριστεί και ως εισαγωγή του κεφαλαίου 5 μιας και αναφέρεται στην συμπιεσμένη δειγματοληψία μια τεχνική πολύ σημαντική για την λήψη και ανάλυση εικόνων. Στο κεφάλαιο αυτό παρουσιάζεται τόσο το πρόβλημα της συμπιεσμένης δειγματοληψίας όσο και οι λύσεις τις. Επιπλέον γίνεται μια αναφορά στις βασικές αρχές που διέπουν την συμπιεσμένη δειγματοληψία και στα ανοιχτά προβλήματα που ακόμα υπάρχουν.

Στο 5^{ο} Κεφάλαιο παρουσιάζεται το πείραμα που πραγματοποιήσαμε με σκοπό την εύρεση του ποσοστού των σωστών εικονοστοιχείων μεταξύ της αρχικής και της τελικής εικόνας σε δείγμα 80 εικόνων. Επιπλέον αναλύουμε τον κώδικα Matlab που χρησιμοποιήσαμε και τον αλγόριθμο BD3M.

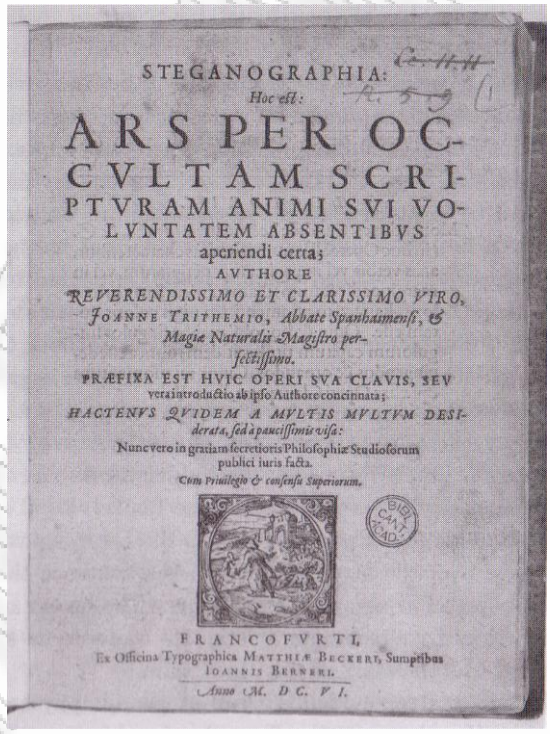
Τέλος στο 6^{ο} Κεφάλαιο αναφέρονται όλα τα γενικά συμπεράσματα που προέκυψαν από αυτή την μεταπτυχιακή διατριβή.

Κεφάλαιο 1

Στεγανογραφία

1.1 Ιστορική αναδρομή της στεγανογραφίας

Η λέξη στεγανογραφία προέρχεται από δύο συστατικά της Ελληνικής γλώσσας. Την λέξη «στεγανό» η οποία σημαίνει ‘‘καλυμμένο’’ και τη λέξη «γραφή» η οποία σημαίνει ‘‘κείμενο ή τέχνη’’. Με άλλα λόγια η στεγανογραφία είναι η τέχνη της απόκρυψης επικοινωνίας κατά την οποία η ύπαρξη ενός μηνύματος είναι κρυφή. Ο όρος στεγανογραφία χρησιμοποιήθηκε για πρώτη φορά από τον Johannes Trithemius στην τριλογία του με τίτλο «Πολυγραφία» και στο βιβλίο του «Στεγανογραφία». Ενώ τα δύο πρώτα κομμάτια από την τριλογία περιέγραφαν αρχαίες μεθόδους για κρυπτογραφία μηνυμάτων, ο τρίτος τόμος αναφερόταν σε μυστικές δυνάμεις, μαύρη μαγεία και μεθόδου επικοινωνίας με πνεύματα. Ο τρίτος αυτός τόμος παρουσιάστηκε το 1606 στην Φρανκφούρτη και το 1609 η Ρωμαιοκαθολική εκκλησία το χαρακτήρισε ως απαγορευμένο βιβλίο. Πολύ σύντομα όμως οι επιστήμονες εκείνης της περιόδου άρχισαν να υποπτεύονται ότι το βιβλίο αυτό ήταν ένας κώδικας και προσπάθησαν να λύσουν το μυστήριο. Στα τέλη του 1996 και 1998 δύο ανεξάρτητοι ερευνητές κατάφεραν ύστερα από μεγάλη προσπάθεια να αποκωδικοποιήσουν τα κρυμμένα μηνύματα που ήταν γραμμένα μέσα στο βιβλίο [1]. Ωστόσο το νόημα των κρυμμένων μηνυμάτων ήταν κοινότυπο χωρίς κάποιο άμεσο ενδιαφέρον [2].


STEGANOGRAPHIA:
Hoc eſt:
ARS PER OC-
CVLTAM SCRI-
PTVRAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanhaimenſi, &
Magiæ Naturalis Magiſtro per-
fectiſſimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera introductio ab ipſo Authore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DESI-
derata, ſed à paucissimis visa:
Nunc vero in gratiam ſecretioris Philoſophiæ Studioſorum
publici iuris facta.
Cum Priuilegio & conſenſu Superiorum.
FRANCOFVRTI,
Ex Officina Typographica MATTHIÆ BECKERI, Sumptibus
IOANNIS BERNERI.
Anno M. D C. V I.

Εικόνα 1.1 Εξώφυλλο του βιβλίου «Στεγανογραφία» του Johannes Trithemius.
Πηγή: (Twilit Grotto: Archives of Western Esoterica)

Το πρώτο καταγεγραμμένο στοιχείο το οποίο αναφέρεται στην χρήση της στεγανογραφίας με σκοπό την αποστολή μηνυμάτων οφείλεται στον Ηρόδοτο, ο οποίος στο βιβλίο του περιγράφει την ιστορία ενός σκλάβου που στάλθηκε από τον αφέντη του στην πόλη Μίλητος με ένα κρυμμένο μήνυμα ζωγραφισμένο πάνω στο κρανίο του. Σύμφωνα με τα ιστορικά

στοιχεία αυτό το μήνυμα προοριζόταν για τον αντιβασιλέα Αρισταγόρα και το οποίο προέτρεπε να ξεκινήσει πόλεμο ενάντια στο βασιλιά της Περσίας [3].

Ένα ακόμα περιστατικό που καταγράφει ο Ηρόδοτος στο βιβλίο του και αναφέρεται στην στεγανογραφία είναι η ιστορία του Δημάρατου. Σύμφωνα λοιπόν με την ιστορία στην αρχαία Ελλάδα τα κείμενα γράφονταν σε πίνακες καλυμμένους με κερί. Ο Δημάρατος ήθελε να ειδοποιήσει τη Σπάρτη ότι ο Ξέρξης προτίθετο να εισβάλει στην Ελλάδα. Για να αποφύγει την κλοπή του μηνύματος έγραψε το μήνυμά του σε ξύλινη πινακίδα, αφού έξυσε το κερί που αυτή είχε και την οποία μετά κάλυψε πάλι με κερί. Οι πινακίδες φαίνονταν λευκές και αχρησιμοποίητες και με αυτό το τρόπο πέρασαν κάθε έλεγχο [3].

Το κρύψιμο μηνυμάτων μέσα σε κείμενα λέγεται γλωσσολογική στεγανογραφία. Η γλωσσολογική στεγανογραφία ήταν μια από τις πιο διαδεδομένες στεγανογραφικές μεθόδους. Για να ενσωματώσουν μια μοναδική υπογραφή στις δουλειές τους, πολλοί ποιητές κρυπτογραφούσαν μυστικά κείμενα σαν αρχικά γραμμάτων προτάσεων. Ένα από τα καλύτερα γνωστά παραδείγματα είναι το «Amorosa uisione» του Giovanni Boccacio. Ο Boccacio κρυπτογράφησε τρεις σονέτες μέσα στα αρχικά γράμματα του πρώτου στοίχου κάθε τρίστιχου από άλλα ποιήματα. Αυτή η γλωσσολογική στεγανογραφία πρωτοεμφανίστηκε στην Κίνα και επινοήθηκε ξανά από τον Cardan. Τα γράμματα του κρυφού μηνύματος διαμορφώνουν ένα τυχαίο σχέδιο που μπορεί να προσεγγιστεί απλά με την τοποθέτηση μιας μάσκας πάνω στο κείμενο. Η μάσκα παίζει τον ρόλο ενός μυστικού «στεγανό» κλειδιού το οποίο πρέπει να μοιράζεται μεταξύ των ατόμων που επικοινωνούν [2].

Ο Francis Bacon ήταν αυτός που περιέγραψε έναν πρόδρομο σχέδιο της σημερινής μοντέρνας στεγανογραφίας. Ο Bacon συνειδητοποίησε ότι χρησιμοποιώντας πλάγια ή κανονική γραμματοσειρά, κάποιος θα μπορούσε να κωδικοποιήσει τη δυαδική αντιπροσώπευση των γραμμάτων στις εργασίες του. Πέντε γράμματα από το αντικείμενο που ήθελε να κρύψει μπορούσε να κρατήσει πέντε bits και ως εκ τούτου ένα γράμμα της αλφαβήτου. Η ασυνέπεια που επικρατούσε στην τυπογραφία τον 16ο αιώνα έκαναν αυτή την μέθοδο σχεδόν απαρατήρητη [2].

Ωστόσο αυτός ο οποίος περιέγραψε την πιο μοντέρνα έκδοση της στεγανογραφία εκείνης της εποχής (16ο-17ο αιώνα) ήταν ο Brassil. Η μέθοδος του ήταν απλή: τα δεδομένα που ήθελε, τα έκρυβε σε αρχεία κειμένων, μετατοπίζοντας ελαφρώς τις γραμμές του κειμένου λίγο πάνω ή λίγο κάτω κατά το 1/300 της ίντσας. Με αυτό τον τρόπο τα μηνύματα δεν γινόντουσαν αντιληπτά και ο μόνος τρόπος για να εξάγει κανείς το μήνυμα ήταν ή να εκτύπωνε τα αρχεία ή να τα φωτοτυπούσε [4].

Το 1857 ο Brewster πρότεινε μια πολύ ενδιαφέρουσα τεχνική η οποία και χρησιμοποιήθηκε πάρα πολύ σε πολλούς από τους πολέμους του 19ου και 20ου αιώνα. Η ιδέα ήταν να συρρικνωθεί το κείμενο σε τέτοιο βαθμό, έτσι ώστε να αρχίζει να μοιάζει με κόκκο βρωμιάς αλλά ταυτόχρονα να μπορεί να διαβαστεί κάτω από υψηλή μεγέθυνση. Τα τεχνολογικά εμπόδια αυτής της μεθόδου ξεπεράστηκαν γρήγορα χάρη στο Γάλλο φωτογράφο Dragon, ο οποίος ανέπτυξε την τεχνολογία της σμίκρυνσης κειμένου σε διαστάσεις μικροσκοπίου. Κατά την διάρκεια του Πρώτου Παγκοσμίου Πολέμου, οι Γερμανοί συνήθιζαν να χρησιμοποιούν τέτοια «μικροστίγματα» κρυμμένα σε γωνίες από καρτ-ποστάλ. Το πρώτο καταγεγραμμένο περιστατικό καταγράφηκε το 1941 όταν ένας γερμανός πράκτορας μετέφερε τέτοια «μικροστίγματα» σε έναν δακτυλογραφημένο φάκελο. Τον 20ο αιώνα αυτά τα «μικροστίγματα» (microdots) επέτρεψαν τη διαβίβαση μεγάλων σε όγκο πληροφοριών συμπεριλαμβανομένων και διαφορών σχεδίων και φωτογραφιών [2].

Εικόνα 1.2 Αναπαράσταση ενός μικροστίγματος (microdot).

Πηγή: (http://www.scienceinafrica.co.za/2005/november/microdot.htm)

Ωστόσο η καλύτερη και πιο γνωστή μορφή στεγανογραφίας ήταν αυτή που χρησιμοποιούσε αόρατο μελάνι. Τα πρώτα αόρατα μελάνια ήταν από οργανικά υγρά όπως το γάλα, το ξίδι, τα ούρα, το αραιωμένο μέλι και η ζάχαρη. Τα μηνύματα τα οποία γραφόντουσαν με αυτό το μελάνι ήταν αόρατα όταν το χαρτί ήταν στεγνό. Για να δει κανείς τα μηνύματα έπρεπε να βάλει το χαρτί πάνω από ένα κερί. Με αυτό τον τρόπο τα υλικά αυτά θερμαίνονται και σκούραιναν με αποτέλεσμα να γίνονται ορατά από το ανθρώπινο μάτι. Με την ανάπτυξη της τεχνολογίας αυτής, αναπτύχθηκαν νέα περιπλοκότερα μελάνια ώστε να αντιδρούν μόνο σε συγκεκριμένες χημικές ουσίες [2].

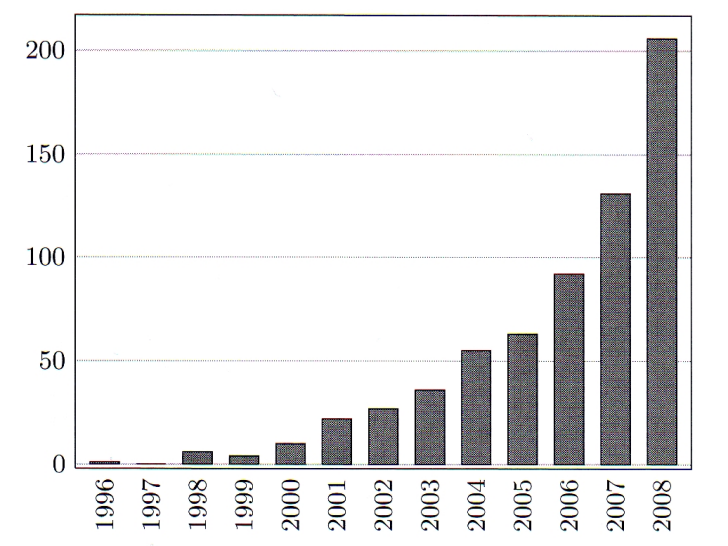
Το 1966 μια εφευρετική και αυτοσχέδια στεγανογραφική μέθοδος αναπτύχθηκε από έναν φυλακισμένο πολέμου τον Jeremiah Denton. Ο Jeremiah Denton αναγκάστηκε από τους Βιετναμέζους να μιλήσει μπροστά στη τηλεόραση, γνωρίζοντας ότι δεν μπορούσε να πει τίποτα επικριτικό για αυτούς που τον είχαν αιχμαλωτίσει. Έτσι ενώ μιλούσε ανοιγόκλεινε τα μάτια του με την μορφή του κώδικα Morse στέλνοντας έτσι την λέξη β-α-σ-α-ν-η-σ-τ-η-ρ-ι-α [5].

Το 1990 η ιστορία του «κώδικα κουρελού» (quilt code) ήρθε στη επιφάνεια από τα μέσα μετάδοσης εκείνης της εποχής. Πιο συγκεκριμένα ένα δίκτυο της εποχής εκείνης το ‘‘Undergroung Railroad’’ εμφανίστηκε με σκοπό να βοηθήσει τους μαύρους σκλάβους να δραπετεύσουν από τις Η.Π.Α. χρησιμοποιώντας κρυφές διαβάσεις και ασφαλή σπίτια. Το δίκτυο αυτό πληροφορούσε τους μαύρους σκλάβους πώς να δραπετεύσουν ζωγραφίζοντας πάνω σε κουρελούδες γεωμετρικά σχήμα. Αυτά τα γεωμετρικά σχήματα ουσιαστικά αποτελούσαν το χάρτη μέσω του οποίου θα δραπέτευαν. Ουσιαστικά εδώ παρατηρούμε μια άλλη μορφή στεγανογραφίας όπου τα μηνύματα κρυβόντουσαν κάτω από γεωμετρικά σχήματα. Ένα τέτοιο κώδικα κουρελού μπορούμε να δούμε στην παρακάτω εικόνα [2].

Εικόνα 1.3 Σύμβολο με δύο κρυπτογραφημένα μηνύματα.

Πηγή: (Owen Sound's Black History-Quilt Code)

Η πρόσφατη έκρηξη ενδιαφέροντος για την στεγανογραφία οφείλεται τόσο στην ξαφνική και διαδεδομένη χρήση ψηφιακών μέσων όσο και στην γρήγορη επέκταση του Διαδικτύου. Στις μέρες μας είναι κοινή πρακτική να μοιραζόμαστε φωτογραφίες, βίντεο και ήχους με τους γνωστούς και τους φίλους μας είτε μέσω του ηλεκτρονικού ταχυδρομείου είτε μέσω των κοινωνικών δικτύων που υπάρχουν (Facebook, MySpace κ. λ. π.). Αυτά τα αντικείμενα (φωτογραφίες, βίντεο, ήχος) παρέχουν ένα πολύ καλό περιβάλλον για απόκρυψη μυστικών μηνυμάτων. Αυτό το γεγονός οφείλεται κυρίως στο ότι τα ψηφιακά αυτά μέσα αποτελούνται από ένα μεγάλο πλήθος ανεξάρτητων δειγμάτων (π.χ. pixels) τα οποία μπορούν να αλλάξουν ελάχιστα με σκοπό να κρύψουν ένα μυστικό μήνυμα. Η αύξηση χρήσης της στεγανογραφίας φαίνεται και στον παρακάτω διάγραμμα το οποίο παρουσιάζει τον αριθμό των άρθρων που έχουν γραφτεί για την στεγανογραφία από το 1966 έως σήμερα.

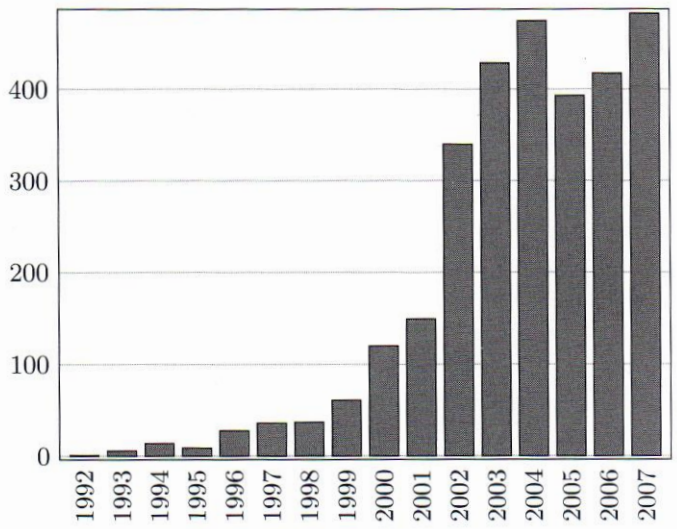


Εικόνα 1.4 Διάγραμμα παρουσίασης της αύξησης αριθμού άρθρων που αναφέρονται στην στεγανογραφία.

Πηγή: (Steganography in Digital media)

Στις μέρες μας, δεν είναι απαραίτητο για κάποιον να γίνει ειδικός στην στεγανογραφία μιας και υπάρχουν πολλά προγράμματα ελεύθερα στο Διαδίκτυο τα οποία παρέχουν λειτουργίες

στεγανογραφίας. Πολλά από αυτά τα λογισμικά (softwares) επικεντρώνονται πάνω στην ασφάλεια, στην ιδιωτικότητα και στην ανωνυμία προσφέροντας την δυνατότητα απόκρυψης κωδικοποιημένων μηνυμάτων σε εικόνες και μουσική. Παραδείγματα τέτοιων λογισμικών είναι το Steganos, Stealthencrupt, MP3Stego, GIFShuffle, JPSeek κ.α. Στο παρακάτω διάγραμμα παρατηρούμε την ραγδαία αύξηση στην ανάπτυξη τέτοιων λογισμικών.



Εικόνα 1.5 Διάγραμμα παρουσίασης αριθμού λογισμικών στην στεγανογραφία.
Πηγή: (Steganography in Digital media)

1.2 Ορισμός και ιδιότητες στεγανογραφίας

Επειδή η ηλεκτρονική επικοινωνία είναι ιδιαίτερα ευάλωτη στις μέρες μας, μιας και υπάρχουν πολλοί κακόβουλοι που προσπαθούν να υποκλέψουν διάφορες πληροφορίες, το θέμα της ασφάλειας και της ιδιωτικότητας πάνω στο τομέα της ηλεκτρονικής επικοινωνίας αποτελεί μείζον θέμα της σύγχρονης κοινωνίας.

Οι παραδοσιακές λύσεις χρησιμοποιούν την κρυπτογραφία, η οποία βασίζεται σε ένα ώριμο και καλά σχεδιασμένο πεδίο με αυστηρά μαθηματικά θεμέλια. Η ιδιωτικότητα επιτυγχάνεται μέσω της κρυπτογραφίας με την βοήθεια κλειδιών κρυπτογράφησης και αποκρυπτογράφησης. Πιο συγκεκριμένα, η κρυπτογραφία μετατρέπει τις ανταλλασσόμενες πληροφορίες σε μη αναγνώσιμες προς αυτούς που δεν διαθέτουν το κλειδί της αποκρυπτογράφησης. Ωστόσο όταν ένα κρυπτογραφημένο μήνυμα υποκλαπεί, παρ όλο που το περιεχόμενό του μηνύματος προστατεύεται, το γεγονός ότι δύο άτομα επικοινωνούν μυστικά αρχίζει και γίνεται εμφανές προς τρίτους.

Για την αποφυγή τέτοιων καταστάσεων χρησιμοποιούμε την στεγανογραφία με την βοήθεια της οποία κρύβουμε το μυστικό μήνυμα σε ένα άλλο αντικείμενο. Με αυτό τον τρόπο όταν κάποιος υποκλέψει το αντικείμενο που περιέχει το μυστικό μήνυμα το μόνο που θα δει είναι απλά ένα αντικείμενο (εικόνα, βίντεο μουσικό αρχείο) και δεν θα αντιληφθεί το μήνυμα το οποίο κρύβεται πίσω από αυτό το αντικείμενο.

Στην πραγματικότητα λοιπόν ο ακριβής όρος της στεγανογραφίας είναι ο εξής:

Στεγανογραφία είναι η τέχνη και η επιστήμη της απόκρυψης μηνυμάτων με τέτοιο τρόπο ώστε κανένας άλλος, εκτός από τον αποστολέα και τον προοριζόμενο παραλήπτη, δεν υποψιάζεται την ύπαρξη του κρυμμένου μηνύματος [7].

Κάθε στεγανογραφικό σύστημα αποτελείται από δύο βασικά συστατικά: τον αλγόριθμο ενσωμάτωσης και τον αλγόριθμο εξαγωγής. Ο αλγόριθμος ενσωμάτωσης δέχεται τρεις εισόδους: το μυστικό μήνυμα που θέλουμε να στείλουμε κατά την επικοινωνία μας με κάποιον άλλον, το διαμοιρασμένο μυστικό κλειδί με το οποίο ρυθμίζονται οι αλγόριθμοι ενσωμάτωσης

και εξαγωγής και το αντικείμενο το οποίο τροποποιείται για να ‘‘μεταφέρει’’ το μυστικό μήνυμα. Η έξοδος του αλγορίθμου ενσωμάτωσης ονομάζεται «στεγο-αντικείμενοο» (stego object). Όταν το στεγο-αντικείμενο μπαίνει σαν είσοδος στον αλγόριθμο εξαγωγής, τότε εξάγεται το μυστικό μήνυμα [2].

Η τεχνική της στεγανογραφίας διαθέτει πέντε βασικές ιδιότητες: την αντίληψη, το ωφέλιμο φορτίου, την ανθεκτικότητα, τη αντοχή και τη ευρωστία. Πιο αναλυτικά [6]:

- Η στεγανογραφία εκμεταλλεύεται την ανθρώπινη αντίληψη και αυτό επειδή η αίσθηση του κάθε ανθρώπου δεν είναι εκπαιδευμένη κατάλληλα έτσι ώστε να αντιλαμβάνεται κρυμμένες πληροφορίες που βρίσκονται ενσωματωμένες μέσα σε αρχεία.
- Το ωφέλιμο φορτίο αναφέρεται στην ποσότητα της πληροφορίας που μπορεί να κρυφτεί πίσω από ένα αντικείμενο. Είναι απολύτως λογικό ότι όταν θέλουμε να κρύψουμε ένα μεγάλο μήνυμα τότε θα χρειαστεί να το ενσωματώσουμε είτε πίσω από μια εικόνα με μεγάλο μέγεθος είτε πίσω από ένα μεγάλο βίντεο ή αρχείο ήχου.
- Όσον αφορά την ανθεκτικότητα αναφερόμαστε στην ικανότητα των ενσωματωμένων στοιχείων να παραμείνουν ανέπαφα, παρ όλο που υφίστανται μετασχηματισμό στο στεγο-αντικείμενο. Με άλλα λόγια το μήνυμα το οποίο έχουμε κρύψει μέσα στο αντικείμενο μας παραμένει το ίδιο κατά την εξαγωγή του.
- Επειδή κάποιοι κακόβουλοι θα προσπαθήσουν να φιλτράρουν και να καταστρέψουν κάθε πληροφορία ενσωματωμένη σε εικόνες, γι’ αυτό το λόγο η ευρωστία είναι ζωτικής σημασίας για προστασία της πνευματικής ιδιοκτησίας του μηνύματος.
- Η αντοχή αναφέρεται στην δυσκολία για έναν εισβολέα να μεταβάλει ή να σφυρηλατήσει ένα μήνυμα τη στιγμή που θα έχει ενσωματωθεί σε ένα στεγο-αντικείμενο. Με αυτή την ιδιότητα η στεγανογραφία προσφέρει πλήρη ασφάλεια στο κρυφό μήνυμα.

1.3. Παράδειγμα στεγανογραφίας

Μια γυναίκα με το όνομα Alice έστειλε το ακόλουθο e-mail στο φίλο της Bob, με τον οποίο μοιράζονται το ίδιο πάθος στην αστρολογία:

My friend Bob,

until yesterday I was using binoculars for stargazing. Today, I decided to try my new telescope. The galaxies in Leo and Ursa Major were unbelievable! Next, I plan to check out some nebulas and then prepare to take a few snapshots of the new comet. Although I am satisfied with the telescope, I think I need to purchase light pollution filters to block the xenon lights from a nearby highway to improve the quality of my pictures.

Cheers,

Alice

Με μια πρώτη ματιά αυτό το γράμμα φαίνεται να είναι μια απλή συζήτηση ανάμεσα σε δύο λάτρεις της αστρονομίας. Η Alice δείχνει να είναι ιδιαίτερα ενθουσιασμένη με το καινούργιο της τηλεσκόπιο και μοιράζεται αυτόν τον ενθουσιασμό της με τον φίλο της, τον Bob. Στην πραγματικότητα όμως η Alice είναι κατάσκοπος και ο Bob είναι ο ανώτερός της, ο οποίος περιμένει σημαντικά νέα από την μυστική πράκτορά του. Επιθυμώντας να μην τραβήξουν την προσοχή τρίτων, αποφασίζουν να μην χρησιμοποιήσουν την μέθοδο της κρυπτογραφίας για να μιλήσουν με μυστικότητα. Έτσι έχουν συμφωνήσει από την αρχή να χρησιμοποιήσουν την στεγανογραφία.

Όταν λοιπόν ο Bob λάβει το μήνυμα από την Alice αμέσως υποπτεύεται ότι η Alice χρησιμοποιεί την στεγανογραφία για να του στείλει κάποιο μήνυμα. Έτσι ο Bob αποφασίζει να ακολουθήσει το προσυμφωνημένο πρωτόκολλο. Καταγράφει όλα τα αρχικά γράμματα της κάθε λέξης από το e-mail που έχει στείλει η Alice με αποτέλεσμα να πάρει την ακόλουθη σειρά γραμμάτων:

mfbuyiwubfstidttmnttgilaumwunitptcosnatpttafsotncaiaswttitintplpftbtxlfanhtitqompca

Στην συνέχεια ο Bob γράφει την δεκαδική επέκταση του π :

π = 3.141592653689793...

και διαβάζει το μήνυμα σύμφωνα με την ακολουθία γραμμάτων που εξήγαγε προηγουμένως. Έτσι αρχικά παίρνει το τρίτο γράμμα που είναι το b στην συνέχεια το πρώτο γράμμα που είναι το u στην συνέχεια το τέταρτο γράμμα που είναι το u κ. λ. π.

Έτσι προκύπτει το μήνυμα

buubdlupnpsspx

Τέλος, ο Bob αντικαθιστά κάθε γράμμα με το γράμμα εκείνο της αλφαβήτου που προηγείται. Έτσι το αληθινό μήνυμα που έστειλε η Alice στο Bob είναι:

attack tomorrow

Παρατηρώντας το παράδειγμα που αναφέραμε προηγουμένως η Alice για να κρυπτογραφήσει το μήνυμά της θα έπρεπε πρώτα να αντιστοιχίσει το κάθε γράμμα του μηνύματος με το αμέσως επόμενο της αλφαβήτου. Η Alice εδώ είχε την δυνατότητα να χρησιμοποιήσει άλλο αλγόριθμο και να αντιστοιχεί το κάθε γράμμα της αλφαβήτου με το 2^{o} στη σειρά ή με το προηγούμενό του κ. λ. π. Στην συνέχεια η Alice έπρεπε να γράψει ένα άσχετο αλλά με νόημα κείμενο ενώ ταυτόχρονα θα έπρεπε να είναι σίγουρη ότι οι λέξεις που τοποθετεί μέσα στο γράμμα ακολουθούν τα ψηφία του π .

Θα πρέπει εδώ να τονίσουμε ότι αντί η Alice και ο Bob να χρησιμοποιήσουν την δεκαδική επέκταση του π θα μπορούσαν να είχαν συμφωνήσει από την αρχή σε μια ακέραια ακολουθία, όπως για παράδειγμα σε αυτή που προκύπτει από μια γεννήτρια ψευδοτυχαίων αριθμών και την οποία θα την είχε στείλει ο ένας στον άλλο με ένα κοινό κλειδί. Η πληροφορία αυτή, που αναφέρεται στο πως θα τοποθετηθούν τα γράμματα του μηνύματος ονομάζεται στεγανογραφικό κλειδί (stego key). Όταν κάποιος δεν γνωρίζει το κλειδί αυτό, είναι πολύ δύσκολο τόσο να διαβάσει το μήνυμα όσο και να ανακαλύψει ότι το αρχικό γράμμα περιέχει μέσα του ένα μήνυμα.

Τέλος, θα πρέπει να αναφέρουμε ότι στην περίπτωση που κάποιος ήθελε να στείλει ένα πιο μεγάλο μήνυμα τότε αυτό θα ήταν πάρα πολύ δύσκολο και μη πρακτικό. Έτσι αντί να κρύβουμε μηνύματα μέσα σε e-mails θα ήταν χρησιμότερο να χρησιμοποιήσουμε εικόνες ή βίντεο και να τα στέλνουμε ως αρχεία. Αυτό είναι και πιο εύκολο και πιο πρακτικό [14].

1.4 Σύγχρονη στεγανογραφία

Ένας επιπλέον λόγος, ο οποίος βοήθησε στην ανάπτυξη και την χρήση της στεγανογραφίας ήταν ότι παρείχε μια εναλλακτική τεχνική για την αποστολή κρυφών μηνυμάτων σε περιοχές όπου η χρήση της κρυπτογραφία είναι απαγορευμένη. Μια ενδιαφέρουσα τεκμηρίωση για την χρήση της στεγανογραφίας παρουσιάστηκε το 2001 στο 4^{o} International Workshop on Information Hiding. Σε αυτό το σεμινάριο παρουσιάστηκε η ιστορία δύο ατόμων, τα οποία ανέπτυξαν ένα σχέδιο στεγανογραφίας με σκοπό να στέλνουν κρυφά μηνύματα ενσωματωμένα μέσα σε μη συμπιεσμένες ψηφιακές εικόνες. Αυτήν την τεχνική την χρησιμοποιούσαν για αρκετά χρόνια μιας και ο ένας από τους δύο κατοικούσε σε περιοχή όπου η χρήση της κρυπτογραφίας ήταν απαγορευμένη [8].

Στις αρχές του 1980, ο Simmons περιέγραψε ενδιαφέρουσες πολιτικές επιπτώσεις μιας ενδεχόμενης πιθανότητας αποστολής δεδομένων μέσω ενός κρυφού καναλιού. Σύμφωνα με την αφοπλιστική συνθήκη SALT, οι Ηνωμένες Πολιτείες της Αμερικής και η τότε Σοβιετική Ένωση συμφώνησαν να εξοπλίσουν τις πυρηνικές εγκαταστάσεις τους με αισθητήρες, οι οποίοι θα μπορούσαν να ενημερώσουν την άλλη χώρα για τον αριθμό των πυραύλων αλλά όχι για άλλες πληροφορίες όπως η τοποθεσίας τους. Για την επικοινωνία χρησιμοποιούσαν ψηφιακές υπογραφές έτσι ώστε να ήταν αδύνατη η αλλαγή των πληροφοριών που διάβαζαν οι αισθητήρες. Παρ όλα αυτά και οι δύο πλευρές αντιλήφθηκαν γρήγορα την ικανότητα να κρύβουν επιπλέον πληροφορίες μέσω των υποσυνείδητων καναλιών τα οποία υπάρχουν στα περισσότερα σχέδια ψηφιακών υπογραφών [2].

1.4.1 Το πρόβλημα των φυλακισμένων

Η πιο σημαντική ιδιότητα που διαθέτει η στεγανογραφία είναι η δυσκολία εντοπισμού της, πράγμα το οποίο σημαίνει ότι είναι αδύνατο για ένα κακόβουλο άνθρωπο να αντιληφθεί αν δύο άτομα που επικοινωνούν κάνουν χρήση της στεγανογραφία ή απλά μιλάνε κανονικά. Ο Simmons παρέχει μια δημοφιλή ανάπτυξη του προβλήματος στης στεγανογραφίας μέσα από το διάσημο πρόβλημα του φυλακισμένου.

Έστω ότι δύο άτομα Α και Β είναι φυλακισμένα σε διαφορετικά κελιά και θέλουν να αναπτύξουν ένα σχέδιο, βάση του οποίου θα δραπετεύσουν. Επιτρέπεται να επικοινωνούν αλλά η επικοινωνία τους παρακολουθείται από έναν φύλακα. Στην περίπτωση όπου ο φύλακας αντιληφθεί ότι οι δύο κρατούμενοι ανταλλάσουν μυστικά μηνύματα τότε θα τους κόψει το κανάλι επικοινωνίας και θα τους βάλει στην απομόνωση. Γι' αυτό οι φυλακισμένοι κατέφυγαν στην στεγανογραφία σαν μέσο ανταλλαγής πληροφοριών και λεπτομερειών έτσι ώστε να δραπετεύσουν. Θα πρέπει εδώ να σημειώσουμε ότι το μόνο που χρειάζεται ο φύλακας είναι να εντοπίσει την παρουσία μυστικών μηνυμάτων χωρίς να χρειαστεί να μάθει το περιεχόμενο των μηνυμάτων αυτών. Με άλλα λόγια αν ο φύλακας ανακαλύψει ότι οι κρατούμενοι επικοινωνούν μυστικά, τότε το στεγανογραφικό σύστημα θα σπάσει.

Θα πρέπει επίσης να τονίσουμε ότι στο πρόβλημα των φυλακισμένων, ο φύλακας γνωρίζει καλά τον στεγανογραφικό αλγόριθμο που μπορεί να χρησιμοποιήσουν οι φυλακισμένοι. Ωστόσο δεν έχει καμία γνώση του μυστικού στεγο-κλειδιού, για το οποίο οι φυλακισμένοι είχαν συμφωνήσει προτού μπουν στην φυλακή. Η απαίτηση ότι ο στεγανογραφικός αλγόριθμος μπορεί να είναι γνωστός στον φύλακα είναι η αρχή του Kerckhoffs' [9] που προέρχονται από την κρυπτογραφία. Αυτή η φαινομενικά δυνατή και παρανοϊκή αρχή δηλώνει ότι η ασφάλεια της επικοινωνίας δεν πρέπει να βρίσκεται στην μυστικότητα του συστήματος αλλά μόνο στο μυστικό κλειδί. Η αρχή αυτή πηγάζει από το γεγονός ότι ο κρυπτογραφικός αλγόριθμος μπορεί να «πέσει» στα χέρια του εχθρού και έτσι να χαθεί η ασφάλεια και η μυστικότητα του καναλιού επικοινωνίας [2].

1.4.2 Ασφάλεια στεγανογραφίας

Μια από τις κύριες προϋποθέσεις της στεγανογραφίας είναι ότι οποιοσδήποτε κακόβουλος που επιδιώκει να μάθει ένα μυστικό μήνυμα, δεν θα μπορέσει να αποφασίσει εάν ή όχι ένα δοθέν αντικείμενο περιέχει το κρυμμένο μήνυμα. Θα πρέπει εδώ να επισημάνουμε ότι η μαθηματική ανάλυση αυτής της προϋπόθεσης είναι ιδιαίτερα δύσκολή.

Σύμφωνα τώρα με την αρχή του Kerckhoffs' και το πρόβλημα των φυλακισμένων, ο φύλακας έχει μια πλήρη γνώση του στεγανογραφικού αλγόριθμου, πράγμα το οποίο σημαίνει ότι έχει όλες εκείνες τις πληροφορίες που χρειάζεται σχετικά με την πηγή του κρυμμένου αντικειμένου και από τους δύο φυλακισμένους. Σε θεωρητικό επίπεδο, μπορούμε να πούμε ότι ο φύλακας γνωρίζει πως μπορεί να είναι το αντικείμενο εκείνο που χρησιμοποιούν οι φυλακισμένοι για να ανταλλάσουν τα μηνύματα που θέλουν. Έτσι πραγματοποιώντας ένα τεστ μπορεί να ανακαλύψει εάν οι φυλακισμένοι επικοινωνούν χρησιμοποιώντας την στεγανογραφία [2].

Επειδή οι ψηφιακές εικόνες είναι αρκετά πολύπλοκα, πολλών διαστάσεων αντικείμενα αποτελούμενα από εκατομμύρια εικονοστοιχεία (pixels) δεν είναι εφικτό κανείς να καταλάβει εάν πίσω από τις εικόνες κρύβονται μυστικά μηνύματα. Η σύγχρονη στεγανάλυση λειτουργεί χρησιμοποιώντας απλοποιημένα μοντέλα τα οποία αποτελούνται από ένα σύνολο στατιστικών μεγεθών προερχόμενα από εικόνες, όπως ένα δείγμα ιστογραμμάτων από τιμές εικονοστοιχείων ή διαφόρων τύπων στατιστικών υπολογισμών από γειτονικά ζευγάρια εικονοστοιχείων. Με αυτό τον τρόπο ο οποιοσδήποτε κακόβουλος υπολογίζει αυτά τα μεγέθη και τα συγκρίνει με τις αναμενόμενες τιμές που υπολογίστηκαν από την εικόνα που χρησιμοποιείται για το κρύψιμο των μηνυμάτων. Σημαντικές στατιστικές αποκλίσεις από τις αναμενόμενες τιμές ερμηνεύονται σαν στοιχεία ότι η εικόνα έχει υποστεί αλλοιώσεις από κάποιον στεγανογραφικό αλγόριθμο [2].

Παρ όλο που αυτή η ποσοτική άποψη της ασφάλειας της στεγανογραφίας επιτρέπει αυστηρές μαθηματικές μεθόδους και αυστηρή μελέτη, είναι μόνο μια προσέγγιση της ιδέας της δυσκολίας εντοπισμού. Για παράδειγμα, τα στατιστικά μεγέθη δεν περιγράφουν καλά την εννοιολογική ερμηνεία των εικόνων επικοινωνίας. Ας πάρουμε για παράδειγμα την περίπτωση όπου κάποιος γράφει ένα μήνυμα πάνω σε ένα χαρτί, στην συνέχεια παίρνει μια φωτογραφία του χαρτιού αυτού και έπειτα προσκολλάει την φωτογραφία αυτή στο mail του. Επειδή η φωτογραφία δεν μπορεί να τροποποιηθεί, οι στατιστικές της ιδιότητες θα είναι «ανεκτικές» (σχεδόν ίδιες) με αυτές που δημιουργήθηκαν από την κάμερα του. Έτσι, οποιοδήποτε αυτόματο σύστημα στεγανάλυσης που θα επιθεωρούσε τις στατιστικές ιδιότητες εικόνων θα θεωρούσε την εικόνα ως ανεκτική [2].

Είναι ενστικτωδώς ξεκάθαρο ότι οι φυλακισμένοι θα μπορούσαν να αυξήσουν την αίσθηση ασφάλειας και να μειώσουν την πιθανότητα να γίνουν αντιληπτοί από τον φύλακα, εάν επικοινωνούσαν μόνο με πολύ μικρά μηνύματα. Αυτό βέβαια θα έκανε την επικοινωνία τους λιγότερη αποτελεσματική και μη πρακτική. Γι' αυτό το λόγο οι φυλακισμένοι θα πρέπει να γνωρίζουν πόσο μεγάλο μέγεθος μηνύματος μπορούν να κρύψουν σε ένα δοθέν αντικείμενο χωρίς να γίνουν αντιληπτοί από τον φύλακα. Το μέγεθος αυτό ονομάζεται χωρητικότητα στεγανογραφίας [2].

1.4.3 Στεγανογραφία και Κρυπτογραφία

Η στεγανογραφία και η κρυπτογραφία είναι δύο παράλληλες τεχνικές ασφαλείας δεδομένων μιας και οι δύο έχουν ως κύριο στόχο τους την απόκρυψη μυστικών μηνυμάτων χωρίς κάποιος τρίτος να μάθει το περιεχόμενο των μηνυμάτων. Και οι δύο τεχνικές μπορούν να εφαρμοστούν δίπλα-δίπλα. Στην πραγματικότητα όμως οι περισσότερες στεγανογραφικές χρησιμότητες εφαρμόζουν την κρυπτογραφική ασφάλεια δεδομένων.

Παρ όλο που οι δύο τομείς δεν έρχονται σε αντίθεση ο ένας με τον άλλον, έχουν τις παρακάτω διαφορετικές ιδιότητες [10]:

- Η στεγανογραφία μπορεί να χρησιμοποιήσει την κρυπτογραφία αλλά το αντίθετο δεν ισχύει.
- Στην κρυπτογραφία, σε αντίθεση με την στεγανογραφία, το μόνο που μπορούμε είναι να προστατεύσουμε το μυστικό μήνυμα αλλά δεν μπορούμε να αποκρύψουμε την ύπαρξή του.
- Στην στεγανογραφία χρειάζεται να παραδώσει κανείς το αντικείμενο στο οποίο είναι κρυμμένο το μυστικό μήνυμα μαζί με το κλειδί και τα στοιχεία που απαιτούνται.

Θα μπορούσαμε εδώ να πούμε ότι δεν υπάρχει κανένα όφελος από την προσπάθεια να κρυφτεί ένα μήνυμα που είναι λογικά προσδοκώμενο. Για παράδειγμα, μια κυβερνητική πύλη (portal) που είναι γνωστή ότι στέλνει ή λαμβάνει μυστικά μηνύματα δεν θα ωφελούταν από αυτήν την τεχνική της στεγανογραφίας. Από την άλλη μεριά όμως, μια επιχειρησιακή εταιρία που επιδιώκει το κρύψιμο κάποιου εγγράφου ή ενός κατασκόπου θα εκτιμούσε βεβαίως μια τέτοια τεχνική καθώς δεν θα γινόταν αντιληπτό το γεγονός της ύπαρξης μυστικής επικοινωνίας [10].

1.4.4 Στεγανογραφία και υδατογράφηση

Στην υποενότητα αυτή θα αναφερθούμε σε μια βασική διαφορά που υπάρχει ανάμεσα στην στεγανογραφία και σε ένα σχετικό τομέα απόκρυψης πληροφοριών που ονομάζεται υδατογράφηση. Παρ όλο που η υδατογράφηση και η στεγανογραφία μοιράζονται πολλές βασικές ομοιότητες σε σχέση πάντα με την απόκρυψη πληροφοριών, απευθύνονται ωστόσο σε διαφορετικές εφαρμογές. Στην στεγανογραφία, η εικόνα στην οποία κρύβουμε το μυστικό μήνυμα χρησιμοποιείται μόνο για αντιπερισπασμό και δεν έχει καμία σχέση με το μυστικό μήνυμα. Αντίθετα, ένα υδατογράφημα συνήθως κρατάει συμπληρωματική πληροφορία σχετικά με την εικόνα που χρησιμοποιείται για κάλυψη ή άλλα δεδομένα σχετικά με το «κάλυμμα», όπως για παράδειγμα ετικέτες οι οποίες προσδιορίζουν τον αποστολέα ή τον παραλήπτη. Για παράδειγμα, έστω ότι κάποιος αγοράζει ένα μουσικό αρχείο mp3 μέσω του Διαδικτύου.

Πληροφορίες σχετικά με τον αγοραστή ή τον πωλητή μπορούν να καταχωρηθούν μέσα στο τραγούδι με την μορφή ενός μη ακουστικού αλλά γερού υδατογραφήματος. Το υδατογράφημα μπορεί έπειτα να χρησιμοποιηθεί για να εμποδίζει την παράνομη αντιγραφή του τραγουδιού [7].

Μια δεύτερη εξίσου σημαντική διαφορά ανάμεσα στην στεγανογραφία και την υδατογράφηση είναι το θέμα της ύπαρξης του μυστικού μηνύματος μέσα στην εικόνα. Ενώ στη στεγανογραφία είναι ιδιαίτερα σημαντικό η εικόνα να μην παρουσιάζει ίχνη των κρυμμένων δεδομένων, στην υδατογράφηση η ύπαρξη του υδατογραφήματος γνωστοποιεί την αποτροπή μιας παράνομης πράξης, όπως είναι η αντιγραφή. Επιπλέον, η στεγανογραφία είναι ένας τρόπος επικοινωνίας χάρις την οποία επιτρέπεται η αποστολή μεγάλης ποσότητας κρυφών δεδομένων. Από την άλλη μεριά, ακόμα και ένα μικρό υδατογράφημα μπορεί να είναι ιδιαίτερα χρήσιμο. Για παράδειγμα, η παρουσία υδατογραφήματος αποτελεί μια κατάθεση της ιδιοκτησίας μιας εικόνας [7].

Τέλος θα μπορούσαμε να πούμε ότι παρ' όλες τις ομοιότητες που μπορεί να έχουν η στεγανογραφία και η υδατογράφηση είναι τελικά δύο διαφορετικοί εφαρμογές απόκρυψης και αποστολής μηνυμάτων.

1.5 Στεγανάλυση

Η στεγανογραφία είναι ένα «ιδιωτικό» εργαλείο και είναι απόλυτα φυσικό να προσελκύει την ανθρώπινη περιέργεια με απώτερο σκοπό την επίθεση. Οι προσπάθειες επικεντρώνονται στην ανάπτυξη μεθόδων που θα είναι ικανές να ανιχνεύσουν την παρουσία μυστικών μηνυμάτων και να εκμαιεύσουν τα μηνύματα αυτά. Όλη αυτή την διαδικασία την ονομάζουμε στεγανάλυση [2].

Στεγανάλυση είναι η τέχνη της ανίχνευσης της χρήσης στεγανογραφίας στο εσωτερικό ενός αρχείου.

Το πεδίο της στεγανάλυσης αναπτύχθηκε ταχύτατα ύστερα από τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001 όταν διαδόθηκε η φημολογία ότι οι τρομοκράτες χρησιμοποίησαν την μέθοδο της στεγανογραφίας για να οργανώσουν τις επιθέσεις τους [11]. Επιπλέον, σε μια διαφορετική περίπτωση εγκλήματος το 2000, το εμπορικό στεγανογραφικό εργαλείο S-tool χρησιμοποιήθηκε στην εξάπλωση της παιδικής πορνείας. Ο ύποπτος ωστόσο συλήθηκε επιτυχώς χάρις την μέθοδο της στεγανάλυσης [12].

Η στεγανάλυση είναι ένας αποτελεσματικός τρόπος για να κριθεί η ασφάλεια των επιδόσεων των στεγανογραφικών τεχνικών. Η στεγανάλυση ασχολείται τόσο με το να εντοπίσει αν ένα αρχείο χρησιμοποιείται για να καλύψει ένα μυστικό μήνυμα όσο και με το να προσπαθεί να αποκρυπτογραφήσει τις πληροφορίες στο εσωτερικό του αρχείου αυτού.

Υπάρχουν δύο ειδών επιθέσεις κατά των στεγανογραφικά κρυμμένων μηνυμάτων. Η πρώτη είναι η ανίχνευση του αρχείου στο οποίο είναι κρυμμένη η πληροφορία και η δεύτερη είναι η απόσπαση τους δηλαδή ο τρόπος με τον οποίο θα πάρουμε την πληροφορία αυτή από το αρχείο[13].

Υπάρχουν πολλές μέθοδοι που μπορούν να χρησιμοποιηθούν για την ανίχνευση της στεγανογραφίας. Μια από αυτές είναι η προβολή του αρχείου και η σύγκριση του με ένα άλλο αντίγραφο του αρχείου που βρέθηκε στο Διαδίκτυο (φωτογραφία, βίντεο, mp3). Στην περίπτωση όπου υπάρχουν διαφορές μεταξύ του ύποπτου αρχείου και του αντιγράφου του από το Διαδίκτυο τότε το αρχείο αυτό χρησιμοποιείται για απόκρυψη μυστικού μηνύματος Οι διαφορές αυτές συνθέτουν το ωφέλιμο φορτίο. Για παράδειγμα εάν φορτώσουμε μία εικόνα JPEG και το ύποπτο αρχείο είναι επίσης μια εικόνα JPEG, τότε και τα δύο είναι σχεδόν όμοια εκτός και αν το ένα είναι μεγαλύτερο από το άλλο. Έτσι συμπεραίνουμε ότι το ύποπτο αρχείο περιέχει πληροφορίες στο εσωτερικό του.

Αντίστοιχη περίπτωση είναι όταν έχουμε ένα μουσικό αρχείο. Για να εντοπίσουμε κρυμμένες πληροφορίες εντός ενός αρχείου ήχου θα πρέπει να βρεθεί ένα αρχείο ήχου ώστε να συγκριθεί με εκείνο που χρησιμοποιεί την ίδια συμπίεση mp3. Στην περίπτωση που υπάρχουν διαφορές τότε συμπεραίνουμε ότι στο αρχείο ήχου υπάρχει κρυμμένη κάποια μυστική πληροφορία.

Όπως ακριβώς η κρυπτανάλυση εφαρμόζει διάφορες τεχνικές με σκοπό την αποκρυπτογράφηση της πληροφορίας, έτσι και η στεγανάλυση εφαρμόζοντας δικές της τεχνικές αποσκοπεί στην ανίχνευση της κρυμμένης πληροφορίας.

Ο στεγαναλυτής χρησιμοποιεί τεχνικές επίθεσης ανάλογα με το τι είδους πληροφορία έχει στα χέρια του. Έτσι η μία τεχνική επίθεσης είναι η στεγο-αποκλειστική. Η στεγο-αποκλειστική είναι διαθέσιμη για ανάλυση μόνο της κρυμμένης πληροφορίας. Εάν τόσο η αρχική όσο και η κρυπτογραφημένη πληροφορία είναι διαθέσιμες τότε μιλάμε για επίθεση «γνωστού μέσου». Η δεύτερη τεχνική επίθεσης είναι η επιλεκτική στεγο-επίθεση, κατά την οποία τόσο ο αλγόριθμος που χρησιμοποιείται όσο και το στεγο-μέσο είναι γνωστά. Μια επίθεση επιλεγμένου μέσου είναι αυτή στην οποία ο στεγαναλυτής δημιουργεί το στεγο-μέσο από κάποιο στεγανογραφικό εργαλείο ή αλγόριθμο γνωστού μηνύματος. Ο στόχος είναι ο καθορισμός συγκεκριμένων ιδιοτήτων του στεγο-μέσου που συγκλίνουν στη χρήση κάποιου στεγανογραφικού εργαλείου ή αλγορίθμου[13].

Δύο είναι οι κύριες κατηγορίες στεγανάλυσης, η παθητική στεγανάλυση και η ενεργή στεγανάλυση. Πιο συγκεκριμένα[2]:

- Η παθητική στεγανάλυση ανιχνεύει την απουσία ή την παρουσία κρυφών δεδομένων σε ένα μήνυμα.
- Η ενεργή στεγανάλυση εκθέτει μερικές ιδιότητες του μηνύματος ή του αλγόριθμου ενσωμάτωσης και εξάγει μια έκδοση του μυστικού μηνύματος κατά προσέγγιση, από ένα στεγο-μήνυμα.

Συμπερασματικά θα μπορούσαμε να πούμε ότι ο κύριος στόχος της στεγανάλυσης είναι να προσδιοριστούν οι πιθανές πληροφορίες και να καθοριστεί με σαφήνεια το γεγονός εάν κάποιος έχει κρύψει ή όχι μηνύματα που κωδικοποιούνται. Οι επιθέσεις και η ανάλυση στις κρυμμένες πληροφορίες μπορούν να λάβουν διάφορες μορφές αλλά και να θέσουν εκτός λειτουργίας ή και να καταστρέψουν τις κρυμμένες πληροφορίες.

1.6 Συμπεράσματα

Η στεγανογραφία, που συνδυάζεται σχεδόν αρμονικά με την τεχνική της κρυπτογραφίας, είναι ένα ισχυρό εργαλείο που επιτρέπει στους ανθρώπους να επικοινωνούν κρυφά, κρύβοντας τα μυστικά μηνύματα μέσα σε αντικείμενα όπως εικόνες, βίντεο και μουσικά αρχεία. Η στεγανογραφία είναι μια επιστήμη πολύ παλιά, ωστόσο η καθιέρωσή της πραγματοποιήθηκε κατά τη διάρκεια του προηγούμενου αιώνα, και κυρίως με την άνοδο της εποχής υπολογιστών.

Αν και η τεχνική της στεγανογραφίας ακόμα δεν χρησιμοποιείται πολύ συχνά, οι δυνατότητες είναι ατελείωτες. Πολλές διαφορετικές μεθόδους στεγανογραφίας υπάρχουν και συνεχίζουν να αναπτύσσονται, ενώ οι τρόποι ανίχνευσης κρυμμένων μηνυμάτων προωθούνται επίσης γρήγορα.

Δεδομένου ότι η ανίχνευση δεν μπορεί ποτέ να δώσει μια εγγύηση εύρεσης όλων των κρυμμένων πληροφοριών, μπορεί να χρησιμοποιηθεί μαζί με τις μεθόδους της στεγανογραφίας με σκοπό την ελαχιστοποίηση των πιθανοτήτων πραγματοποίησης μιας μυστικής επικοινωνίας. Ακόμα και τότε όμως, το μυστικό κλειδί δεν θα μπορεί να γίνει ανιχνεύσιμο, επειδή η πηγή κάλυψης δεν περιέχει καμία πληροφορία για το μυστικό κλειδί.

Στο άμεσο μέλλον, η σημαντικότερη χρήση των τεχνικών στεγανογραφίας θα απαντηθεί πιθανώς στον τομέα της υδατογράφησης παρ όλες τις διαφορές που έχουν. Πολλοί προμηθευτές επιθυμούν να προστατεύσουν τις εργασίες ενάντια στην παράνομη διανομή και τα ψηφιακά υδατογραφήματα παρέχουν έναν τρόπο τους ιδιοκτήτες αυτών των υλικών για να το πραγματοποιήσουν.

Τέλος θα πρέπει να επισημάνουμε ότι η στεγανογραφία χρησιμοποιείται τόσο για ειρηνικούς σκοπούς όσο και για τρομοκρατικές επιθέσεις και αυτός είναι ο κύριος λόγος του περιορισμού χρήση της, βάση κυβερνητικών νόμων που ισχύουν σε κάθε χώρα.

Βιβλιογραφία

[1] G. Kolata. “A mystery unraveled, twice” The New York Times, pages F1-F6, April 1998.

[2] Jessica Fridrich “Steganography in Digital Media” Cambridge University Press 2010.

[3] Ζωή Σπανάκου “Ηροδότου Ιστορίες” ΟΕΔΒ Αθήνα.

[4] J. Brassil, S.Low, N. F. MAxemchunk, and L. O’Gorman. “Hiding information in document images.” In Procceedings of the Conference on Information Sciences and Systems, CISS, pages 482-489, March 22-24 1995.

[5] Denton Jr. Blinking Morse Code 'T-O-R-T-U-R-E' [http://www.dentongenealogy.org Jeremiah%20Andrew%20Denton.htm].

[6] Udit Budddia and Deepak Kundur, “Digital video steganalysis exploiting collusion Sensitivity” Department of Electrical Engineering, Texas A&M University, 2006.

[7] Ingermar J. Cox ‘‘Digital watermarking and steganography’’ Morgan Kaufmann 2008.

[8] T. Sharp. An implementation of key-based digital signal Steganography.In I.S. Moskowitz, editor, “Information Hiding, 4th international workshop on information hiding”, 25-27 April 2001, Spronger-Verlag, New York.

[9] Kahn, David, “The Codebreakers: the story of secret writing, Scribners” Second Edition, 1996 p.235.

[10] Mohammad Fahmi Alalem and Abdallah Muhanah Manasrah “A Steganographic Data Security Algorithm with Reduced Steganalysis Threat” Birzeit University.

[11] S. Coll and S. B. Glasser, “Terrorists turn to web as base of operations” Washington Post, August 2005.

[12] N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen. IEEE Computer” February 1998.

[13] J.R. Krenn, “Steganography and Steganalysis” January 2004.

[14] Το παράδειγμα που περιγράψαμε στο υποκεφάλαιο 1.3 προέρχεται από το βιβλίο “Steganography in Digital Media” της Jessica Fridrich.

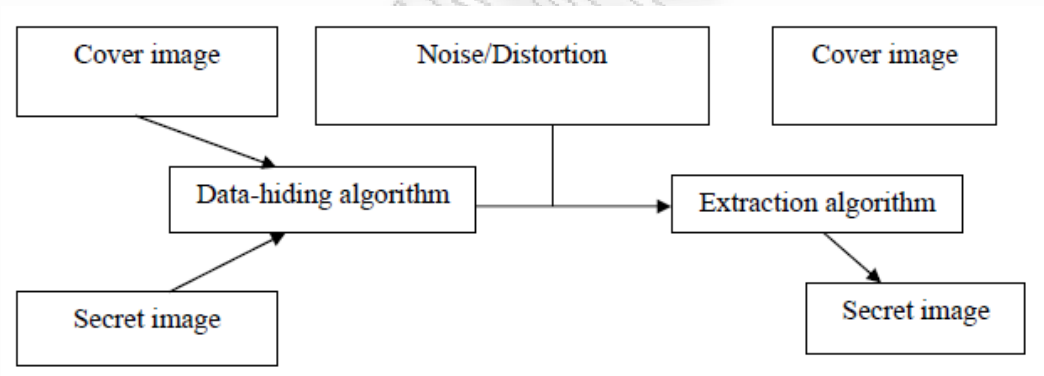
Κεφάλαιο 2

Η στεγανογραφία σε βάθος

2.1 Τεχνικές στεγανογραφίας

Οι στεγανογραφικές τεχνικές στοχεύουν στο μυστικό κρύψιμο δεδομένων μέσα σε πολυμεσικούς «ξενιστές» όπως είναι το κείμενο, η εικόνα ή το βίντεο, χωρίς να προκαλούν υποψίες για το περιεχόμενο τους. Οι «ξενιστές» ονομάζονται αντικείμενα κάλυψης (cover objects) σύμφωνα με την ορολογία του τομέα της στεγανογραφίας. Στην παρούσα μεταπτυχιακή διατριβή θα επικεντρωθούμε κυρίως στην στεγανογραφία όπου τα αντικείμενα κάλυψης είναι εικόνες [3].

Η εικόνα που ακολουθεί αναπαριστά ένα βασικό σύστημα απόκρυψης πληροφοριών στο οποίο η τεχνική ενσωμάτωσης λαμβάνει μια εικόνα κάλυψης και μια μυστική εικόνα ως είσοδος και παράγει ως έξοδο μια στεγο-εικόνα (stego image), η οποία είναι φαινομενικά αμετάβλητη παρ' όλο που περιέχει τα ενσωματωμένα δεδομένα που εμείς θέλουμε να κρύψουμε. Η στεγο-εικόνα μπορεί να σταλεί μέσω διαφόρων καναλιών επικοινωνίας. Ο αποδέκτης που λαμβάνει την στεγο-εικόνα μπορεί έπειτα να πραγματοποιήσει τη διαδικασία εξαγωγής για να ανακτήσει το μυστικό μήνυμα από την στεγο-εικόνα [3].



Εικόνα 2.1 Αναπαράσταση στεγανογραφικού συστήματος
Πηγή: (Steganography in Digital Media)

Υπάρχουν τριών ειδών προσεγγίσεις που μπορούν να χρησιμοποιηθούν έτσι ώστε να κρύψουμε μια πληροφορία μέσα σε ένα αντικείμενο κάλυψης. Αυτές είναι οι εξής:

- Έγχυση.
- Αντικατάσταση.
- Παραγωγή.

2.1.1 Έγχυση

Τα δεδομένα μπορούν να κρυφτούν στα τμήματα ενός αρχείου τα οποία αγνοούνται κατά την επεξεργασία μιας εφαρμογής χρησιμοποιώντας την τεχνική έγχυσης (injection technique). Επομένως τα bits του αρχείου που είναι σχετικά με έναν τελικό χρήστη (end-user) δεν τροποποιούνται, καθιστώντας το αρχείο κάλυψης απόλυτα λειτουργικό. Για παράδειγμα, μπορούμε να προσθέσουμε αβλαβείς bytes σε ένα εκτελέσιμο ή δυαδικό αρχείο. Επειδή αυτά τα bytes δεν έχουν επιπτώσεις στη διαδικασία επεξεργασίας του αρχείου, ο τελικός χρήστης δεν

μπορεί να συνειδητοποιήσει ότι το αρχείο περιέχει τις πρόσθετες κρυμμένες πληροφορίες. Παρ όλα αυτά, η χρησιμοποίηση μιας τεχνικής έγχυσης αλλάζει το μέγεθος του αρχείου σύμφωνα με το ποσό των κρυμμένων δεδομένων και επομένως, εάν το αρχείο φαίνεται ασυνήθιστα μεγάλο, μπορεί να προκαλέσει υποψίες. Επομένως θα μπορούσαμε να πούμε ότι η χρησιμοποίηση της τεχνικής έγχυσης πρέπει να πραγματοποιείται για πολύ μικρό μήνυμα [4].

2.1.2 Αντικατάσταση

Η τεχνική αντικατάστασης (substitution technique) χρησιμοποιείται για να αντικαταστήσει το λιγότερο σημαντικό bits των πληροφοριών που καθορίζουν το σημασιολογικό περιεχόμενο του αρχικού αρχείου με το νέο δεδομένο, κατά τέτοιο τρόπο ώστε να προκαλεί το λιγότερο ποσό διαστρέβλωσης. Το κύριο πλεονέκτημα αυτής της τεχνικής είναι ότι το μέγεθος του αρχείου κάλυψης δεν αλλάζει μετά από την εκτέλεση του αλγορίθμου. Από την άλλη μεριά, αυτή η προσέγγιση έχει τουλάχιστον δύο μειονεκτήματα. Κατ' αρχάς, το στεγο-αντικείμενο μπορεί να επηρεαστεί αρνητικά από την ποιότητα υποβάθμιση (αλλάζει η ποιότητα της εικόνας) με αποτέλεσμα να προκαλέσει υποψίες. Δεύτερον, η τεχνική της αντικατάσταση περιορίζει το ποσό δεδομένων που μπορούμε να κρύψουμε στον αριθμό των λιγότερο σημαντικών bits του αρχείου [2].

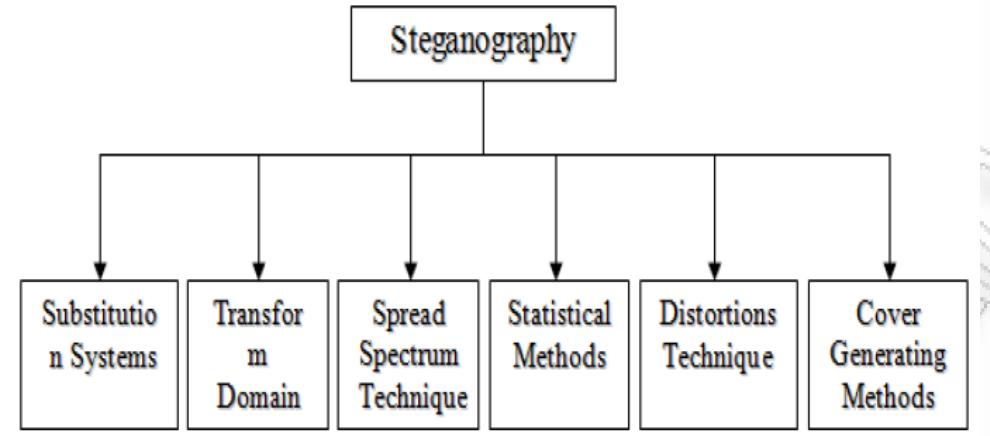
2.1.3 Παραγωγή

Αντίθετα από τις τεχνικές της έγχυση και της αντικατάστασης, η τεχνική παραγωγής δεν απαιτεί την ύπαρξη ενός αρχείου κάλυψης. Αυτή η τεχνική παράγει ένα αρχείο κάλυψης με αποκλειστικό σκοπό το κρύψιμο του μήνυμα. Το κύριο μειονέκτημα των τεχνικών της έγχυσης και της αντικατάστασης είναι ότι οι άνθρωποι μπορούν να συγκρίνουν το στεγο-αντικείμενο με οποιοδήποτε προϋπάρχον αντίγραφο του αντικειμένου κάλυψης (το οποίο υποτίθεται πως είναι το ίδιο αντικείμενο) και να ανακαλύψουν τις διαφορές μεταξύ των δύο. Με την χρήση όμως της τεχνικής παραγωγής δεν θα έχουμε αυτό το πρόβλημα, επειδή το αποτέλεσμα είναι ένα αυθεντικό αρχείο, και επομένως δεν αποσκοπούν σε τίποτα οι δοκιμές σύγκρισης [5].

2.2 Κατηγορίες στεγανογραφίας

Σε όλες τις μεθόδους της στεγανογραφίας, πραγματοποιούνται διάφορες διαδικασίες με σκοπό την απόκρυψη του μηνύματος. Αυτές οι διαδικασίες ή αλλιώς αυτές οι τεχνικές μπορούν να διαχωριστούν και να αναλυθούν, έτσι ώστε να μάθουμε τι ακριβώς συμβαίνει κατά την διάρκεια ολόκληρης της διαδικασίας. Οι έξι κατηγορίες της στεγανογραφίας είναι οι εξής [1]:

- Substitution system techniques
- Transform domain techniques
- Spread spectrum techniques
- Statistical methods
- Distortion techniques
- Cover generation methods



Εικόνα 2.2 Κατηγορίες στεγανογραφίας.

Πηγή: (Journal of Computing, Volume 2, Issue 3, March 2010)

Στην συνέχεια αυτού του υποκεφαλαίου θα παρουσιάσουμε κάθε μια από τις παραπάνω κατηγορίες της στεγανογραφίας.

2.2.1 Τεχνική συστήματος αντικατάστασης

Το σύστημα αντικατάστασης (substitution system) αντικαθιστά περιττά ή αχρείαστα bits του αντικειμένου κάλυψης με τα bits του μυστικού μηνύματος. Πολλά στεγανογραφικά εργαλεία χρησιμοποιούν την μέθοδο του λιγότερο σημαντικού bit (Least-Significant Bit) με σκοπό να κρυπτογραφήσουν το μυστικό μήνυμα. Η μέθοδος LSB λειτουργεί με το ακόλουθο τρόπο:

Έστω ότι διαθέτουμε ένα ψηφιακό αντικείμενο (εικόνα, ήχος, βίντεο). Σε ένα τέτοιο αντικείμενο υπάρχει ένα τεράστιο ποσό άχρηστου ή περιττού χώρου. Αυτόν ακριβώς τον χώρο χρησιμοποιεί η στεγανογραφία για να κρύψει το μυστικό μήνυμα που θέλει μέσα στο ψηφιακό αντικείμενο. Για παράδειγμα έστω ότι η ακόλουθη σειρά από bytes αντιπροσωπεύει ένα μέρος του αντικειμένου κάλυψης (εικόνα) [1]:

10000100 10000110 100001001 10001101

01111001 01100101 01001010 00100110

Κάθε byte αποτελείται από 8bits. Αυτά τα bits δημιουργούν την τιμή χρώματος της εικόνας μας που μπορεί να είναι η απόχρωση του πράσινου, του κόκκινου, του μπλε κ. λ. π. Θα πρέπει να επισημάνουμε στο σημείο αυτό ότι, τα αριστερότερα bits που φτιάχνουν το byte είναι μεγαλύτερης σημαντικότητας από τα δεξιότερα bits. Με άλλα λόγια καθώς πηγαίνουμε από τα αριστερά προς τα δεξιά μειώνεται η σημαντικότητα των bits. Και αυτό συμβαίνει διότι τα αριστερότερα bits είναι αυτά τα οποία καθορίζουν την απόχρωση του χρώματος. Για παράδειγμα αλλάζοντας το πρώτο bit από 1 σε 0 της ακολουθία 10000100 τότε έχουμε μια μεγάλη αλλαγή χρώματος. Ωστόσο αν αλλάζουμε το τελευταίο bit από 0 σε 1 στην ακολουθία 10000100 τότε το χρώμα θα παραμείνει σχεδόν το ίδιο. Αυτός είναι ακριβώς και ο λόγος για το οποίο χρησιμοποιούμε την μέθοδο LSB με σκοπό να μην έχουμε μεγάλες αλλαγές.

Έστω, λοιπόν ότι έχουμε την παραπάνω ακολουθία και θέλουμε να χρησιμοποιήσουμε την στεγανογραφία για να κρύψουμε ένα μυστικό μήνυμα. Στόχος μας είναι να κρύψουμε τον αριθμό 213 ο οποίος αντιστοιχεί στον δωμάτιο ενός ξενοδοχείου. Η δυαδική αναπαράσταση του αριθμού 213 είναι η εξής [1]:

11010101

Τώρα θα χρησιμοποιήσουμε την μέθοδο του λιγότερου γνωστού bit έτσι ώστε να κρύψουμε τον αριθμό 213, που είναι το μυστικό μας μήνυμα, μέσα στην εικόνα (αντικείμενο κάλυψης). Έχουμε λοιπόν ότι:

10000100 → Το 0 αντικαθίσταται με το 1, που είναι το πρώτο bit του κρυφού μηνύματος.

10000110 → Το 0 αντικαθίσταται με το 1, που είναι το δεύτερο bit του κρυφού μηνύματος.

10001001 → Το 1 αντικαθίσταται με το 0, που είναι το τρίτο bit του κρυφού μηνύματος.

10001101 → Το 1 παραμένει το ίδιο γιατί αντιπροσωπεύει το 1 του κρυφού μηνύματος.

01111001 → Το 1 αντικαθίσταται με το 0, που είναι το πέμπτο bit του κρυφού μηνύματος.

01100101 → Το 1 παραμένει το ίδιο γιατί αντιπροσωπεύει το 1 του κρυφού μηνύματος.

01001010 → Το 1 παραμένει το ίδιο γιατί αντιπροσωπεύει το 1 του κρυφού μηνύματος.

00100110 → Το 0 αντικαθίσταται με το 1, που είναι το όγδοο bit του κρυφού μηνύματος.

Όπως μπορούμε να συμπεράνουμε από τα παραπάνω χρειάστηκε να αλλάξουμε μόνο πέντε από τα οκτώ bytes έτσι ώστε να ενσωματώσουμε την πληροφορία μας μέσα στο αντικείμενο κάλυψης. Μπορεί λοιπόν να φανταστεί κανείς το πλήθος της περιττής πληροφορίας σε μια εικόνα κάλυψης της οποίας το μέγεθος είναι 500KB ή 1 MB. Με τόσα πολλά 1 και 0 τα οποία χαρακτηρίζονται λιγότερα σημαντικά bits η αλλοίωση της εικόνας είναι μηδαμινή.

Η τεχνική της LSB μεθόδου είναι η πιο κοινά χρησιμοποιούμενη στις εφαρμογές της στεγανογραφία και αυτό γιατί ο αλγόριθμος είναι μικρός και εύκολος στην χρήση του. Θα πρέπει εδώ να προσθέσουμε ότι η μέθοδο της LSB λειτουργεί το ίδιο καλά τόσο σε ασπρόμαυρες εικόνες όσο και σε έγχρωμες.

Ωστόσο η μέθοδος LSB έχει και τα μειονεκτήματά της. Πιο συγκεκριμένα, υπάρχουν κάποιες περιπτώσεις όπου η χρήση της μεθόδου LSB μπορεί να επηρεάσει δραματικά τις ιδιότητες των εικονοστοιχείων, κάνοντας τα να φαίνονται έξω από το πλαίσιο της εικόνας. Έτσι είναι εύκολο για κάποιον κακόβουλο να εντοπίσει ότι δύο άτομα επικοινωνούν κάνοντας χρήση της στεγανογραφίας. Αυτό το πρόβλημα μπορεί να λυθεί στην περίπτωση όπου το μήνυμα μας είναι μικρό. Με αυτό τον τρόπο μειώνονται τα προς αντικατάσταση bits.

Ένα άλλο πρόβλημα είναι ότι πολλές φορές η εικόνα στην οποία έχουμε κρύψει το μυστικό μας μήνυμα μπορεί να κοπεί ή να περιστραφεί. Σε αυτή την περίπτωση ο αλγόριθμος δεν θα είναι ικανός να εντοπίσει ποιο λιγότερο σημαντικό bit είναι μέρος του μηνύματος και πιο όχι. Αυτό θα έχει σαν αποτέλεσμα να μην έχουμε την σωστή εξαγωγή του μηνύματος που κρύψαμε.

2.2.1.1 Αλγόριθμος της μεθόδου LSB

Η μέθοδος LSB μπορεί να χαρακτηριστεί ως ο πιο απλός αλγόριθμος στεγανογραφίας. Μπορεί να εφαρμοστεί σε οποιαδήποτε αριθμητική συλλογή δεδομένων σε ψηφιακή μορφή. Ας υποθέσουμε λοιπόν ότι $x[i] \in X = \{0,...,2^{n_c}-1\}$ είναι μια ακολουθία ακεραίων. Για παράδειγμα το $x[i]$ μπορεί να είναι μια «ελαφριά» ένταση του $i^{ου}$ εικονοστοιχείου σε μια 8-bit grayscale εικόνα $(n_c = 8)$ ή ένας δείκτης της χρωματιστής κλίμακα ενός GIF αρχείου $(n_c = 8)$. Ανάλογα με την μορφή της εικόνας κάθε $x[i]$ μπορεί να αναπαρασταθεί χρησιμοποιώντας n_c bits $b[i,1],...,b[i,n_c]$, [2]

$$x[i] = \sum_{k=1}^{n_c} b[i,k]2^{n_c-k} \quad (1)$$

Έτσι μπορούμε να σκεφτούμε μια ακολουθία $(b[i,1],...,b[i,n_c])$ σαν δυαδική αναπαράσταση του $x[i]$ σε big-endian μορφή (το πιο σημαντικό bit $b[i,1]$ είναι πρώτο). Η μέθοδος LSB είναι το τελευταίο bit $b[i,n_c]$.

Η μέθοδος LSB όπως αναφέραμε και στην προηγούμενη υποενότητα λειτουργεί αντικαθιστώντας το λιγότερο σημαντικό bit του $x[i]$ με το bit του μηνύματος $m[i]$, δημιουργώντας έτσι την στεγο-εικόνα $y[i]$. Ο παρακάτω αλγόριθμος παρουσιάζει ένα ψευδό-κώδικα που σαν στόχο έχει την ενσωμάτωση μιας ακολουθίας bit σε μια εικόνα κατά μήκος ενός

ψευδό-τυχαίου μονοπατιού που δημιουργείται από το μυστικό κλειδί που μοιράζονται τα δύο άτομα που θέλουν να επικοινωνήσουν [2].

Αλγόριθμος ενσωμάτωσης μηνύματος σε μια εικόνα κάλυψης

// Ξεκίνα δημιουργώντας ένα στεγο-κλειδί χρησιμοποιώντας την PRGN.

// Είσοδος: μήνυμα $m \in \{0,1\}^m$ εικόνα κάλυψης $x \in X^n$.

Path = Perm (n);

// Perm είναι μια ψευδό-τυχαία μετάθεση των $\{1,2,...,n\}$.

y = x;

m = min (m, n);

// Εάν το μήνυμα είναι μεγαλύτερο από την επιτρεπτή χωρητικότητα παριέκοψε το.

for I = 1 to m {

y [Path[i]] = x [Path[i]] + m[i] - x [Path[i]]mod2;

}

// Το y είναι η στεγο-εικόνα στην οποία είναι ενσωματωμένα τα bits του μηνύματος.

Θα πρέπει να προσθέσουμε σε αυτό το σημείο ότι σε μια έγχρωμη εικόνα ο αριθμός των στοιχείων στο αντικείμενο που χρησιμοποιείται για την κάλυψη είναι τρεις φορές μεγαλύτερος από τα στοιχεία μιας grayscale εικόνας. Ο προηγούμενος αλγόριθμος χρησιμοποιείται για την ενσωμάτωση του μυστικού μηνύματος μέσα στην εικόνα ενώ αυτός που ακολουθεί αναφέρεται στην εξαγωγή του μηνύματος από μια στεγο-εικόνα [2].

Αλγόριθμος εξαγωγής μηνύματος από μια στεγο-εικόνα.

// Ξεκίνα δημιουργώντας ένα στεγο-κλειδί χρησιμοποιώντας την PRGN.

// Είσοδος: στεγο-εικόνα $y \in X^n$

Path = Perm (n);

// Perm είναι μια ψευδό-τυχαία μετάθεση των $\{1,2,...,n\}$.

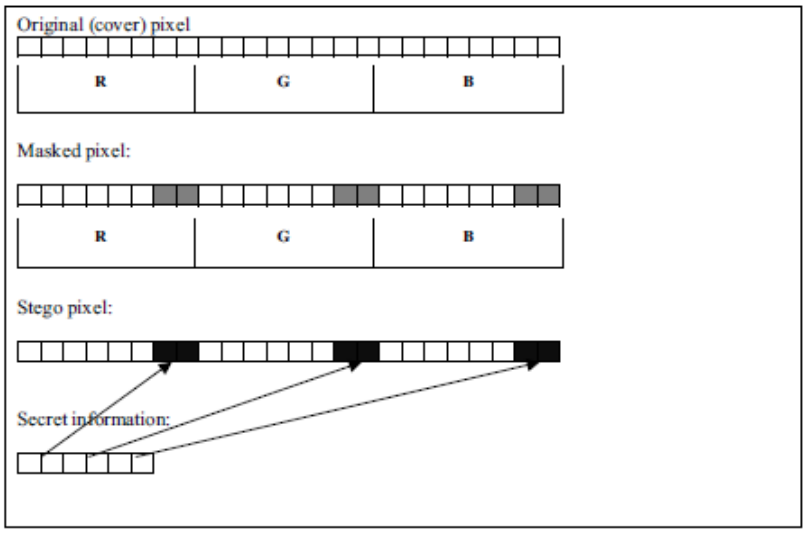
for I = 1 to m {

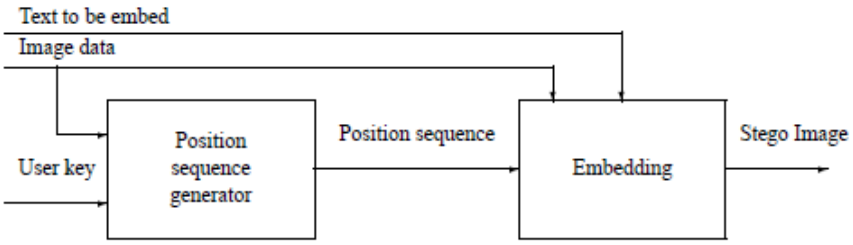
m[i] = y [Path[i]]mod2;

}

// m είναι το εξαγόμενο μήνυμα.

Στην συνέχεια ακολουθεί μια εικόνα η οποία περιγράφει με σχήματα την μέθοδο LSB.





Εικόνα 2.3 Σχηματική αναπαράσταση της μεθόδου LSB.
Πηγή: (Periodica Polytechica SER. EL. ENG. VOL. 44, NO. 3–4, PP. 249–258 (2000))

2.2.2 Τεχνική μετατροπής τομέα

Και αυτή η τεχνική της μετατροπής τομέα (transform domain techniques) είναι ιδιαίτερα αποτελεσματική και εύκολη στην χρήση της όπως η LSB. Η τεχνική αυτή έχει σαν στόχο να κρύψει το μυστικό μήνυμα σε μια «μεταβαλλόμενη περιοχή» ενός σήματος [1].

Πολλοί είναι οι άνθρωποι που χρησιμοποιούν το Διαδίκτυο καθημερινά με σκοπό να ανταλλάξουν φωτογραφίες μεταξύ τους. Η πιο κοινή μορφή φωτογραφιών είναι αυτή της JPEG και αυτό δεν είναι τυχαίο μιας και οι φωτογραφίες της μορφής JPEG συμπιέζονται από μόνες τους όταν πυκνώνουν. Για να πραγματοποιηθεί αυτή η διαδικασία «ξεφορτώνονται» τα πλεονάζοντα δεδομένα και τα πλεονάζοντα bits τα οποία θα εμπόδιζαν την φωτογραφία να συμπιεστεί. Κατά την διαδικασία της συμπίεσης, η φωτογραφία JPEG θα κάνει υπολογισμούς από μόνη της με σκοπό να γίνει μικρότερη σε μέγεθος. Αυτή η αλλαγή, αυτός ο υπολογισμός ονομάζεται «μεταβαλλόμενη περιοχή» (transform domain) και αυτή η αλλαγή μπορεί να χρησιμοποιηθεί για να κρύψουμε πληροφορία [1].

2.2.2.1 Αλγόριθμος της τεχνικής μετατροπής τομέα

Η τεχνική της μετατροπής τομέα κρύβει δεδομένα σε μαθηματικές συναρτήσεις οι οποίες βρίσκονται μέσα σε αλγορίθμους συμπίεσης. Η τεχνική Discrete Cosine Transform (DCT) είναι ένας πολύ κοινός αλγόριθμος μετατροπής τομέα ο οποίος εκφράζει μια κυματομορφή σαν ένα

σταθμισμένο ποσό συνημίτονων. Τα δεδομένα κρύβονται στα αρχεία της εικόνας με την αλλαγή του συντελεστή DCT της εικόνας. Συγκεκριμένα, οι συντελεστές DCT που μειώνονται κάτω από ένα συγκεκριμένο κατώτατο όριο αντικαθίστανται με τα μυστικά bits. Η λήψη της αντίστροφης μετατροπής θα δημιουργήσει την στεγο-εικόνα. Η διαδικασία εξαγωγής συνίσταται από την ανάκτηση εκείνων των συγκεκριμένων συντελεστών DCT [7].

Η τεχνική που αναλύσαμε παραπάνω βασίζεται στην τεχνική LSB η οποία αντικαθιστά περισσότερα από ένα bit κάθε εικονοστοιχείου για να κρύψει τα μυστικά δεδομένα. Αλλά η ασφάλεια του μυστικού μηνύματος μπορεί να ενισχυθεί με το συνδυασμό της τεχνικής του λιγότερου σημαντικού bit (LSB), της διακριτής μετατροπής συνημίτονου (DCT) και της τεχνικής συμπίεσης. Η τεχνική LSB χρησιμοποιείται για να κρύψει το μυστικό μήνυμα μέσα στην εικόνα κάλυψης με σκοπό να πάρουμε την στεγο-εικόνα. Η στεγο-εικόνα μετασχηματίζεται από τη χωρική περιοχή σε περιοχή συχνότητας χρησιμοποιώντας τη τεχνική DCT. Και τελικά ο αλγόριθμος συμπίεσης δεδομένων χρησιμοποιείται για τη συμπίεση της στεγο-εικόνα με σκοπό να ενισχύσουν την ασφάλεια της [8].

2.2.3 Τεχνική διάδοσης φάσματος

Η τεχνική διάδοσης φάσματος (spread spectrum technique) είναι μια άλλη κατηγορία στεγανογραφίας που χρησιμοποιείται για να συγκαλύψει πληροφορίες στο εσωτερικό ενός αρχείου κάλυψης και κυρίως ενός αρχείου ήχου. Η κατηγορία στεγανογραφίας spread spectrum technique χωρίζεται σε δύο είδη αυτή της direct sequence και αυτή της frequency hopping.

- **Direct Sequence**

Στην άμεση ακολουθία εξάπλωσης φάσματος (direct sequence spread spectrum), η ροή της πληροφορίας που πρόκειται να μεταδοθεί διαιρείται σε μικρά κομμάτια. Κάθε ένα από αυτά τα κομμάτια κατανέμεται σε ένα κανάλι συχνότητας του φάσματος. Το σήμα δεδομένων, κατά την διαδικασία της μετάδοσης, είναι συνδυασμένο με ένα bit ακολουθίας υψηλότερου ρυθμού το οποίο διαιρεί τα δεδομένα σε μια προαποφασισμένη αναλογία εξάπλωσης. Περιττά bit ακολουθίας υψηλότερου ρυθμού βοηθούν το σήμα τόσο στο να αντισταθεί στις παρεμβάσεις όσο και να ανακτηθεί το αυθεντικό σήμα στην περίπτωση όπου κάποιο από τα bits δεδομένων καταστραφεί κατά την διαδικασία της μετάδοσης [1].

- **Frequency Hopping**

Αυτή η τεχνική διαιρεί ένα ευρύ μερίδιο του φάσματος εύρους ζώνης (bandwidth) σε πολλές πιθανές συχνότητες μετάδοσης. Γενικά, οι συσκευές frequency-hopping χρησιμοποιούν τη λιγότερη δύναμη ενέργεια και είναι φτηνότερες, αλλά η απόδοση των άμεσων συστημάτων απλωμένου φάσματος ακολουθίας (direct sequence spread-spectrum) είναι συνήθως καλύτερη και πιο αξιόπιστη [1].

2.2.4 Τεχνική στατιστικής μεθόδου

Η στατιστική μέθοδος χρησιμοποιεί αυτό που ονομάζεται «1-bit» στεγανογραφικό σχέδιο. Αυτό το σχέδιο ενσωματώνει ένα bit πληροφορίας μόνο μέσα σε ένα ψηφιακό «ξενιστή» και με αυτό τον τρόπο δημιουργεί μια στατιστική αλλαγή, ακόμα και αν αυτή είναι μικρή.

Όταν πραγματοποιείται μια στατιστική αλλαγή στο αντικείμενο κάλυψης τότε υποδεικνύεται το «1» ενώ όταν το αντικείμενο αφήνεται αμετάβλητο τότε υποδεικνύεται το «0» Αυτό το σύστημα λειτουργεί βάση της δυνατότητας του δέκτη να διακρίνει μεταξύ των τροποποιημένων και όχι αντικειμένων κάλυψης [1].

2.2.5 Τεχνική παραμόρφωσης

Αυτή η μέθοδο στεγανογραφίας δημιουργεί μια αλλαγή στο αντικείμενο κάλυψης με σκοπό να κρυφτεί η πληροφορία η οποία θέλουμε. Το μυστικό μήνυμα ανακτάται όταν ο αλγόριθμος συγκρίνει το αλλαγμένο, διαστρεβλωμένο αντικείμενο κάλυψης με τον αρχικό [1].

2.2.6 Τεχνική παραγωγής αντικειμένου κάλυψης

Η τεχνική παραγωγής αντικειμένου κάλυψης (cover generation method) είναι πιθανόν η πιο περίεργη μέθοδος στεγανογραφίας από όλες. Χαρακτηριστικά, ένα αντικείμενο κάλυψης επιλέγεται για να κρύψει ένα μήνυμα. Ωστόσο αυτό το οποίο είναι περίεργο σε αυτή τη μέθοδο είναι ότι η Cover generation method δημιουργεί από μόνη της ένα αντικείμενο κάλυψης με αποκλειστικό σκοπό το κρύψιμο των πληροφοριών [1].

2.3 Τύποι στεγανογραφίας

Στο υποκεφάλαιο αυτό θα παρουσιάσουμε τους δύο τύπους στεγανογραφίας που υπάρχουν μέχρι σήμερα και αυτοί είναι οι εξής [1]:

- Η γλωσσολογική στεγανογραφία.
- Η τεχνική στεγανογραφία.

2.3.1 Γλωσσολογική στεγανογραφία

Η γλωσσολογική στεγανογραφία μπορεί να χαρακτηριστεί ως η πιο εύκολη απ' όλες τις μορφές στεγανογραφίας. Το όνομά της οφείλεται στο γεγονός ότι χρησιμοποιεί την γλώσσα (ένα κείμενο) ως μέσο κάλυψης. Υπάρχουν δύο βασικές κατηγορίες γλωσσολογικής στεγανογραφίας: αυτή του ανοικτού κώδικα (open code) και αυτή του συμβολισμού μέσα σε κείμενα (text semagrams) [1].

Το Nicetext είναι ένα πρόγραμμα το οποίο χρησιμοποιεί τα οφέλη της γλωσσολογικής στεγανογραφίας με έναν εφευρετικό τρόπο. Στόχος του προγράμματος αυτού είναι να μετατρέψει ένα κρυπτογραφημένο κείμενο, σε κείμενο το οποίο να μοιάζει κατά πολύ στη φυσική γλώσσα που χρησιμοποιούμε παρέχοντας ταυτόχρονα κάλυψη στο κρυπτογραφημένο κείμενο [1].

2.3.1.1 Ανοικτός κώδικας

Στην περίπτωση του ανοιχτού κώδικα (open code), τα κείμενα που δημιουργούνται είναι πολύ καλά κατασκευασμένα. Περιέχουν συγκεκριμένες λέξεις ή προτάσεις, των οποίων τα γράμματα τοποθετούνται σε συγκεκριμένα μέρη μέσα στο κείμενο, ενώ οι λέξεις μπορούν να είναι κρυμμένες σε οριζόντια ή κάθετη θέση [1].

2.3.1.2 Σύμβολα κειμένου

Τα σύμβολα κειμένου (text semagrams) αναφέρονται σε γραφικές τροποποιήσεις του κειμένου, δηλαδή τελείες στίγματα κ. λ. π. τα οποία περιέχουν πληροφορίες που είναι πολύ μικροσκοπικές αλλά ορατές. Εκτός από τα σύμβολα κειμένου υπάρχουν και τα σκέτα σύμβολα (semagrams) τα οποία δεν χρησιμοποιούνται μέσα σε κείμενο [1].

2.3.2 Τεχνική στεγανογραφία

Η τεχνική στεγανογραφία δεν έχει απαραιτήτως άμεση σχέση με τη γραπτή λέξη ακόμα κι αν μεταβιβάζει πληροφορίες. Η τεχνική στεγανογραφία είναι η μέθοδος στεγανογραφίας όπου ένα εργαλείο, μια συσκευή, ή μια μέθοδος χρησιμοποιούνται για να κρύψουν το μυστικό μήνυμα. Στην πραγματικότητα, η γλωσσολογική στεγανογραφία θα μπορούσε να θεωρηθεί τεχνική στεγανογραφία επειδή είναι μια μέθοδος. Μερικές μεθόδους τεχνικής στεγανογραφίας είναι το αόρατο μελάνι, τα Microdots κ. λ. π. [1]

2.4 Τύποι στεγανογραφικών πρωτοκόλλων

Στις μέρες μας η επικοινωνία μεταξύ των ανθρώπων και των οργανισμών γίνεται κατά κύριο λόγο χρησιμοποιώντας τηλέφωνο, fax, ραδιόφωνο και ηλεκτρονικούς υπολογιστές. Το βασικό χαρακτηριστικό όμως είναι η ασφάλεια της επικοινωνίας. Έχοντας λοιπόν, αναλύσει τις κατηγορίες και τους τύπους της στεγανογραφίας, κλείνουμε αυτό το κεφάλαιο παρουσιάζοντας τους τρεις τύπους στεγανογραφικών πρωτοκόλλων που υπάρχουν και οι οποίοι είναι οι εξής [10]:

- Καθαρή Στεγανογραφία (Pure Steganography).
- Μυστικού Κλειδιού Στεγανογραφία (Secret Key Steganography).
- Δημόσιου Κλειδιού Στεγανογραφία (Public Key Steganography).

2.4.1 Καθαρή στεγανογραφία

Καθαρή στεγανογραφία ονομάζουμε εκείνο το στεγανογραφικό σύστημα το οποίο δεν έχει την ανάγκη ανταλλαγής στεγο-κλειδιού. Αυτή η μέθοδος στεγανογραφίας παρέχει πολύ μικρή ασφάλεια μιας και η επικοινωνία μεταξύ ενός αποστολέα και ενός παραλήπτη βασίζεται μόνο στο γεγονός ότι κανένας άλλος κακόβουλος δεν έχει γνώση του μυστικού μηνύματος. Η χρησιμοποίηση αυτού του τύπου στεγανογραφικού πρωτοκόλλου είναι απαγορευμένη, όταν η επικοινωνία γίνεται μέσω του Διαδικτύου [6].

Η καθαρή στεγανογραφία μπορεί να οριστεί από μια τετράδα (C M, D και E) όπου [10]:

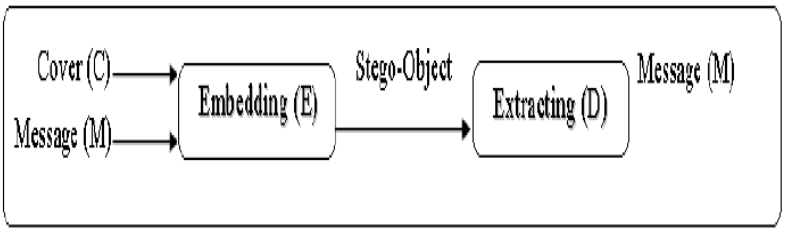
C είναι ένα σύνολο πιθανόν αντικειμένων κάλυψης,

M είναι ένα σύνολο μυστικού μηνύματος με $|C| \geq |M|$,

E είναι η συνάρτηση ενσωμάτωσης $CxM \rightarrow C$,

D είναι η συνάρτηση εξαγωγής $C \rightarrow M$ με την προϋπόθεση ότι $D(E(c,m)) = m$ για κάθε $m \in M$ και $c \in C$.

Η παρακάτω εικόνα παρουσιάζει γραφικά την καθαρή στεγανογραφία.



Εικόνα 2.4 Αναπαράσταση καθαρής στεγανογραφίας (Pure Steganography).
Πηγή: (JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010)

2.4.2 Μυστικού κλειδιού στεγανογραφία

Στεγανογραφία μυστικού κλειδιού ονομάζουμε το στεγανογραφικό σύστημα το οποίο απαιτεί την ανταλλαγή μυστικού κλειδιού πριν από την αρχή της επικοινωνίας. Η στεγανογραφία μυστικού κλειδιού λαμβάνει ένα αντικείμενο κάλυψης και ενσωματώνει το μυστικό μήνυμα χρησιμοποιώντας το μυστικό κλειδί (στεγο-κλειδί). Μόνο τα άτομα τα οποία έχουν το μυστικό κλειδί μπορούν να αντιστρέψουν την διαδικασία που περιγράψαμε πιο πάνω και να πάρουν το μυστικό μήνυμα. Σε σχέση με την καθαρή στεγανογραφία, η στεγανογραφία μυστικού κλειδιού είναι δύσκολο να παρεμποδιστεί. Το όφελος της στεγανογραφίας μυστικού κλειδιού είναι ότι ακόμα κι αν παρεμποδιστεί η επικοινωνία μεταξύ δύο ατόμων από ένα τρίτο κακόβουλο άτομο,

μόνο τα συμβαλλόμενα μέρη που ξέρουν το μυστικό κλειδί μπορούν να εξαγάγουν το μυστικό μήνυμα [9].

Η στεγανογραφία μυστικού κλειδιού μπορεί να οριστεί από μια πεντάδα (C, M, K, DK,EK) όπου [10]:

C είναι ένα σύνολο πιθανόν αντικειμένων κάλυψης,

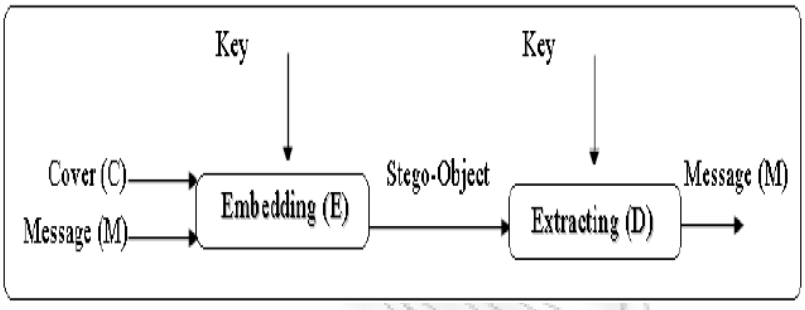
M είναι ένα σύνολο μυστικού μηνύματος,

K είναι το σύνολο των μυστικών κλειδιών,

EK είναι η συνάρτηση ενσωμάτωσης $CxMxK \to C$,

DK είναι η συνάρτηση εξαγωγής με την προϋπόθεση ότι $D(EK(c,m,k),k) = m$ για κάθε $m \in M$, $c \in C$ και $k \in K$.

Η παρακάτω εικόνα παρουσιάζει γραφικά την στεγανογραφία μυστικού κλειδιού.



Εικόνα 2.5 Αναπαράσταση στεγανογραφίας μυστικού κλειδιού (Secret Key Steganography). Πηγή: (JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010)

2.4.3 Δημοσίου κλειδιού στεγανογραφίας

Στεγανογραφία δημοσίου κλειδιού ονομάζουμε το στεγανογραφικό σύστημα το οποίο χρησιμοποιεί ένα δημόσιο και ένα ιδιωτικό κλειδί με σκοπό να διασφαλίσει την επικοινωνία μεταξύ δύο ατόμων που θέλουν να επικοινωνήσουν μυστικά. Ο αποστολές θα χρησιμοποιήσει το δημόσιο κλειδί κατά την διαδικασία της κρυπτογράφησης με σκοπό να κρυπτογραφήσει το μυστικό μήνυμα. Μόνο το ιδιωτικό κλειδί που έχει μια άμεση μαθηματική σχέση με το δημόσιο κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα. Η στεγανογραφία δημοσίου κλειδιού παρέχει ένα πιο εύρωστο τρόπο εφαρμογής της στεγανογραφίας. Επιπλέον αυτός ο τύπος πρωτοκόλλου στεγανογραφίας παρέχει μια πολύ-επίπεδη ασφάλεια δεδομένου ότι το κακόβουλο άτομο που θέλει να βρει το μυστικό μήνυμα πρέπει πρώτα να υποπτευθεί την χρήση στεγανογραφίας και μετά να βρει τρόπο να σπάσει τον αλγόριθμο [9].

2.4 Συμπεράσματα

Η στεγανογραφία είναι μια τέχνη που προσφέρει πολλούς τρόπους ασφάλειας του μυστικού μηνύματος. Δύο άτομα τα οποία θέλουν να επικοινωνήσουν μυστικά θα πρέπει να αναζητήσουν το κατάλληλο στεγανογραφικό σύστημα που θα τους δώσει την μέγιστη ασφάλεια. Παρ όλα αυτά θα πρέπει να επισημάνουμε ότι όσο πιο ασφαλές είναι ένα στεγανογραφικό σύστημα τόσο πιο μικρό θα είναι και το μήνυμα που μπορούν να ανταλλάξουν τα δύο άτομα αυτά.

Επίσης θα πρέπει να επισημάνουμε ότι το καλύτερο αντικείμενο κάλυψης για ένα στεγανογραφικό σύστημα είναι μια εικόνα και μάλιστα μια εικόνα grayscale. Κι αυτό γιατί σε μια τέτοια εικόνα μπορεί να χρησιμοποιηθεί καλύτερα και πιο γρήγορα ο αλγόριθμος LSB με τρόπο τέτοιο ώστε οι τυχόν αλλοιώσεις στην εικόνα να είναι μηδαμινές. Έτσι δύσκολα θα γίνει αντιληπτή η χρήση μεθόδου στεγανογραφίας από κάποιον κακόβουλο.

Βιβλιογραφία

[1] Gregory Klipper,“Investigator's Guide to Steganography”, Auerbach Puplication 2003.

[2] Jessica Fridrich “Steganography in Digital Media” Cambridge University Press 2010.

[3] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, “Information hiding-Survey”, IEEE, 87(7):1062-1078, 1999.

[4] Mastronardi, G., Castellano, M. Marino, “Intelligent Data Acquisition and Advanced Computing Systems” IEEE,11:116 – 119, 2003.

[5] M. Shirali-Shahreza and M.H. Shirali-Shahreza, “An Improved Version of Persian/Arabic Text Steganography Using "La” Word’” Proceedings of the 6th National Conference on Telecommunication Technologies 2008 (NCTT 2008), Malaysia, August 26–28, 2008.

[6] Johnson, Neil F., “Steganography” 2000, [http://www.jjtc.com/stegdoc.index2.html]

[7] Ying Wang, Moulin, P, “Statistical Signal Processing” , IEEE, 56(11) : 339 – 342, 2003.

[8] Nameer N. EL-Emam, “Hiding a Large Amount of Data with High Security Using Steganography Algorithm” Jordan Journal of Science publications, 3 (4): 223-232, 2007.

[9] Bender, W., Gruhl D., IBM Systems Journal “Techniques for Data Hiding”, [http://www.research.ibm.com/journal/sj/mit/sectiona/bender.pdf].

[10] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi ‘‘Overview: Main Fundamentals for Steganography’’, Journal Of Computing, Volume 2, Issue 3, March 2010, ISSN 2151-9617

Κεφάλαιο 3

Στεγανογραφικό σύστημα

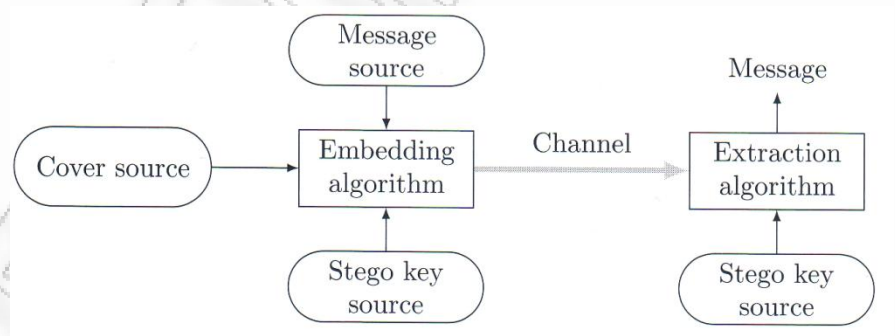
3.1 Εισαγωγή στο στεγανογραφικό σύστημα

Κύριος στόχος της στεγανογραφίας είναι η μετάδοση μυστικών μηνυμάτων μεταξύ δύο οντοτήτων χωρίς να γίνεται φανερό το γεγονός, ότι ένα μυστικό μεταδίδεται. Αυτό μπορεί να επιτευχθεί αρχικά με το κρύψιμο μηνυμάτων σε αντικείμενα τα οποία είναι συνηθισμένα στην καθημερινότητα όπως για παράδειγμα οι εικόνες, και έπειτα με την αποστολή τους με ένα απλό τρόπο μέσω ενός καναλιού μετάδοσης.

Προτού δύο οντότητες ξεκινήσουν να επικοινωνούν μυστικά θα πρέπει πρώτα να συμφωνήσουν πάνω σε ένα βασικό επικοινωνιακό πρωτόκολλο το οποίο θα ακολουθούν στο μέλλον. Στην πραγματικότητα αυτό για το οποίο αρχικά καλούνται να διαλέξουν είναι ο τύπος των αντικειμένων κάλυψης που θα χρησιμοποιήσουν για να στείλουν τα μυστικά μηνύματα ο ένας στον άλλο. Στην συνέχεια χρειάζεται να σχεδιάσουν τόσο τον αλγόριθμο που θα χρησιμοποιηθεί για την ενσωμάτωση του μηνύματος μέσα στο αντικείμενο κάλυψης όσο και τον αλγόριθμο για την εξαγωγή του μηνύματος. Η δημιουργία αλγορίθμων οι οποίοι εξαρτώνται από το μυστικό κλειδί αυξάνουν την ασφάλεια, κι αυτό γιατί κανένας άλλος εκτός από το άτομο που διαθέτει το μυστικό κλειδί δεν μπορεί να διαβάσει το μυστικό μήνυμα. Επιπλέον, εκτός από τα αντικείμενα κάλυψης και τους στεγανογραφικούς αλγόριθμους αυτό στο οποίο πρέπει να δώσει κανείς ιδιαίτερη προσοχή είναι το μέγεθος του μυστικού μηνύματος. Όσο πιο μικρό τόσο πιο δύσκολο είναι για έναν κακόβουλο να ανακαλύψει την μυστική επικοινωνία. Τέλος, θα πρέπει να προσεχθεί ιδιαίτερα το στεγανογραφικό κανάλι από το οποίο θα μεταδοθεί το μυστικό μήνυμα.

Όπως μπορούμε να διαπιστώσουμε και από την παρακάτω εικόνα πέντε είναι τα βασικά στοιχεία ενός στεγο-συστήματος:

- Πηγή των αντικειμένων κάλυψης.
- Αλγόριθμοι ενσωμάτωσης δεδομένων και εξαγωγής τους.
- Πηγή στεγο-κλειδιών.
- Πηγή μηνυμάτων.
- Κανάλι επικοινωνίας που χρησιμοποιείται για την ανταλλαγή των μηνυμάτων.



Εικόνα 3.1 Βασικά στοιχεία ενός στεγανογραφικού καναλιού.

Πηγή: (Steganography in digital media)

Η πηγή των αντικειμένων κάλυψης μπορεί να είναι μια ψηφιακή εικόνα, ένα ψηφιακό βίντεο ή ακόμα και ένα μουσικό αρχείο mp3. Ωστόσο εμείς θα θεωρήσουμε σαν πηγή δεδομένων την ψηφιακή εικόνα μιας και στο τελευταίο κεφάλαιο μας την χρησιμοποιήσουμε σαν αντικείμενο κάλυψης [1].

Ο αλγόριθμος ενσωμάτωσης είναι μια διαδικασία μέσω της οποίας ο αποστολέας καθορίζει την εικόνα με την βοήθεια της οποίας θα μεταδοθεί το μυστικό μήνυμα. Η διαδικασία αυτή βασίζεται στο στεγο-κλειδί. Αυτό το κλειδί είναι απαραίτητο για την σωστή εξαγωγή του μηνύματος από την στεγο-εικόνα. Για παράδειγμα, ο αποστολέας μπορεί να ενσωματώσει την μυστική ακολουθία bit σαν το λιγότερο σημαντικό bit των εικονοστοιχείων διαλέγοντας ένα ψευδό-τυχαίο μονοπάτι μέσα από στην εικόνα [1].

Το πρωτόκολλο, που θα χρησιμοποιήσει τόσο ο αποστολέας όσο και ο παραλήπτης, για την επιλογή του στεγο-κλειδιού, διαμορφώνεται συνήθως με μια τυχαία μεταβλητή από το χώρο όλων των κλειδιών. Μια λογική στρατηγική είναι να επιλεγεί το στεγο-κλειδί τυχαία από ένα σύνολο όλων των πιθανών στεγο-κλειδιών [1].

Η πηγή των μηνυμάτων έχει σημαντική επιρροή στην ασφάλεια του στεγανογραφικού καναλιού. Ας θεωρήσουμε δύο ακραίες καταστάσεις. Η πρώτη περίπτωση επιτρέπει στις δύο οντότητες που επικοινωνούν να μεταδίδουν ένα μικρό μήνυμα, για παράδειγμα 16 bits σε κάθε στεγο-εικόνα. Η δεύτερη περίπτωση αναφέρεται στην επιθυμία των δύο οντοτήτων να μεταδίδουν όσο το δυνατόν μεγαλύτερα μηνύματα και να ενσωματώνουν στην στεγο-εικόνα τόσα bits όσα επιτρέπει ο αλγόριθμος που χρησιμοποιούν. Όπως μπορούμε να συμπεράνουμε η δεύτερη περίπτωση κρύβει μεγαλύτερο κίνδυνο ως προς την ασφάλεια του μεταδιδόμενου μυστικού μηνύματος. Η διανομή των μηνυμάτων μπορεί να διαμορφωθεί χρησιμοποιώντας μια τυχαία μεταβλητή από το διάστημα όλων πιθανών μηνυμάτων [1].

Ας θεωρήσουμε τώρα ότι το πραγματικό κανάλι μετάδοσης που χρησιμοποιείται για την αποστολή εικόνων παρακολουθείται από μια κακόβουλη οντότητα. Η οντότητα αυτή μπορεί να πάρει τρεις διαφορετικούς ρόλους. Ο πρώτος ρόλος είναι αυτός του παθητικού παρατηρητή. Σε αυτό τον ρόλο η κακόβουλη οντότητα απλά επιθεωρεί μόνο την κίνηση στο μεταδιδόμενο κανάλι και δεν παρεμβαίνει σε αυτή. Ο δεύτερος ρόλος είναι αυτός του ενεργού παρατηρητή. Στην περίπτωση αυτή η κακόβουλη οντότητα υποψιάζεται την χρήση της στεγανογραφίας και προληπτικά επιχειρεί να διακόψει το στεγανογραφικό κανάλι παραμορφώνοντας τις εικόνες που στέλνουν οι δύο οντότητες. Για παράδειγμα συμπιέζει την εικόνα χρησιμοποιώντας JPEG, ή αλλάζει το μέγεθος ή κόβει την εικόνα κ. λ. π. Στην περίπτωση όπου οι δύο οντότητες δεν χρησιμοποιούν ανθεκτική στεγανογραφία, το στεγανογραφικό κανάλι θα σπάσει από αυτές τις ενέργειες της κακόβουλης οντότητας. Τέλος ο τρίτος ρόλος της κακόβουλης οντότητας είναι αυτή του «δόλιου παρατηρητή». Ουσιαστικά προσπαθεί να μαντέψει την στεγανογραφική μέθοδο που χρησιμοποιούν οι δύο οντότητες και επιχειρεί να μιμηθεί μια από τις δύο οντότητες με σκοπό να τις μπερδέψει [4].

Η διαφορά μεταξύ του ενεργού παρατηρητή και του δόλιου παρατηρητή είναι μεγάλη. Στην περίπτωση του ενεργού παρατηρητή η κακόβουλη οντότητα προσπαθεί απλά να διακόψει την επικοινωνία μπλοκάροντας το στεγανογραφικό κανάλι ενώ στη περίπτωση του «δόλιου παρατηρητή» προσπαθεί να χρησιμοποιήσει το στεγανογραφικό κανάλι προς όφελός του είτε χρησιμοποιείται στεγανογραφία είτε όχι. Ο πιο κοινός ρόλος μιας κακόβουλης οντότητας είναι αυτός του ενεργού παρατηρητή μιας και τα κανάλια επικοινωνίας είναι error-free [4].

Οι αλγόριθμοι ενσωμάτωσης και εξαγωγής αποτελούν τα πιο σημαντικά μέρη ενός στεγο-συστήματος. Οι στεγανογραφικοί αλγόριθμοι αξιοποιούν τρεις διαφορετικές βασικές αρχιτεκτονικές οι οποίες προσδιορίζουν τον εσωτερικό μηχανισμό για τους αλγόριθμους ενσωμάτωσης και εξαγωγής. Η οντότητα που στέλνει το μυστικό μήνυμα μπορεί να πραγματοποιήσει την ενσωμάτωση διαλέγοντας μια εικόνα κάλυψης η οποία έχει ήδη το επιθυμείτο μυστικό μήνυμα μέσα της. Αυτή η στεγανογραφία ονομάζεται στεγανογραφία επιλογής αντικειμένου κάλυψης (steganography by cover selection). Μια εναλλακτική στεγανογραφία είναι αυτή, κατά την οποία η οντότητα μπορεί να δημιουργήσει ένα αντικείμενο το οποίο περιέχει το μυστικό μήνυμα. Αυτή η στρατηγική ονομάζεται στεγανογραφία δημιουργίας αντικειμένου κάλυψης (steganography by cover synthesis). Τέλος η τρίτη επιλογή είναι η στεγανογραφία τροποποίησης του αντικειμένου κάλυψης (steganography by cover modification). Αυτή η μορφή στεγανογραφίας είναι η πιο κοινή μιας και επιτρέπει την μετάδοση μεγάλων μηνυμάτων. Και τις τρεις αυτές κατηγορίες που χρησιμοποιούνται στα στεγανογραφικά κανάλια θα τις εξετάσουμε αναλυτικά στις παρακάτω υποενότητες [1].

3.2 Στεγανογραφία επιλογής αντικειμένου κάλυψης

Στην στεγανογραφία επιλογής αντικειμένου κάλυψης, η οντότητα που στέλνει το μυστικό μήνυμα έχει στην διάθεσή της μια σταθερή βάση δεδομένων με εικόνες από την οποία μπορεί να διαλέξει αυτή η οποία περιέχει το επιθυμείτο μήνυμα. Για παράδειγμα ένα bit πληροφορίας μπορεί να σταλεί από την επιλογή μιας εικόνας που απεικονίζει ένα τοπίο. Εναλλακτικά, η εμφάνιση ενός ζώου σε μια εικόνα μπορεί να έχει μια κρυφή ερμηνεία όπως για παράδειγμα «συνάντηση σε μια ώρα». Ο αλγόριθμος ενσωμάτωσης μπορεί να λειτουργεί απλά τραβώντας τυχαία εικόνες από την βάση δεδομένων μέχρι να βρεθεί η κατάλληλη που περιέχει το επιθυμητό μήνυμα για μετάδοση. Το στεγο-κλειδί είναι πολύ σημαντικό στην συγκεκριμένη περίπτωση γιατί θέτει ένα σύνολο κανόνων, βάση των οποίων ερμηνεύονται οι εικόνες [1].

Μια σημαντική περίπτωση της στεγανογραφίας επιλογής αντικειμένου κάλυψης είναι αυτή που εμπλέκει μήνυμα συναρτήσεων κατακερματισμού (hash functions) ή αλλιώς μήνυμα σύνοψης. Η οντότητα που στέλνει το μυστικό μήνυμα διαλέγει μια εικόνα από την βάση δεδομένων και εφαρμόζει σε αυτή ένα μήνυμα συνάρτησης κατακερματισμού. Εάν το μήνυμα συνάρτησης κατακερματισμού ταιριάζει με την επιθυμητό πλήθος bit του μυστικού μηνύματος η εικόνα προωθείται στην οντότητα που λαμβάνει το μυστικό μήνυμα. Σε αντίθετη περίπτωση επιλέγεται μια διαφορετική εικόνα μέχρι να επιτευχτεί το επιθυμητό ταίριασμα. Ο αριθμός των επαναλήψεων που χρειάζονται μέχρι να βρεθεί το ταίριασμα εξαρτάται αποκλειστικά από το μήκος του μηνύματος συνάρτησης κατακερματισμού. Όταν η οντότητα παραλήπτης λάβει την εικόνα απλά εξάγει το μήνυμα συνάρτησης κατακερματισμού με σκοπό να διαβάσει το μυστικό μήνυμα. Το πλεονέκτημα αυτής της προσέγγισης είναι ότι το αντικείμενο κάλυψης είναι απόλυτα φυσικό χωρίς να έχει υποστεί καμία αλλαγή. Ωστόσο το μειονέκτημα είναι το πολύ μικρό ωφέλιμο φορτίο [1] [3]. Δηλαδή τα μηνύματα είναι πολύ μικρά σε μέγεθος.

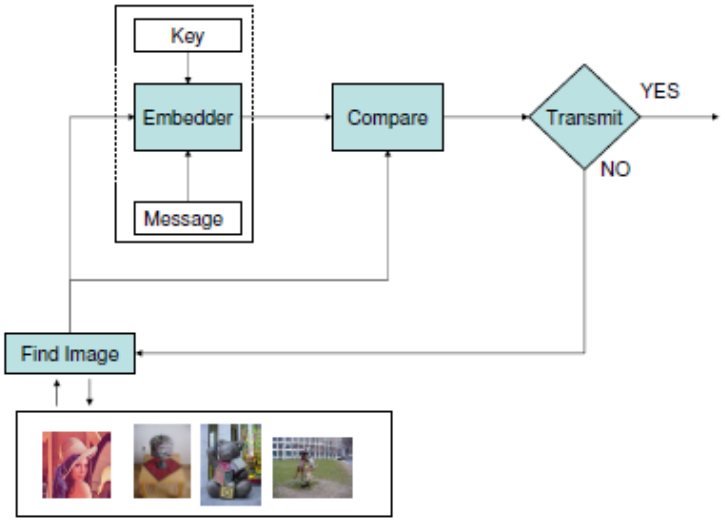
Ένα πιθανό πρόβλημα που έχει η στεγανογραφία επιλογής αντικειμένου κάλυψης είναι ότι δεν μπορεί να χαρακτηριστεί ως απόλυτα μη αναγνωρίσιμη. Με άλλα λόγια είναι εύκολο για την κακόβουλη οντότητα να εντοπίσει την χρήση στεγανογραφίας. Για να γίνει αυτό ακόμα πιο κατανοητό, χρησιμοποιούμε μια πολύ απλή συνάρτηση κατακερματισμού σχηματιζόμενη από τα λιγότερο σημαντικά bits των τριών πρώτων εικονοστοιχείων της εικόνας,

$$h(x) = \{x[1] \bmod 2, x[2] \bmod 2, x[3] \bmod 2\} \quad (1).$$

Παρατηρούμε ότι η συνάρτηση κατακερματισμού αποτελείται από τρία bits. Το πρόβλημα θα προκύψει όταν οι οντότητες αποφασίσουν ότι θα χρησιμοποιήσουν αυτή την τεχνική για να επικοινωνήσουν όχι μόνο μία φορά αλλά συνέχεια. Εάν η οντότητα που στέλνει το μυστικό μήνυμα, στείλει κάθε τριάδα των bits από τις οκτώ συνολικά πιθανές τριάδες των bits, τότε οι στεγο-εικόνες που στέλνονται από αυτή, θα παράγουν οποιαδήποτε από τις τριάδες των 8 bits σαν συνάρτηση κατακερματισμού. Το πρόβλημα εδώ όμως είναι ότι δεν ξέρουμε εάν η κατανομή που χρησιμοποιούμε παραπάνω είναι ίδια με την κατανομή των λιγότερο σημαντικών bits των τριών πρώτων εικονοστοιχείων μιας φυσικής εικόνας στην αριστερή πάνω γωνία. Για παράδειγμα εάν χρησιμοποιήσουμε μια εικόνα και αυτά τα εικονοστοιχεία είναι ένα κομμάτι ουρανού τότε η τιμή του ενός εικονοστοιχείου εξαρτάται άμεσα από του άλλου [1].

Αυτό το πρόβλημα προέκυψε επειδή θεωρήσαμε ότι το στεγανογραφικό κανάλι θα χρησιμοποιηθεί πολλές φορές επιτρέποντας έτσι στην κακόβουλη οντότητα να αντιληφτεί την ανταλλαγή μηνυμάτων. Αυτό θα μπορούσε να είχε αποφευχθεί εάν χρησιμοποιήσουμε μια εικόνα την φορά [1].

Η παρακάτω εικόνα παρουσιάζει ένα διάγραμμα επιλογής αντικειμένου κάλυψης.



Εικόνα 3.2 Διάγραμμα παρουσίασης για επιλογή αντικειμένου κάλυψης.
Πηγή: (Cover Selection For Steganographic Embedding)

3.3 Στεγανογραφία δημιουργίας αντικειμένου κάλυψης

Στην στεγανογραφία δημιουργίας αντικειμένου κάλυψης, η οντότητα που στέλνει το μυστικό μήνυμα δημιουργεί το αντικείμενο κάλυψης έτσι ώστε να περιλαμβάνει το επιθυμητό μήνυμα. Παράδειγμα τέτοιου είδους στεγανογραφίας είναι τα βίντεο του Bin Laden τα οποία πιστεύεται ότι περιέχουν κρυμμένα μηνύματα επικοινωνίας. Τα μηνύματα απορρέουν από τον τρόπο με το οποίο στέκεται, από τα ρούχα τα οποία φοράει ή ακόμα και από τις λέξεις που χρησιμοποιεί στην ομιλία του [2].

Η στεγανογραφία δημιουργίας αντικειμένου κάλυψης μπορεί να συνδυαστεί με την στεγανογραφία επιλογής αντικειμένου κάλυψης με σκοπό την μείωση της πολυπλοκότητας ενσωμάτωσης. Ας θεωρήσουμε ότι μπορούμε να πάρουμε ένα μεγάλο αριθμό από εικόνες με ακριβώς το ίδιο φόντο, οι οποίες προέρχονται από την ίδια φωτογραφική κάμερα. Για να πραγματοποιηθεί αυτό τοποθετούμε την φωτογραφική κάμερα πάνω σε ένα τρίποδο και παίρνουμε πολλαπλές φωτογραφίες με σταθερές συνθήκες φωτισμού. Υποθέτουμε ότι οι φωτογραφίες είναι 8 bit grayscale με $x_j[i]$ σταθερό για την ένταση του iου εικονοστοιχείου της jης εικόνας με $i = 1,...,n$ και $j = 1,...,K$. Μπορούμε πια να παρατηρήσουμε ότι η ένταση του φωτός ποικίλει σε ένα σταθερό εικονοστοιχείο, i , όταν παρατηρήσουμε όλες τις εικόνες j. Αυτό οφείλεται σε διάφορους θορύβους που παρουσιάζονται στις εικόνες [1].

Ας υποθέσουμε ότι η οντότητα που στέλνει το μυστικό μήνυμα θα χρησιμοποιήσει μια τροποποιημένη συνάρτηση κατακερματισμού με σκοπό να επιστρέφει 4 bits όταν απευθύνεται σε 16 εικονοστοιχεία. Για παράδειγμα θα μπορούσε να χρησιμοποιήσει τα τελευταία 4 bits από μια συνάρτηση κατακερματισμού MD5. Για να ενσωματώσει το μυστικό μήνυμα θα χωρίσει κάθε εικόνα σε κομματιασμένα μπλοκ των 4*4 εικονοστοιχείων και θα δημιουργήσει μια νέα εικόνα κατά τέτοιο τρόπο ώστε κάθε ένα 4*4 μπλοκ να περιέχει 4 bits του μηνύματος. Για να ενσωματώσει τα 4 πρώτα bits στο πρώτο 4*4 μπλοκ των εικονοστοιχείων θα αναζητήσει ανάμεσα στις συναρτήσεις κατακερματισμού των εικόνων $h(x_j[1],...x_j[16])$ όπου $j \in \{1,2,...,K\}$ μέχρι να βρει ένα ταίριασμα ανάμεσα στη συνάρτηση κατακερματισμού των 16 πρώτων εικονοστοιχείων και του μηνύματος. Με τον ίδιο ακριβώς τρόπο θα συνεχίσει και για τα υπόλοιπα μπλοκ. Η τελική στεγο-εικόνα y θα είναι ένα «μωσαϊκό» που θα αποτελείται από μπλοκ των διάφορων εικόνων

$$y = (x_{j1}[1],...x_{j1}[16], x_{j2}[17],...x_{j2}[32]x_{j3}[33],...)$$

Η πιθανότητα εύρεσης ταιριάσματος σε ένα συγκεκριμένο μπλοκ ανάμεσα σε όλα είναι $1-(1-1/16)^K$ όπου K είναι ο αριθμός των εικόνων. Από την άλλη μεριά η πιθανότητα να ενσωματωθεί όλο το μυστικό μήνυμα το οποίο αποτελείται από $n/16$ μπλοκ των 4 bits είναι $n/16$. Εάν αυξήσουμε τον αριθμό των εικόνων η πιθανότητα αυτή πλησιάζει το 1. Για παράδειγμα ένα μπλοκ εικόνας $n = 512x512$ και μόνο με $K = 400$ εικόνες η πιθανότητα είναι 0.99999 [1].

Η μέθοδο που μόλις περιγράψαμε είναι κυρίως θεωρητική παρά πρακτική. Και αυτό διότι είναι πολύ δύσκολο να έχουμε πολλαπλές ίδιες εικόνες.

Η ποιοτική διαφορά μεταξύ στεγανογραφίας επιλογής αντικειμένου κάλυψης και στεγανογραφίας δημιουργίας αντικειμένου κάλυψης ονομάζεται data masking. Όλα τα εργαλεία στεγανάλυσης είναι αυτόματα και λειτουργούν με σκοπό να εξάγουν ένα σύνολο αριθμητικών χαρακτηριστικών από την στεγο-εικόνα, τα οποία αργότερα θα αναλυθούν για να εντοπιστεί η πιθανή συμβατότητα με τα χαρακτηριστικά μιας κανονικής ίδιας εικόνας Επομένως το μόνο που χρειάζεται να κάνει η οντότητα που στέλνει το μήνυμα για να αποφύγει τον εντοπισμό χρήσης στεγανογραφίας είναι να μετατρέψει τα χαρακτηριστικά της στεγο-εικόνας με σκοπό να μοιάζουν πάρα πολύ με αυτά της αληθινής εικόνας [1].

Επομένως αυτό στο οποίο πρέπει να δώσει ιδιαίτερη προσοχή η οντότητα που στέλνει το μυστικό μήνυμα είναι να μοιάζει η στεγο-εικόνα πάρα πολύ με την φυσική εικόνα έτσι ώστε η κακόβουλη οντότητα να μην μπλοκάρει το στεγανογραφικό κανάλι και διακόψει την επικοινωνία και τη μετάδοση του μηνύματος [1].

3.4 Στεγανογραφία τροποποίησης αντικειμένου κάλυψης

Η πιο διαδεδομένη στεγανογραφία είναι αυτή της τροποποίησης του αντικειμένου κάλυψης. Η οντότητα που στέλνει το μυστικό μήνυμα ξεκινάει με την επιλογή ενός αντικειμένου κάλυψης και συνεχίζει με την τροποποίηση του με σκοπό την ενσωμάτωση του μυστικού μηνύματος. Και οι δύο οντότητες δουλεύουν με ένα σύνολο πιθανόν αντικειμένων κάλυψης και με ένα σύνολο κλειδιών και μηνυμάτων στο οποίο ισχύουν τα εξής [4]:

C …είναι ένα σύνολο αντικειμένων κάλυψης με $x \in C$.

$K(x)$ …είναι ένα σύνολο όλων των στεγο-κλειδιών για τα x.

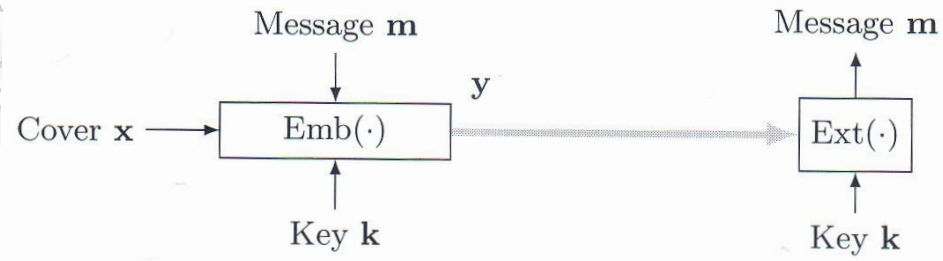
$M(x)$ …είναι ένα σύνολο μηνυμάτων που μπορούν να μεταδοθούν με την βοήθεια του x.

Σύμφωνα με την παρακάτω εικόνα ένα στεγανογραφικό σχέδιο είναι ένα ζευγάρι συναρτήσεων ενσωμάτωσης και εξαγωγής όπου ισχύει ότι [4]:

Συνάρτηση ενσωμάτωσης: $CxKxM \rightarrow C$

Συνάρτηση εξαγωγής: $CxK \rightarrow M$

όπου $x \in C$, $k \in K(x)$ και $m \in M(x)$, $Ext(Emb(x,k,m),k) = m$.



Εικόνα 3.2 Στεγανογραφία τροποποίησης του αντικειμένου κάλυψης.
Πηγή: (Steganography in digital media)

Με άλλα λόγια, η οντότητα που στέλνει το μυστικό μήνυμα μπορεί να πάρει οποιοδήποτε αντικείμενο κάλυψης $x \in C$ και να ενσωματώσει σε αυτό οποιοδήποτε μήνυμα $m \in M(x)$ χρησιμοποιώντας οποιοδήποτε κλειδί $k \in K(x)$ και στο τέλος να πάρει στην στεγο-εικόνα $y = Emb(x,k,m)$. Ο αριθμός των μηνυμάτων που μπορούν να μεταδοθούν σε ένα συγκεκριμένο αντικείμενο κάλυψης *x* εξαρτάται από το στεγανογραφικό σχέδιο και πολλές φορές εξαρτάται και από το ίδιο το αντικείμενο κάλυψης. Για παράδειγμα, εάν το *C* είναι ένα σύνολο από εικόνες grayscale διαστάσεων 512x512 και κατά την ενσωμάτωση ένα bit μηνύματος ενσωματώνεται σε ένα εικονοστοιχείο τότε έχουμε ότι $M = \{0,1\}^{512x512}$ και $|M(x)| = 2^{512x512}$ για κάθε $x \in C$. Από την άλλη πλευρά, εάν το *C* είναι ένα σύνολο από εικόνες grayscale JPEG διαστάσεων 512x512 με συντελεστή ποιότητας $g_f = 75$ και κατά την ενσωμάτωση ενσωματώνεται ένα bit για κάθε μη μηδενικό DCT συντελεστή, τότε ο αριθμός των μηνυμάτων που μπορούν να ενσωματωθούν σε ένα συγκεκριμένο αντικείμενο κάλυψης εξαρτάται από το ίδιο το αντικείμενο επειδή ο αριθμός των μη μηδενικό DCT συντελεστών σε ένα JPEG αρχείο εξαρτάται από το περιεχόμενο της εικόνας [1] [3] [4].

Όλα τα παραπάνω έχουν σαν αποτέλεσμα να ορίσουμε την χωρητικότητα ενσωμάτωσης (ωφέλιμο φορτίο) ενός αντικειμένου κάλυψης *x* σαν

$$\log_2 |M(x)| \quad (2),$$

Και την σχετική χωρητικότητα ενσωμάτωσης σαν

$$\frac{\log_2 |M(x)|}{n} \quad (3),$$

όπου το *n* είναι ο αριθμός των στοιχείων του *x* δηλαδή ο αριθμός των εικονοστοιχείων ή των μη αρνητικών συντελεστών DCT [1].

Η πιο σημαντική ίσως ιδέα στην στεγανογραφία είναι η στεγανογραφική χωρητικότητα η οποία ορίζεται ως ο μέγιστος αριθμός bits που μπορούν να ενσωματωθούν χωρίς να προκαλέσουν ανίχνευση χρήσης στεγανογραφίας. Κατά γενική ομολογία η στεγανογραφική χωρητικότητα είναι πολύ μικρότερη από την χωρητικότητα ενσωμάτωσης [1].

Οι αλγόριθμοι ενσωμάτωσης πολλών στεγανογραφικών σχεδίων απαιτούν μια αναπαράσταση του αντικειμένου κάλυψης και των στεγο-εικόνων χρησιμοποιώντας bits ή σύμβολα από μια αλφάβητο A. Τέτοιο παράδειγμα είναι αυτό κατά το οποίο χρησιμοποιούμε μια συνάρτηση ανάθεσης συμβόλου π,

$$\pi : X \to A \quad (4),$$

όπου X είναι ένα εύρος ατομικών στοιχείων του αντικειμένου κάλυψης, όπως είναι τα εικονοστοιχεία ή οι συντελεστές DCT. Μια συχνά χρησιμοποιούμενη συνάρτηση ανάθεσης bit είναι αυτή της LSB όπου

$$LSB(x) = x \bmod 2 \quad (5).$$

Στην περίπτωση που ο αλγόριθμου ενσωμάτωσης έχει σχεδιαστεί με σκοπό να αποφεύγει να πραγματοποιεί ενσωματωμένες αλλαγές σε συγκεκριμένες περιοχές της εικόνας κάλυψης, τότε μιλάμε για προσαρμοσμένη στεγανογραφία. Το υποσύνολο της εικόνας στο οποίο οι αλλαγές ενσωμάτωσης επιτρέπονται ονομάζεται επιλεγμένο κανάλι (selection channel) [1].

Τέλος, θα πρέπει να αναφέρουμε ότι η στεγανογραφία τροποποίησης του αντικειμένου κάλυψης εισάγει την έννοια της παραμόρφωσης στο αντικείμενο κάλυψης. Η παραμόρφωση μετράται με τον υπολογισμό του $d(x,y)$ όπου $d : CxC \to [0,\infty)$. Μια συνήθως χρησιμοποιημένη οικογένεια των μέτρων διαστρεβλώσεων παραμετροποιείται από το $\gamma \geq 1$, με αποτέλεσμα να προκύπτει ο παρακάτω τύπος υπολογισμού της παραμόρφωσης [1]:

$$d_{\gamma}(x.y) = \sum_{i=1}^{n} | x[i] - y[i] |^{\gamma} \quad (6)$$

3.5 Συμπεράσματα

Στο κεφάλαιο αυτό ουσιαστικά αναλύσαμε τρεις αρχές για την δημιουργία στεγανογραφικών μεθόδων. Όπως μπορούμε να συμπεράνουμε από τα παραπάνω η καλύτερη αρχή είναι αυτή της δημιουργίας τροποποιημένων αντικειμένων κάλυψης μιας και επιτρέπει την αποστολή μεγάλου μεγέθους μηνύματος μεταξύ των οντοτήτων αλλά επιπλέον παρέχει και μεγαλύτερο βαθμό ασφάλειας κατά την μετάδοση του. Κατ' αυτό τον τρόπο προστατεύεται το στεγανογραφικό κανάλι από πιθανή εμπλοκή και διακοπή από μια κακόβουλη οντότητα.

Επιπλέον αναφερθήκαμε και στους τρεις ρόλους που μπορεί να «παίξει» μια κακόβουλη οντότητα. Ο χειρότερος ρόλος είναι αυτός του δόλιου παρατηρητή μιας και μπορεί να προκαλέσει μεγάλο πρόβλημα στην επικοινωνία των δύο οντοτήτων και χωρίς μάλιστα να γίνεται αντιληπτός.

Τέλος αυτό το οποίο είναι σημαντικό είναι ο ορισμός της στεγανογραφική χωρητικότητα, της χωρητικότητα ενσωμάτωσης (ωφέλιμο φορτίο) ενός αντικειμένου κάλυψης και της σχετική χωρητικότητα ενσωμάτωσης. Μεγέθη πολύ αναγκαία για την μελέτη και χρήση της στεγανογραφίας.

Βιβλιογραφία

[1] Jessica Fridrich “Steganography in Digital Media” Cambridge University Press 2010.

[2] J. Rutenberg. “A nation challenged: Videotape.” New York Times February 2002.

[3] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon ‘‘Cover Selection For Steganographic Embedding’’ Dept. of Electrical and Computer Eng., Polytechnic University, Brooklyn, NY, USA.

[4] Ingermar J. Cox ‘‘Digital watermarking and steganography’’ Morgan Kaufmann 2008.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Κεφάλαιο 4

Συμπιεσμένη δειγματοληψία

4.1 Εισαγωγή

Η παραδοσιακή προσέγγιση της αναπαράστασης σημάτων ή εικόνων από μετρήσιμα δεδομένα (data) ακολουθεί το γνωστό θεώρημα του Shannon για την δειγματοληψία [3], το οποίο υποστηρίζει ότι ο ρυθμός (rate) της δειγματοληψίας πρέπει να είναι διπλάσιος της υψηλότερης συχνότητας. Παρόμοια το βασικό θεώρημα της γραμμικής άλγεβρας προτείνει ότι ο αριθμός των συλλεγόμενων δειγμάτων ενός μεμονωμένου σήματος πρέπει να είναι το λιγότερο τόσο μεγάλος όσο το μήκος του (ή η διάστασή του) έτσι ώστε να μπορεί να πραγματοποιηθεί η αναπαράσταση. Αυτή η αρχή αποτελεί την βάση για την λειτουργία των περισσοτέρων συσκευών όπως για παράδειγμα η μετατροπή σήματος από το αναλογικό σε ψηφιακό και η απεικόνιση ιατρικών εικόνων [1].

Η καινοτόμος θεωρία της συμπιεσμένης δειγματοληψίας (compressed theory), γνωστή είτε ως compressive sensing είτε ως compressive sampling, παρέχει μια νέα προσέγγιση στην ανάκτηση δεδομένων η οποία ωστόσο είναι ενάντια στην κοινή φιλοσοφία που ισχύει μέχρι τώρα. Η θεωρία της συμπιεσμένης δειγματοληψίας υποστηρίζει ότι συγκεκριμένα σήματα ή εικόνες μπορούν να ανακτηθούν από πολύ λιγότερα δείγματα ή μετρήσεις σε σχέση με τις παραδοσιακές μεθόδους. Για να υλοποιηθεί αυτό η συμπιεσμένη δειγματοληψία βασίζεται σε δύο αρχές: στην αραιότητα (sparsity), και στην μη συνοχή (incoherence) [2].

Η αραιότητα εκφράζει την ιδέα ότι ο «ρυθμός πληροφορίας» ενός συνεχόμενου σήματος μπορεί να είναι πολύ μικρότερος από αυτόν που προτείνει το εύρος (bandwidth) του σήματος. Πιο συγκεκριμένα η μέθοδος της συμπιεσμένης δειγματοληψίας εκμεταλλεύεται το γεγονός ότι πολλά φυσικά σήματα είναι αραιά ή συμπιεσμένα με την λογική ότι έχουν περιεκτικές αναπαραστάσεις όταν εκφράζονται σε μια κατάλληλη βάση Ψ. Από την άλλη μεριά, η μη συνοχή επεκτείνει την διττότητα μεταξύ χρόνου και συχνότητας και εκφράζει την ιδέα ότι τα αντικείμενα που έχουν μια αραιή αναπαράσταση στη βάση Ψ πρέπει να απλώνονται αραιά μέσα στο τομέα από τον οποίο αποκτήθηκαν. Με άλλα λόγια η αρχή της μη συνοχής εκφράζει ότι η οι κυματομορφές του πηλίκου sampling/sensing είναι πολύ πυκνές αναπαραστάσεις πάνω στην βάση Ψ [2].

Η συμπιεσμένη δειγματοληψία βασίζεται κυρίως στην εμπειρική παρατήρηση ότι πολλοί τύποι σημάτων ή εικόνων μπορούν να προσεγγιστούν καλά από μια αραιή επέκταση σε μια κατάλληλη βάση, δηλαδή, από μόνο έναν μικρό αριθμό διαφορετικών από το μηδέν συντελεστών. Γενικά αυτό είναι τα κλειδί για μια αποτελεσματική συμπίεση όπως είναι αυτή των εικόνων JPEG και των μουσικών αρχείων mp3. Η συμπίεση επιτυγχάνεται από μια απλή αποθήκευση μόνο των μέγιστων βασικών συντελεστών (coefficients). Όταν αναπαρίσταται το σήμα οι μη αρνητικοί συντελεστές (non-zero coefficients) απλά τίθενται μηδέν. Αυτό είναι μια ασφαλής στρατηγική όταν είναι διαθέσιμη μια πλήρης πληροφορία για το σήμα. Παρ όλα αυτά όταν το σήμα αρχικά πρέπει να αποκτηθεί από κάτι το οποίο κοστίζει και χρειάζεται μια δύσκολη διαδικασία μέτρησης, τότε μιλάμε για χάσιμο πόρων και αυτό γιατί αρχικά πρέπει να γίνουν μεγάλες προσπάθειες έτσι ώστε να αποκτηθεί η πλήρη πληροφορία του σήματος και στη συνέχεια η περισσότερη από την πληροφορία αυτή χάνεται κατά τη διαδικασία της συμπίεσης [1].

Μια λύση στο παραπάνω πρόβλημα θα ήταν αν μπορούσαμε να αποκτήσουμε την συμπιεσμένη έκδοση ενός σήματος πιο άμεσα, παίρνοντας ένα μικρό αριθμό μετρήσεων του σήματος. Ωστόσο αυτό δεν είναι καθόλου εύκολο μιας και η απευθείας μέτρηση των μεγάλων συντελεστών απαιτεί να γνωρίζουμε εκ των προτέρων την τοποθεσία τους [1].

Η συμπιεσμένη δειγματοληψίας όμως παρέχει ένα τρόπο για αναπαράσταση μιας συμπιεσμένης έκδοσης του αυθεντικού σήματος παίρνοντας ένα μόνο μικρό ποσό από

γραμμικές και μη προσαρμοστικές μετρήσεις. Ο ακριβής αριθμός των απαιτούμενων μετρήσεων είναι ανάλογος του μεγέθους συμπίεσης του σήματος. Ωστόσο, οι μετρήσεις πρέπει να σχεδιαστούν κατάλληλα. Ένα αξιοπρόσεκτο γεγονός είναι ότι όλες οι καλές μήτρες μέτρησης που σχεδιάζονται μέχρι τώρα είναι τυχαίες μήτρες. Αυτός είναι και ο κύριος λόγο ότι η θεωρία της συμπιεσμένης δειγματοληψίας χρησιμοποιεί πολλά εργαλεία από τη θεωρία πιθανότητας. [1]. Τέλος, άλλο σημαντικό χαρακτηριστικό της συμπιεσμένης δειγματοληψίας είναι ότι η πρακτική αναπαράσταση μπορεί να εκτελεστεί χρησιμοποιώντας αποτελεσματικούς αλγορίθμους [5].

Στην συνέχεια του κεφαλαίου αυτού θα πραγματοποιήσουμε μια βαθύτερη προσέγγιση στο νέο αυτό πεδίου που ονομάζεται συμπιεσμένης δειγματοληψίας παρουσιάζοντας αναλυτικότερα τις δύο αρχές που ισχύουν για την συμπιεσμένη δειγματοληψία, το πρόβλημα της συμπιεσμένης δειγματοληψίας και τις εφαρμογές στις οποίες βρίσκει εφαρμογή η συμπιεσμένη δειγματοληψία. Τέλος θα χρησιμοποιήσουμε ένα λογισμικό με σκοπό να παρουσιάσουμε τα αποτελέσματα μιας συμπιεσμένης δειγματοληψίας.

4.2 Το πρόβλημα της συμπιεσμένης δειγματοληψίας

Στην υποενότητα αυτή θα παρουσιάσουμε αναλυτικά το πρόβλημα της συμπιεσμένης δειγματοληψίας με την βοήθεια μαθηματικών σχέσεων και στην συνέχεια θα δώσουμε τις κατάλληλες λύσεις για την επίλυσή του.

Θεωρούμε ένα πεπερασμένου μήκους μονοδιάστατο σήμα x το οποίο μπορεί να αναπαρασταθεί σαν ένα διάνυσμα ^{Nx1} με πεδίο ορισμού $\mathbb{R}^N$ και στοιχεία x[n] όπου $n = 1,2,...,N$. Οποιοδήποτε σήμα μέσα στο $\mathbb{R}^N$, μπορεί να απεικονιστεί, με την βοήθεια της βάσης ^{Nx1} διανυσμάτων σαν $\{\psi_i\}_{i=1}^N$. Για απλότητα, θεωρούμε ότι η βάση είναι ορθογώνια. Χρησιμοποιώντας τώρα την βάση μήτρας $\Psi = [\psi_1 | \psi_2 | ... | \psi_N]$ διαστάσεως NxN με τα διανύσματα $\{\psi_i\}$ σαν στήλες, ένα σήμα x μπορεί να εκφραστεί σαν

$$x = \sum_{i=1}^{N} s_i \psi_i \quad \text{ή} \quad x = \psi s \quad (1)$$

όπου s είναι ένα Nx1 διάνυσμα στήλης με συντελεστή στάθμισης $s_i = \langle x, \psi_i \rangle = \psi_i^T x$ με το T να δηλώνει μετάθεση. Όπως μπορούμε να συμπεράνουμε, τόσο το s όσο και το x είναι ίδιες αναπαραστάσεις του σήματος, με το x στην περιοχή του χρόνου και το s στην περιοχή της βάσης μήτρας Ψ [4].

Το σήμα x είναι K-αραιό εάν είναι ένας γραμμικός συνδυασμός από διανύσματα βάσης K. Αυτό έχει σαν αποτέλεσμα, K των συντελεστών s_i της σχέσης (1) να είναι μη μηδενικά και (N-K) να είναι μηδενικά. Η περίπτωση όμως που μας ενδιαφέρει είναι όταν ισχύει $K \ll N$. Τότε το σήμα x μπορεί να συμπιεστεί εάν η αναπαράσταση της σχέσης (1) έχει μερικούς μεγάλους συντελεστές και πολλούς μικρούς συντελεστές [4].

Το γεγονός ότι τα συμπιεσμένα σήματα είναι πολύ καλά προσεγγισμένα από K-αραιές αναπαραστάσεις, βοηθούν στο να διαμορφωθεί το θεμέλιο της αλλαγής κωδικοποίησης. Στην ανάκτηση δεδομένων από συστήματα, όπως για παράδειγμα, στις ψηφιακές κάμερες, η αλλαγή κωδικοποίησης έχει πρωταρχικό ρόλο: το πλήρες σήμα x N-δειγμάτων ανακτάται. Αυτό πραγματοποιείται ως εξής: αρχικά το πλήρες σύνολο της αλλαγής συντελεστών $\{s_i\}$ υπολογίζεται μέσω της σχέσης $s = \psi^T x$, στην συνέχεια οι K μεγαλύτεροι συντελεστές εντοπίζονται και οι (N-K) μικρότεροι συντελεστές απορρίπτονται. Τέλος οι τιμές των K και οι θέσεις των μεγαλύτερων συντελεστών κωδικοποιούνται [4].

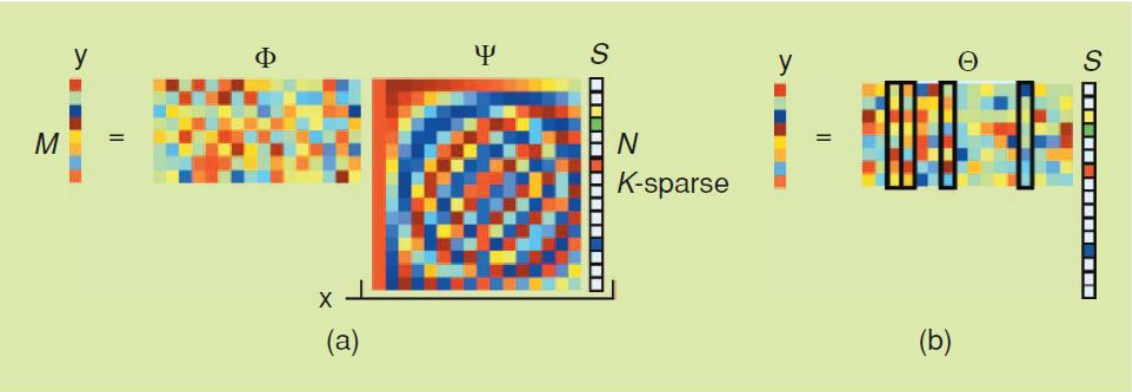
Δυστυχώς, αυτή η διαδικασία κωδικοποίησης που περιγράψαμε πιο πάνω πάσχει από τρία σοβαρά προβλήματα. Πρώτον, ο αρχικός αριθμός δειγμάτων N μπορεί να είναι μεγάλος ακόμη και εάν το επιθυμητό K είναι μικρό. Δεύτερον, το σύνολο όλων των N αλλαγών συντελεστών $\{s_i\}$ πρέπει να υπολογιστεί ακόμα κι αν όλοι εκτός από K θα απορριφθούν. Τρίτον, οι θέσεις των μεγάλων συντελεστών πρέπει να είναι κωδικοποιημένες, εισάγοντας κατά συνέπεια μεγαλύτερο κόστος [4].

Η συμπιεσμένη δειγματοληψία (compressive sensing) λύνει αυτά τα προβλήματα με μια άμεση ανάκτηση της αναπαράστασης του συμπιεσμένου σήματος χωρίς να χρειάζεται να περάσει από το ενδιάμεσο στάδιο της ανάκτησης N δειγμάτων. Θεωρούμε μια γενική γραμμική διαδικασία μέτρησης που υπολογίζει το $M < N$ εσωτερικό γινόμενο μεταξύ x και a συλλογής διανυσμάτων $\{\varphi_j\}_{j=1}^{M}$ με $\{y_j\} = \langle x, \varphi_j \rangle$. Στην συνέχεια τακτοποιούμε τις μετρήσεις y_j σε ένα $Mx1$ διάνυσμα y και τις μετρήσεις των διανυσμάτων φ_j^T ως γραμμές σε έναν πίνακα Φ διαστάσεων MxN. Έπειτα με αντικατάσταση του Ψ από την σχέση (1) το y μπορεί να γραφτεί ως εξής:

$$y = \Phi x = \Phi\Psi s = \Theta s \quad (2)$$

όπου $\Theta = \Phi\Psi$ είναι ένας πίνακας διαστάσεων MxN. Η διαδικασία μέτρησης δεν είναι προσαρμοστική πράγμα το οποίο σημαίνει ότι ο πίνακας Φ είναι προκαθορισμένος και δεν βασίζεται πάνω στο σήμα x. Το πρόβλημα όμως που δημιουργείται έγκειται:

- στο σχεδιασμό μιας σταθερής μήτρας Φ έτσι ώστε οι βασικές πληροφορίες σε κάθε K-αραιό ή συμπιεσμένο σήμα να μην καταστρέφονται από την μείωση της διάστασης από $x \in \mathbb{R}^N$ σε $y \in \mathbb{R}^M$ και
- στο σχεδιασμό ενός αλγορίθμου αναπαράστασης ο οποίος θα ανακτά το σήμα x από $M \approx K$ μετρήσεις του διανύσματος y. Η εικόνα που ακολουθεί είναι η γραφική αναπαράσταση όλων των παραπάνω μαθηματικών σχέσεων [4].



Εικόνα 4.1 Γραφική αναπαράσταση του προβλήματος συμπιεσμένης δειγματοληψίας

Πηγή: (IEE Signal Processing Magazine July 2007)

4.2.1 Λύση στο πρόβλημα της συμπιεσμένης δειγματοληψίας

Όπως αναφέραμε παραπάνω δύο είναι οι βασικές λύσεις που υπάρχουν στον πρόβλημα της συμπιεσμένης δειγματοληψίας. Η πρώτη είναι να δημιουργήσουμε μια σταθερή μήτρα Φ και η δεύτερη είναι η δημιουργία ενός αλγορίθμου αναπαράστασης. Στην συνέχεια θα αναλύσουμε περαιτέρω αυτές τις λύσεις.

4.2.1.1 Δημιουργία μιας σταθερής μετρήσιμης μήτρας

Η μήτρα Φ πρέπει να επιτρέπει την αναπαράσταση ενός σήματος x μήκους N από M < N μετρήσεις (διάνυσμα y). Όσο ισχύει η σχέση M < N τόσο το πρόβλημα φαίνεται άλυτο. Εάν, όμως, το σήμα x είναι K-αραιό και οι K τοποθεσίες των μη αρνητικών συντελεστών s είναι γνωστές, τότε το πρόβλημα μπορεί να λυθεί αρκεί να ισχύει $M \geq K$. Ένας απαραίτητος και ικανοποιητικός όρος για αυτό το απλουστευμένο πρόβλημα είναι ο εξής: για κάθε διάνυσμα v το οποίο μοιράζεται τις ίδιες μη μηδενικές εισαγωγές K όπως το s και για $\varepsilon \succ 0$ ισχύει ότι:

$$1-\varepsilon \leq \frac{\| \Theta v \|_2}{\| v \|_2} \leq 1+\varepsilon \quad (3)$$

όπου ο πίνακας Θ πρέπει να αντιπροσωπεύει το μήκος των συγκεκριμένων K-αραιών διανυσμάτων. Φυσικά, η τοποθεσία στην οποία βρίσκονται οι K μη μηδενικές εισαγωγές στο διάνυσμα s δεν είναι γνωστές. Παρ όλα αυτά, ένας ικανοποιητικός όρος για μια σταθερή λύση τόσο για τα K-αραιά σήματα όσο και για τα συμπιεσμένα είναι ότι ο πίνακας Θ ικανοποιεί την σχέση (3) για ένα αυθαίρετο 3K-αραιό διάνυσμα v. Η παραπάνω προϋπόθεση είναι γνωστός ως RIP (Resticted Isometry Property). Μια παρόμοια προϋπόθεση, η οποία αναφέρεται σαν μη συνοχή (incoherence), και την οποία αναλύσαμε σε προηγούμενη υποενότητα, απαιτεί ότι οι γραμμές $\{\varphi_j\}$ της μήτρας Φ δεν μπορούν να αναπαρασταθούν από τις στήλες $\{\psi_i\}$ της μήτρας Ψ και αντίστροφα [4].

Γενικά θα λέμε ότι ένας πίνακας A ικανοποιεί το RIP (Resticted Isometry Property) εάν για οποιαδήποτε K-αραιά διανύσματα ισχύει η σχέση

$$(1-\delta_S)\|y\|_{l2}^2 \leq \|A_S y\|_{l2}^2 \leq (1+\delta_S)\|y\|_{l2}^2 \quad (4)$$

όπου A ένας πίνακας διαστάσεων mxp, $s < p$ όπου s είναι ένας ακέραιος και δ_S είναι μια σταθερά. Στη περίπτωση αυτή, όπου ο πίνακας A έχει αυτή την προϋπόθεση, μπορούμε να ανακτήσουμε την αραιή λύση y ενός συστήματος $Ay = b$ χρησιμοποιώντας το γραμμικό προγραμματισμό $(l1)$ αντί της συνδυαστικής αναζήτησης $(l0)$ που θα παρουσιάσουμε παρακάτω.

Τόσο ο όρος RIP όσο και ο όρος της μη συνοχής (incoherence) μπορούν να επιτευχθούν με μεγάλη πιθανότητα απλά διαλέγοντας την μήτρα Φ σαν μια τυχαία μήτρα. Για παράδειγμα, ας αφήσουμε τα στοιχεία της μήτρας Φ $\varphi_{j,i}$ να είναι ανεξάρτητες και παρόμοια διασκορπισμένες τυχαίες μεταβλητές από μια γκαουσιανή (Gaussian) συνάρτηση πυκνότητας πιθανότητας με μέσο μηδέν και διαφορά $\frac{1}{N}$. Τότε οι μετρήσεις y είναι απλώς M διαφορετικοί τυχαίοι γραμμικοί συνδυασμοί των στοιχείων x του σήματος όπως φαίνεται και στην εικόνα 6.1 (a). Οι γκαουσιανές μετρήσεις της μήτρας Φ έχουν δύο ενδιαφέρουσες και χρήσιμες ιδιότητες οι οποίες είναι οι εξής [4]:

- Μια MxN ανεξάρτητη και παρόμοια διασκορπισμένη Gaussian μήτρα $\Theta = \Phi I = \Phi$ μπορεί να έχει την ιδιότητα RIP με υψηλή πιθανότητα $M \geq cK\log(\frac{N}{K})$ εάν c είναι μια μικρή σταθερά. Άρα ένα K-αραιό και συμπιεσμένο σήμα μήκους N μπορεί να ανακτηθεί μόνο από τυχαίες $M \geq cK\log(\frac{N}{K}) \ll N$ Gaussian μετρήσεις.

- Η μήτρα Φ είναι καθολική (universal) με την έννοια ότι αφού ισχύει ότι $\Theta = \Phi\Psi$ τότε θα είναι ανεξάρτητη και παρόμοια διασκορπισμένη Gaussian μήτρα και έτσι θα έχει την ιδιότητα RIP με υψηλή πιθανότητα ανεξαρτήτου επιλογής της ορθογώνιας βάσης Ψ.

4.2.1.2 Δημιουργία ενός αλγορίθμου ανάκτησης του σήματος

Ο αλγόριθμός ανάκτησης σήματος πρέπει να παίρνει τις M μετρήσεις του διανύσματος y και τις τυχαίες μετρήσεις της μήτρας Φ και της βάσης Ψ και να ανακατασκευάζει το σήμα x μήκους N ή ισοδύναμα, τον συντελεστή διασποράς-αραιότητας (sparse) του διανύσματος s. Για K-αραιά σήματα, για M < N και με βάση την σχέση (2) υπάρχουν άπειρα πολλά s' τα οποία ικανοποιούν την σχέση $\Theta s' = y$. Αυτό ισχύει επειδή εάν $\Theta s = y$ τότε $\Theta(s + r) = y$ για κάθε διάνυσμα r στον μηδενικό χώρο $N(\Theta)$ του Θ [4].

- **Ελάχιστη l_2 νόρμα ανάκτησης**

Ορίζουμε την l_p νόρμα του διανύσματος s σαν $(\| s \|_p)^p = \sum_{i=1}^{N} | s_i |^p$. Η κλασσική προσέγγιση των αντίστροφων προβλημάτων τέτοιου τύπου είναι να βρούμε το διάνυσμα με την μικρότερη l_2 νόρμα λύνοντας την παρακάτω σχέση:

$$\hat{s} = \text{argmin} \| s' \|_2 \text{ τέτοιο ώστε } \Theta s' = y \quad (5)$$

Δυστυχώς όμως η ελαχιστοποίηση του l_2 δεν βρίσκει σχεδόν ποτέ μια K-αραιή λύση, επιστρέφοντας έτσι ένα μη αραιό $\hat{s}$ με πολλά μη μηδενικά στοιχεία [4].

- **Ελάχιστη l_0 νόρμα ανάκτησης**

Μιας και η l_2 νόρμα μετράει την ενέργεια του σήματος και όχι την αραιότητα του σήματος, θεωρούμε την l_0 νόρμα η οποία υπολογίζει τον αριθμό των μη μηδενικών εισαγωγών στο διάνυσμα s. Η σχέση που ακολουθεί μπορεί να ανακτήσει ένα K-αραιό σήμα με υψηλή πιθανότητα χρησιμοποιώντας μόνο $M = K + 1$ ανεξάρτητες και παρόμοιες διασκορπισμένες Gaussian μετρήσεις.

$$\hat{s} = \text{argmin} \| s' \|_0 \text{ τέτοιο ώστε } \Theta s' = y \quad (6)$$

Δυστυχώς όμως λύνοντας την σχέση (6) προκύπτει αριθμητική αστάθεια με αποτέλεσμα να χρειάζεται να υπολογίζουμε όλες τις $\binom{N}{K}$ πιθανές τοποθεσίες των μη μηδενικών εγγραφών του διανύσματος s. Πράγμα το οποίο είναι εξαντλητικό [4].

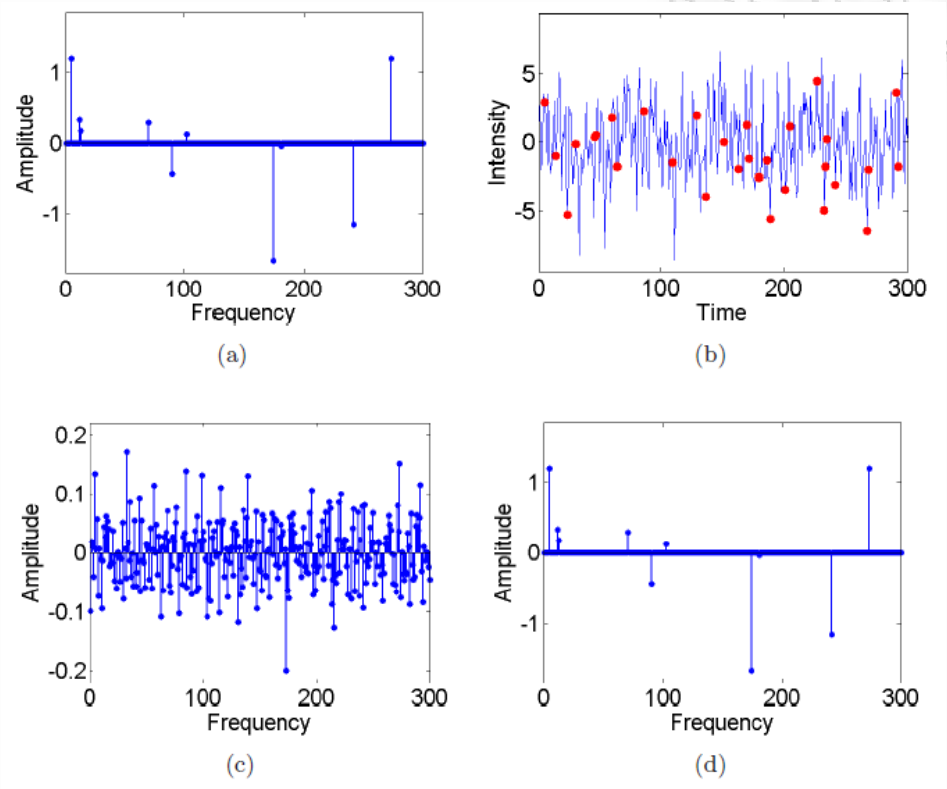
- **Ελάχιστη l_1 νόρμα ανάκτησης**

Ωστόσο η παρακάτω σχέση είναι αυτή που μπορεί να ανακτήσει K-αραιά σήματα και συμπιεσμένα σήματα με υψηλή πιθανότητα χρησιμοποιώντας μόνο τυχαίες ανεξάρτητες και παρόμοια διασκορπισμένες $M \geq cK\log(\frac{N}{K}) \ll N$ Gaussian μετρήσεις.

$$\hat{s} = \text{argmin} \| s' \|_1 \text{ τέτοιο ώστε } \Theta s' = y \quad (7)$$

Αυτό είναι μια βελτιστοποίηση του προβλήματος που μειώνει την λύση σε ένα γραμμικό πρόγραμμα γνωστό ως αναζήτηση βάσης (basis pursuit) του οποίου η υπολογιστική πολυπλοκότητα είναι περίπου $O(N^3)$ [4].

Η παρακάτω εικόνα απεικονίζει την δύναμη της συμπιεσμένης δειγματοληψίας. Παρουσιάζει ένα παράδειγμα ανάκτησης ενός διεσπαρμένου σήματος από μόνο 30 δείγματα. Κάποιος θα πίστευε ότι η αναπαράσταση του σήματος από 30 μόνο δείγματα θα ήταν κάτι το ακατόρθωτο. Και όντως όπως μπορούμε να δούμε από την εικόνα 4.2 c χρησιμοποιώντας την μέθοδο ℓ2-minimization που αναλύσαμε παραπάνω, κατορθώνουμε να αναπαραστήσουμε ένα σήμα πολύ διαφορετικό από το αρχικό, ενώ χρησιμοποιώντας την μέθοδο ℓ1-minimization αναπαριστούμε το σήμα μας ακριβώς όπως ήταν στην αρχή και χωρίς κανένα λάθος [1].



Εικόνα 4.2 Ανάκτηση σήματος με την μέθοδο ℓ1-minimization και ℓ2-minimization

Πηγή : (Massimo Fornasier and Holger Rauhut "Compressing Sensing")

4.3 Βασικές αρχές της συμπιεσμένης δειγματοληψίας

Όπως γνωρίζουμε από την εισαγωγή του κεφαλαίου αυτού η συμπιεσμένη δειγματοληψία βασίζεται σε δύο αρχές: στην αραιότητα (sparsity), και στην μη συνοχή (incoherence). Στην συγκεκριμένη υποενότητα θα αναλύσουμε αυτές τις δύο αρχές.

4.3.1 Αραιότητα

Πολλά φυσικά σήματα έχουν συνοπτικές αναπαραστάσεις όταν εκφράζονται σε βολικές βάσεις. Ας υποθέσουμε ότι έχουμε την εικόνα 4.3 a και την κυματομορφή της που είναι η εικόνα 4.3 b. Αν και σχεδόν όλα τα pixels της εικόνας έχουν μη μηδενικές τιμές οι συντελεστές του κύματος προσφέρουν μια συνοπτική περίληψη: οι περισσότεροι συντελεστές είναι μικροί και οι σχετικά μεγάλοι συντελεστές συλλαμβάνουν την περισσότερη πληροφορία.

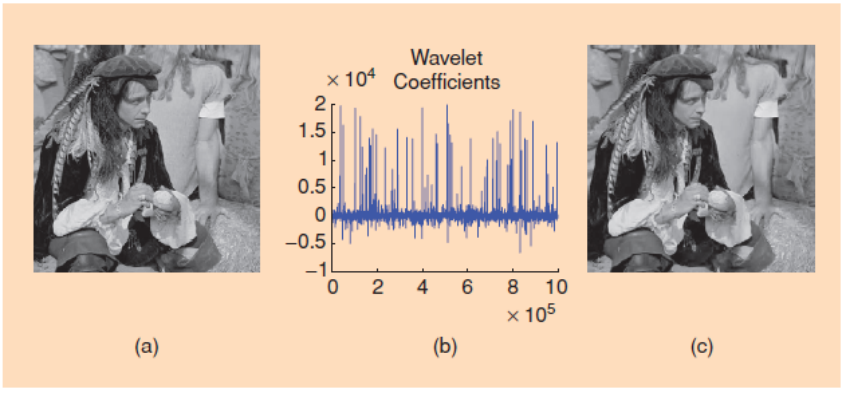
Μιλώντας από τη μαθηματική πλευρά των πραγμάτων, έχουμε ένα διάνυσμα $f \in \mathbb{R}^n$ (τέτοιο ώστε το n να είναι ο αριθμός των pixels της εικόνας 4.3) το οποίο επεκτείνεται σε μια ορθογώνια βάση $\Psi = [\psi_1\psi_2...\psi_n]$ όπως φαίνεται στην παρακάτω σχέση:

$$f(t) = \sum_{i=1}^{n} x_i\psi_i(t) \quad (8)$$

όπου x είναι μια ακολουθία συντελεστών της f, $x_i = \langle f, \psi_i \rangle$. Θα ήταν βέβαια καλύτερο να εκφράζαμε την συνάρτηση f ως Ψx (όπου Ψ είναι ένας πίνακας διαστάσεων nxn με $\psi_1,...,\psi_n$ ως στήλες). Η επίπτωση που έχει η αραιότητα (sparsity) είναι πια ξεκάθαρη: όταν ένα σήμα έχει μια αραιή επέκταση, τότε μπορεί κανείς να απορρίψει μερικούς μικρούς συντελεστές χωρίς μεγάλη απώλεια της αντίληψης. Ας θεωρήσουμε την συνάρτηση $f_S(t)$ η οποία κρατάει μόνο εκείνους τους όρους αντιστοιχίζοντας στο S τις υψηλότερες τιμές των x_i από την σχέση (8). Εξ ορισμού, $f_S := \Psi x_S$ όπου x_S είναι το διάνυσμα των συντελεστών (x_i) με το μεγαλύτερο S να τίθεται μηδέν. Αυτό το διάνυσμα είναι αραιό υπό την αυστηρή έννοια του όρου μιας και όλες εκτός από μερικές από τις εγγραφές του είναι μηδέν. Θα ονομάζουμε S-αραιά (S-sparse) εκείνα τα αντικείμενα με τις περισσότερες μη μηδενικές εγγραφές [2].

Μιας και η βάση Ψ είναι ορθογώνια έχουμε ότι $\| f - f_S \|_{l_2} = \| x - x_S \|_{l_2}$ και εάν το x είναι αραιό ή συμπιεσμένο με την έννοια ότι τα ταξινομημένα μεγέθη των (x_i) φθίνουν γρήγορα, τότε το x έχει προσεγγιστεί καλά από το x_S και γι' αυτό τον λόγο το λάθος $\| f - f_S \|_{l_2}$ είναι μικρό. Συμπερασματικά θα μπορούσαμε να πούμε ότι μπορούμε να απορρίψουμε ένα μεγάλο μέρος των συντελεστών χωρίς να χάσουμε πολλά στοιχεία από την εικόνα μας.

Η εικόνα 4.3 c παρουσιάζει ένα παράδειγμα στο οποίο η αντιληπτική απώλεια είναι μετά βίας αξιοπρόσεχτη από μια εικόνα ως προς την προσέγγισή της που λαμβάνεται όταν απορρίψουμε το 97.5% των συντελεστών της [2].



Εικόνα 6.3 a) Αρχική εικόνα b) Κυματομορφή συντελεστών εικόνας c) Ανακτημένη εικόνα

Πηγή : (Emmanuel J. Candes "An Introduction to Compressing Sampling")

Η αρχή που περιγράψαμε πιο πάνω είναι αυτή που κρύβεται πίσω τις σύγχρονες κωδικοποιήσεις όπως είναι αυτή της JPEG-2000 και πολλές άλλες, μιας και μια απλή μέθοδο για συμπίεση δεδομένων θα ήταν να υπολογίζει το x από την f και έπειτα να κωδικοποιεί τις θέσεις και τις τιμές των S σημαντικών συντελεστών. Μια τέτοια διαδικασία απαιτεί την γνώση όλων των n συντελεστών x, δεδομένου ότι οι θέσεις των σημαντικών πληροφοριών δεν μπορούν να μαθευτούν εκ των προτέρων (εξαρτώμενο σήμα) [2].

Τέλος θα πρέπει να επισημάνουμε ότι, η αραιότητα (sparsity) είναι ένα βασικό εργαλείο διαμόρφωσης το οποίο επιτρέπει την αποδοτική επεξεργασία σήματος όπως για παράδειγμα την ακριβής στατιστικής εκτίμηση και ταξινόμηση, αποδοτική συμπίεση στοιχείων κ.λ.π [2].

4.3.2 Μη συνοχή

Ας υποθέσουμε ότι έχουμε ένα ζευγάρι (Φ,Ψ) με ορθογώνιες βάσεις ορισμένες στο $\mathbb{R}^n$. Η πρώτη βάση Φ χρησιμοποιείται για την δειγματοληψία του αντικειμένου f και η δεύτερη βάση για την αναπαράσταση του f. Ο περιορισμός στα ζευγάρια των ορθογώνιων βάσεων δεν είναι ουσιαστικός και το μόνο που προσφέρει είναι απλοποίηση στην επεξεργασίας [2].

Η σχέση η οποία ενώνει την δειγματοληπτική βάση Φ με την βάση αναπαράστασης Ψ είναι η παρακάτω:

$$\mu(\Phi,\Psi) = \sqrt{n} * \max_{1\le k,j\le n} \left| \left\langle \varphi_k, \psi_j \right\rangle \right| \quad (9)$$

Γενικά η συνοχή (coherence) μετράει τη μεγαλύτερη συσχέτιση μεταξύ οποιοδήποτε δύο στοιχείων των Φ και Ψ. Στην περίπτωση που τα Φ και Ψ διαθέτουν στοιχεία τα οποία είναι συσχετισμένα τότε η συνοχή είναι μεγάλη αλλιώς είναι μικρή. Τώρα, όσον αναφορά πόσο μεγάλη ή πόσο μικρή είναι αυτό εξαρτάται από την γραμμική άλγεβρα στην οποία ισχύει ότι $\mu(\Phi,\Psi) \in [1,\sqrt{n}]$. Η συμπιεσμένη δειγματοληψία ασχολείται κυρίως με τα ζευγάρια που έχουν χαμηλή συνοχή (low coherence) [2]. Στην συνέχεια αυτής της υποενότητας θα παρουσιάσουμε παραδείγματα με ζευγάρια που δεν έχουν συνοχή (incoherence pairs).

- Στο πρώτο παράδειγμα η βάση Φ είναι είτε κανονική είτε βάση ακίδων $\varphi_k(t) = \delta(t-k)$ και η βάση Ψ είναι μια βάση Fourier $\psi_j(t) = n^{-1/2} e^{i2\pi jt/n}$. Αφού η βάση Φ είναι ένας πίνακας δειγματοληψίας, τότε αντιστοιχεί στο κλασσικό σχέδιο δειγματοληψίας χρόνου ή διαστήματος. Το ζευγάρι χρόνος-συχνότητας υπακούει στην σχέση $\mu(\Phi,\Psi) = 1$ και γι αυτό το λόγο έχουμε την μέγιστη μη συνοχή (incoherence) [2].
- Στο δεύτερο παράδειγμα ας υποθέσουμε ότι οι τυχαίες μήτρες είναι κατά ένα μεγάλο μέρος χωρίς συνοχή με οποιαδήποτε σταθερή βάση Ψ. Επιλέγουμε μια ομοιόμορφη ορθογώνια βάση Φ στην τύχη πράγμα το οποίο μπορεί να πραγματοποιηθεί διαλέγοντας ορθογώνια διανύσματα n τα οποία είναι ανεξάρτητα και τυχαία. Τότε με μεγάλη πιθανότητα, η συνοχή μεταξύ Φ και Ψ είναι περίπου $\sqrt{2\log n}$. Κατ' επέκταση, οι τυχαίες κυματομορφές $(\varphi_k(t))$ με ανεξάρτητες παρόμοιες διασκορπισμένες καταχωρήσεις θα έχουν επίσης μια πολύ χαμηλή συνοχή με οποιαδήποτε σταθερή αντιπροσώπευση της βάσης Ψ [2].

4.4 Εφαρμογές συμπιεσμένης δειγματοληψίας

Το γεγονός ότι ένα συμπιέσιμο σήμα μπορεί αποτελεσματικά να συλληφθεί χρησιμοποιώντας διάφορες μετρήσεις χωρίς συνοχή (incoherent), οι οποίες είναι ανάλογες προς το επίπεδο πληροφορίας $S \ll n$, έχει εκτεταμένες εφαρμογές τις οποίες και θα περιγράφουμε παρακάτω.

Σε ορισμένες καταστάσεις, η αραιή (sparse) βάση Ψ μπορεί να είναι άγνωστη στον κωδικοποιητή ή μπορεί να μην είναι πρακτική στο να εφαρμοστεί για τη συμπίεση στοιχείων. Σύμφωνα με την θεωρία της «Τυχαίας Δειγματοληψίας» [2] μια τυχαία σχεδιασμένη βάση Φ μπορεί να θεωρηθεί σαν καθολική στρατηγική κωδικοποίησης, δεδομένου ότι δεν χρειάζεται να σχεδιαστεί με βάση την δομή της βάσης Ψ. (Η γνώση και η δυνατότητα εφαρμογής της βάσης Ψ απαιτείται μόνο για την αποκωδικοποίηση ή την αποκατάσταση του σήματος f). Αυτή η

καθολικότητα μπορεί να είναι ιδιαίτερα χρήσιμη σε μια πηγή κωδικοποίησης σε καταστάσεις πολλαπλών σημάτων (multi-signals) όπως τα δίκτυα αισθητήρων (network sensors) [6]. Επομένως μπορούμε να συμπεράνουμε ότι η συμπιεσμένη δειγματοληψία βρίσκει εφαρμογή στα δίκτυα αισθητήρων.

Ένας άλλος τομέας στον οποίο εφαρμόζεται η συμπιεσμένη δειγματοληψία είναι αυτός της κωδικοποίησης καναλιών. Πιο συγκεκριμένα οι αρχές που διέπουν την συμπιεσμένη δειγματοληψία μπορούν να αναστραφούν και να εφαρμοστούν έτσι ώστε να σχεδιάζουν γρήγορους κώδικες διόρθωσης λάθους για να προστατεύουν από λάθη κατά τη διάρκεια της μετάδοσης [7].

Επιπλέον η συμπιεσμένη δειγματοληψία χρησιμοποιείται για την επίλυση των αντιστρόφων προβλημάτων. Πιο συγκεκριμένα, σε διάφορες άλλες καταστάσεις, ο μόνος τρόπος για να αποκτηθεί το σήμα f είναι να χρησιμοποιηθεί ένα σύστημα μέτρησης Φ μιας ορισμένης μορφής. Εντούτοις, θεωρώντας μια αραιή βάση Ψ η οποία προέρχεται από το f και δεν έχει καμία συνοχή με την βάση Φ, μπορούμε να πραγματοποιήσουμε μια αποδοτική δειγματοληψία. Μια τέτοια εφαρμογή είναι η MR angiography [8], όπου η βάσης Φ καταγράφει ένα υποσύνολο του μετασχηματισμού Φουριέ, και της επιθυμητής εικόνας f [2].

Μια άλλη εφαρμογή η οποία χρησιμοποιεί τη θεωρία της συμπιεσμένης δειγματοληψίας είναι η απόκτηση στοιχείων. Σε μερικές σημαντικές καταστάσεις η πλήρης συλλογή n χρονικά μεμονωμένων δειγμάτων ενός αναλογικού σήματος μπορεί να είναι δύσκολη να πραγματοποιηθεί (και ενδεχομένως δύσκολη στη συνέχεια και η συμπίεση). Εδώ, θα ήταν χρήσιμο να σχεδιαστούν φυσικές συσκευές δειγματοληψίας που καταγράφουν άμεσα ιδιαίτερα χαμηλού ρυθμού ασυνάρτητες μετρήσεις του συναφούς αναλογικού σήματος [2].

Η εφαρμογή που περιγράψαμε ακριβώς παραπάνω προτείνει ότι οι μαθηματικές και υπολογιστικές μέθοδοι θα μπορούσαν να ασκήσουν τεράστια επίδραση στις περιοχές όπου ο παραδοσιακός σχεδιασμός λογισμικού έχει σημαντικούς περιορισμούς. Παραδείγματος χάριν, οι συμβατικές (παραδοσιακές) συσκευές απεικόνισης που χρησιμοποιούν την τεχνολογία CCD ή CMOS περιορίζονται ουσιαστικά στο ορατό φάσμα. Εντούτοις, μια κάμερα που χρησιμοποιεί την μέθοδο Compressive Sensing που συλλέγει μετρήσεις χωρίς συνοχή χρησιμοποιώντας ένα ψηφιακό πίνακα micromirror (και απαιτεί μόνο ένα φωτοευαίσθητο στοιχείο αντί των εκατομμυρίων) θα μπορούσε σημαντικά να επεκτείνει αυτές τις ικανότητες [9] [2].

Επιπροσθέτως, στην αυτοματοποιημένη τομογραφία, για παράδειγμα, κάποιος θα επιθυμούσε να λάβει εικόνα του εσωτερικού ενός ανθρώπινου σώματος με τη λήψη εικόνων ακτίνας Χ από διαφορετικές γωνίες. Ωστόσο η λήψη ενός σχεδόν πλήρους συνόλου εικόνων θα εξέθετε τον ασθενή σε μια μεγάλη και επικίνδυνη δόση της ακτινοβολίας. Ως εκ τούτου το ποσό μετρήσεων πρέπει να είναι όσο το δυνατόν μικρότερο, και παράλληλα να εγγυάται μια αρκετά καλή ποιότητα εικόνας. Τέτοιες εικόνες είναι συνήθως σχεδόν σταθερά τμηματοποιημένες και επομένως σχεδόν αραιές (sparse) στην κλίση. Γι' αυτό το λόγο η συμπιεστική δειγματοληψία βρίσκει εφαρμογή σε αυτήν αυτοματοποιημένη τομογραφία. Και πράγματι, είναι ακριβώς αυτή η εφαρμογή που άρχισε τις έρευνες πάνω στη συμπιεστική δειγματοληψία [8] [1].

Επίσης η απεικόνιση ραντάρ φαίνεται να είναι μια πολύ ελπιδοφόρος εφαρμογή για την συμπιεστική δειγματοληψία. Κάποιος συνήθως παρακολουθεί μόνο έναν μικρό αριθμός στόχων, και ως εκ τούτου η αραιότητα (sparsity) είναι μια πολύ ρεαλιστική υπόθεση. Οι τυποποιημένες μέθοδοι για την απεικόνιση ραντάρ χρησιμοποιούν την υπόθεση της αραιότητας, αλλά μόνο στο τέλος της διαδικασίας επεξεργασίας σήματος, προκειμένου να καθαριστεί ο θόρυβος στην προκύπτουσα εικόνα. Η συστηματική χρησιμοποίηση της αραιότητας από την αρχή με την εκμετάλλευση των μεθόδων της συμπιεστικής δειγματοληψίας είναι μια φυσική προσέγγιση.

Συμπερασματικά θα μπορούσαμε να πούμε ότι η συμπιεστική δειγματοληψία μπορεί ενδεχομένως να χρησιμοποιηθεί σε όλες τις εφαρμογές όπου ο στόχος είναι η αναδημιουργία ενός σήματος ή μιας εικόνα από τις γραμμικές μετρήσεις, ενώ από την άλλη μεριά το να παίρνεις πολλές από εκείνες τις μετρήσεις (πιο συγκεκριμένα, ένα πλήρες σύνολο από μετρήσεις) αποτελεί μια δαπανηρή, μεγάλη, δύσκολη, επικίνδυνη, αδύνατη ή αλλιώς μια ανεπιθύμητη διαδικασία. Επιπλέον, υπάρχουν λόγοι έτσι ώστε να θεωρηθεί ότι το σήμα είναι αραιό σε μια κατάλληλη βάση (ή κατάλληλο πλαίσιο). Εμπειρικά, το τελευταίο ισχύει για τους περισσότερους τύπους σημάτων [1].

4.5 Λογισμικό συμπιεσμένης δειγματοληψίας

Στην υποενότητα αυτή θα παραθέσουμε έναν κώδικα Matlab ο οποίος λύνει το πρόβλημα της ανάκτησης ενός αραιού – διεσπαρμένου σήματος χρησιμοποιώντας την μέθοδο $\ell 1$-minimization. Όπως θα δούμε παρακάτω χρησιμοποιώντας αυτό το κώδικα έχουμε μια ακριβής αναπαράσταση του αρχικού σήματος σχεδόν χωρίς κανένα λάθος.

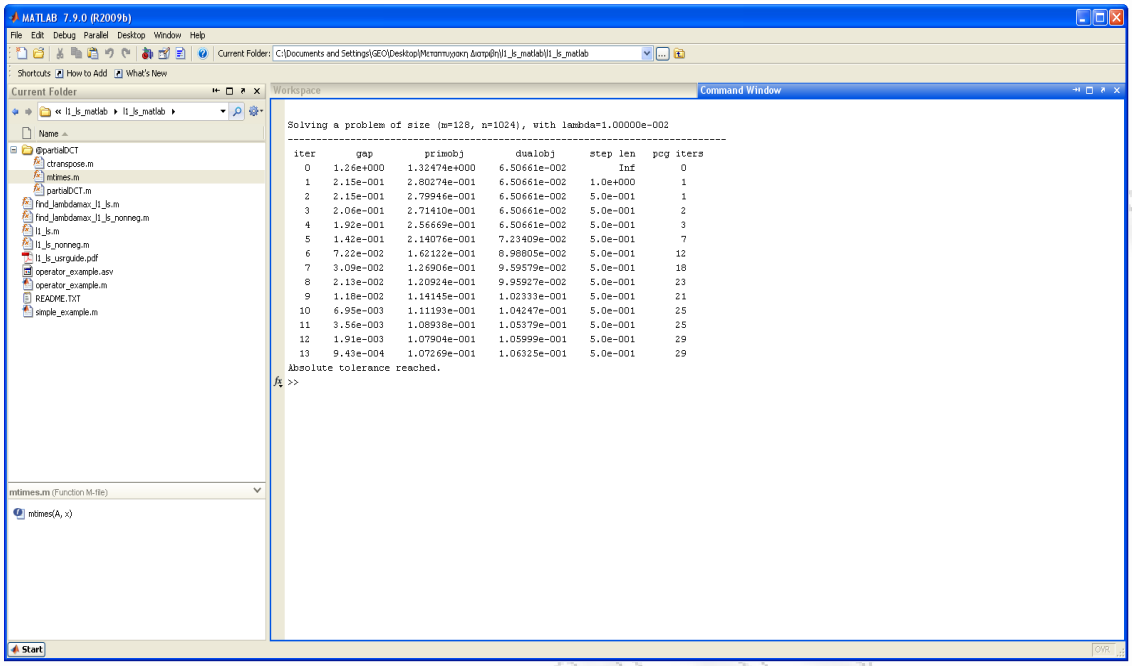
```
% Matlab script το οποίο λύνει το πρόβλημα της ανάκτησης ενός αραιού - διεσπαρμένου
σήματος χρησιμοποιώντας τον object-oriented programming της Matlab.

rand('state',0);randn('state',0);   % αρχεικοποίηση

n = 1024;   % Διάσταση σήματος
m = 128;    % Αριθμός μετρήσεων

J = randperm(n); J = J(1:m);    % Τυχαία μετάθεση ενός integer 1:m δηλαδή 1:128 μιας και
έχουμε θέσει m=128

% Δημιουργία μιας m*n DCT μήτρας της οποίας οι m σειρές, είναι σειρές της
% n*n DCT μήτρας στους πινάκες που έχουν καθορισθεί από το J
A  = partialDCT(n,m,J); % Δημιουργία της μήτρας A
At = A';                % Αντιμετάθεση της μήτρας A

% Δημιουργία σήματος
T  = 10; %Ορισμός T και ανάθεση τιμής όπου T αριθμός ακίδων
x0 = zeros(n,1); % Επιστρέφει έναν πίνακα nx1 με μηδενικά
q  = randperm(n); % Τυχαία μετάθεση του q
x0(q(1:T)) = sign(randn(T,1));

% Παρατηρήσεις για θόρυβο
sigma = 0.01;   % απόκλιση θορύβου
y = A*x0 + sigma*randn(m,1); % Συνάρτηση υπολογισμού του θορύβου

lambda  = 0.01; % Ρύθμιση παραμέτρων
rel_tol = 0.01; % Συγκριτικός στόχος ανεκτικότητας

% Εκτέλεση του l1-regularized least squares solver
[x,status]=l1_ls(A,At,m,n,y,lambda,rel_tol);

% Μετά από την εκτέλεση του κώδικα η εικόνα figure 1 μας δίνει τα αποτελέσματα
figure(1)
subplot(2,1,1); bar(x0); ylim([-1.1 1.1]); title('original signal x0');
subplot(2,1,2); bar(x);  ylim([-1.1 1.1]); title('reconstructed signal x');
```

Η συνάρτηση l1-regularized least squares solver, η οποία καλείται από το παραπάνω κώδικα Matlab, ουσιαστικά λύνει το πρόβλημα της παρακάτω μορφής:

minimize ||A*x-y||^2 + lambda*sum|x_i|

Όπως μπορούμε να δούμε τα αποτελέσματα αυτής της συνάρτησης είναι το x και το status. Το x είναι ένα n – διάνυσμα ενώ το status είναι μια συμβολοσειρά (string). Στην περίπτωση που το status έχει τιμή «Solved» τότε το x που προκύπτει είναι η λύση, ενώ αν το status έχει τιμή «Failed» τότε το x είναι η τελευταία τιμή της επανάληψης.

Τρέχοντας λοιπόν το παραπάνω κώδικα Matlab, τα αποτελέσματα εξάγονται στη επιφάνεια εργασίας (workspace) της Matlab. Αυτά φαίνονται στην παρακάτω εικόνα.

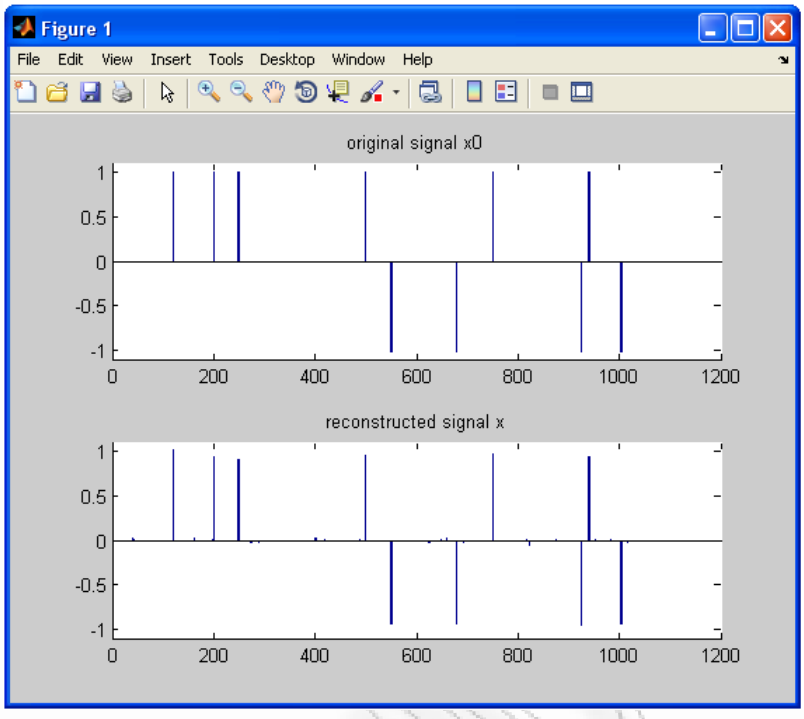


Εικόνα 4.4 Αποτελέσματα κώδικα

Τα αποτελέσματα είναι ένας πίνακας του οποίου οι στήλες αντιπροσωπεύουν τις επαναλήψεις της μεθόδου Truncated Newton interior – point [13]. Οι στήλες αντιπροσωπεύουν τα εξής:

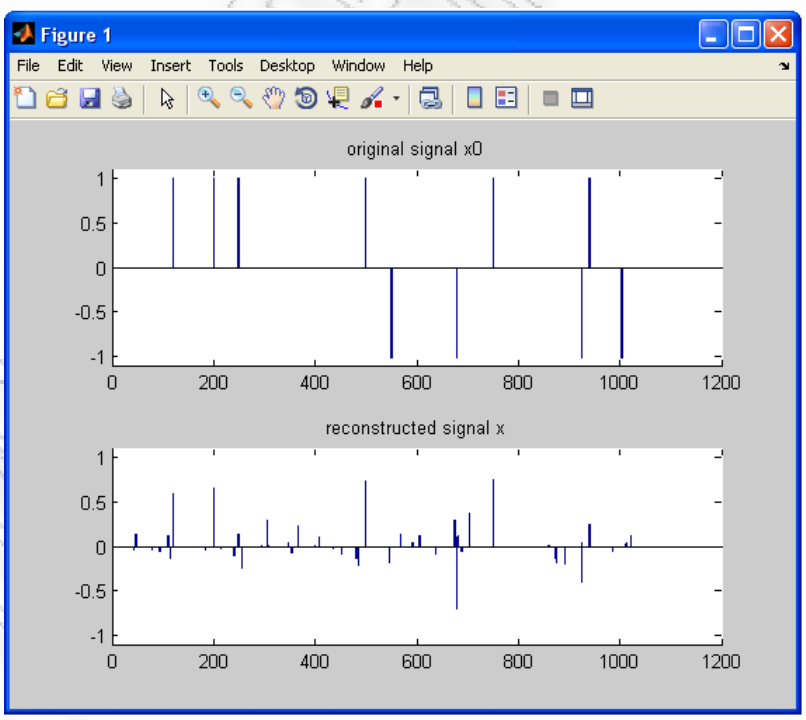
- Πρώτη στήλη → gap
- Δεύτερη στήλη → primal objective
- Τρίτη στήλη → dual objective
- Τέταρτη στήλη → step size
- Πέμπτη στήλη → pcg iterations
- Έκτη στήλη → pcg status flag

Τέλος τα αποτελέσματα παράγονται και σε μια εικόνα η οποία παρουσιάζει το αρχικό σήμα και το σήμα που προέκυψε από την μέθοδο.



Εικόνα 4.5 Αναπαράσταση original και reconstructed signal

Όπως μπορούμε να παρατηρήσουμε οι 128 μετρήσεις είναι το οριακό σημείο για να έχουμε μια 100% αναπαράσταση του αρχικού σήματος. Στην περίπτωση που οι μετρήσεις μας είναι κάτω από 128 τότε η αναπαράσταση του σήματος δεν είναι επιτυχής. Παρακάτω παραθέτουμε ένα παράδειγμα στο οποίο έχουμε θέσει n =54.



Εικόνα 4.6 Αναπαράσταση σήματος για n=54

4.6 Ανοιχτά Προβλήματα

Ο τομέας της συμπιεσμένης δειγματοληψίας είναι ένας τομέας σχετικά καινούργιος, με αποτέλεσμα να είναι πολλές οι κατευθύνσεις που πρέπει ακόμα να εξερευνηθούν. Στην συνέχεια αυτού του υποκεφαλαίου, θα απαριθμούμε δύο σοβαρά προβλήματα που παραμένουν άλυτα μέχρι τώρα.

4.6.1 Ντετερμενιστικοί πίνακες συμπιεσμένης δειγματοληψίας

Μέχρι στιγμής, μόνο μερικοί τύποι τυχαίων πινάκων $A \in C^{mxN}$ είναι γνωστό ότι μπορούν να ικανοποιήσουν την προυπόθεση RIP $\delta_S \le \delta \le 0,4$ με

$$m = C_\delta slog^a(N) \quad (10)$$

για κάποια σταθερά C_δ και για κάποιο εκθέτη a (με υψηλή πιθανότητα). Ωστόσο αυτό το οποίο είναι ακόμα ανοιχτό και το οποίο χρήζει συζήτησης είναι αν μπορούμε να δημιουργήσουμε ντετερμινιστικούς και σαφής πίνακες mxN οι οποίοι να ικανοποιούν το RIP $\delta_S \le \delta \le 0,4$ για ένα επιθυμητό εύρως της σχέσης (10) [1].

Για να παρέχει κανείς υπολογισμούς RIP με βάση την σχέση (9) πρέπει αρχικά να ακυρώσει όλες τις θετικές και αρνητικές εισαγωγές στον πίνακα. Αυτό όμως γίνεται «αυτόματα» με την βοήθεια μεθόδων από τον τομέα των πιθανοτήτων. Ωστόσο παρουσιάζει μεγάλη δυσκολία να εκμεταλλευτούμε το γεγονός αυτό, όταν ο δοθέν πίνακας είναι ντετερμινιστικός [1].

Οι καλύτερες κατασκευές ντετερμινιστικών πινάκων συμπιεσμένης δειγματοληψίας μέχρι στιγμής χρησιμοποιούν ντετερμινιστικούς αποσυμπιεστές γραφικών παραστάσεων [11]. Οι γνωστότεροι ντετερμινιστικοί αποσυμπιεστές αποφέρουν μια αραιή αποκατάσταση υπό την εξής συνθήκη :

$$m \ge Cs(logN)^{clog^2(N)} \quad (11)$$

Παρ όλο που η κλίμακα του s είναι γραμμική, πράγμα το οποίο είναι επιθυμητό,ο $(logN)^{clog^2(N)}$ όρος αυξάνεται γρηγορότερα από οποιοδήποτε πολυώνυμο του $logN$. Ένα άλλο μειονέκτημα είναι ότι οι ντετερμινιστικοί αποσυμπιεστές γραφικών παραστάσεων είναι οι έξοδος ενός πολυωνιμικού χρονικού αλγορίθμου, και αυτό το γεγονός προκαλέι ερωτήματα εάν το αποτέλεσμα του πίνακα μπορεί να θεωρηθεί σαφές [1].

Επομένως μπορούμε να συμπεράνουμε ότι ακόμα δεν είναι εφικτό να δημιουργήσουμε ντετερμινιστικούς και σαφής πίνακες mxN οι οποίοι να ικανοποιούν το RIP $\delta_S \le \delta \le 0,4$ για ένα επιθυμητό εύρως της σχέσης (10).

4.6.2 Απομάκρυνση των παραγόντων log από τον υπολογισμό του Fourier-RIP

Είναι γνωστό ότι ένας τυχαίος Φουριερ πίνακας $A \in C^{mxN}$ ικανοποιεί το RIP με υψηλή πιθανότητα αρκεί να ισχύει ότι:

$$\frac{m}{\log(m)} \ge C_\delta slog^2(s)\log(N) \quad (12)$$

Ωστόσο αποτελεί εικασία να πιστεύει κανείς ότι μπορούν να απομακρυνθούν οι παράγοντες του log. Παρ όλα αυτά είναι δύσκολο να βελτιωθεί η παραπάνω σχέση (12) σε ένα

καλύτερο υπολογισμό από τον $m \geq C_{\delta} s\log^2(s)\log(N)$. Πράγματι, αυτό υπονοεί το συμπέρασμα του Talagrand σχετικά με την ισότητα των πινάκων I1 και I2 ενός γραμμικού συνδυασμού ενός υποσυνόλου χαρακτήρων [12] [1].

Επομένως και εδώ παρατηρούμε ότι είναι ακόμα δύσκολο να απομακρύνουμε τους παράγοντες log από τον υπολογισμό του Fourier-RIP πράγμα το οποίο οδηγεί στην δυσκολία αντιμετώπισης του υπολογισμού της σχέσης (12).

4.7 Συμπεράσματα

Η συμπιεσμένη δειγματοληψία έχει ήδη καθιερωθεί ως μια νέα θεωρία δειγματοληψίας η οποία επιδεικνύει θεμελιώδεις συνδέσεις με διάφορους μαθηματικούς τομείς, όπως οι πιθανότητες, η γεωμετρία και η θεωρία της πολυπλοκότητας. Η σύνδεση με την βελτιστοποίηση και τη ανάπτυξη των πολύ αποδοτικών και γερών αριθμητικών μεθόδων κάνουν την συμπιεσμένη δειγματοληψία μια έννοια χρήσιμη για ένα ευρύ φάσμα εφαρμογών όπως η φυσική επιστήμη, η εφαρμοσμένη μηχανική, και η απόκτηση και επεξεργασία εικόνας από ένα σήμα. Πολύ είναι αυτοί που πιστεύουν ότι η συμπιεσμένη δειγματοληψία θα εισαχθεί σε διάφορους κλάδους της επιστήμης και της τεχνολογίας και θα έχει ξεχωριστή επίδραση πάνω σε αυτούς. Ωστόσο αυτή την στιγμή υπάρχουν πολλά ανοιχτά θέματα τα οποία πρέπει πρώτα να επιλυθούν.

Πρόσφατες μελέτες προτείνουν νέες πιθανές επεκτάσεις της συμπιεσμένης δειγματοληψίας σε πιο σύνθετες δομές. Επιπλέον, νέες προκλήσεις προκύπτουν τώρα στις αριθμητικές αναλύσεις και στην προσομοίωση όπου προβλήματα υψηλών διαστάσεων (π.χ., πιθανολογικές διαφορικές εξισώσεις στους υπολογισμούς δομών χρηματοδότησης και ηλεκτρονίων στη χημεία και τη βιοχημεία) έχουν προκαλέσει αδιέξοδο. Σε αυτό το πλαίσιο η συμπιεσμένη δειγματοληψία είναι μια πολλά υποσχόμενη ιδέα η οποία μπορεί στο μέλλον να υποστηρίξει την ανάπτυξη διάφορων τυχαίων αλγορίθμων. Τέλος, η θεωρία της συμπιεσμένη δειγματοληψία παρέχει βοήθεια για μια περαιτέρω επέκταση της στεγανογραφίας για την οποία αναφερθήκαμε στα προηγούμενα κεφάλαιά μας.

Βιβλιογραφία

[1] Massimo Fornasier and Holger Rauhut “Compressing Sensing”, April 2010

[2] Emmanuel J. Candès and Michael B. Wakin An introduction to Compressive Sampling IEEE Signal Processing Magazine March 2008.

[3] M. Unser. Sampling—50 Years after Shannon. Proceedings of the IEEE, 88(4):569–587, 2000.

[4] Fred Harris “Compressive Sensing” IEEE Signal Processing Magazine July 2007.

[5] Cleve Moler “Magic Reconstruction: Compressed Sensing” MathWorks News&Notes 2010.

[6] D. Baron, M.B. Wakin, M.F. Duarte, S. Sarvotham, and R.G. Baraniuk, “Distributed compressed sensing,” 2005, Preprint.

[7] E. Candès and T. Tao, “Decoding by linear programming,” IEEE Trans. Inform. Theory, vol. 51, no. 12, pp. 4203-4215, Dec. 2005.

[8] E. Candès, J. Romberg, and T. Tao, “Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information,” IEEE Trans. Inform. Theory, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[9] D. Takhar, V. Bansal, M. Wakin, M. Duarte, D. Baron, K.F. Kelly, and R.G. Baraniuk, “A compressed sensing camera: New theory and an implementation using digital micromirrors,” in Proc. Comp. Imaging IV SPIE Electronic Imaging, San Jose, CA, 2006.

[10] CCD vs. CMOS http://www.dalsa.com/corp/markets/ccd_vs_cmos.aspx

[11] R. Berinde, A. Gilbert, P. Indyk, H. Karloff, and M. Strauss. “Combining geometry and combinatorics: A unified approach to sparse signal recovery.” Preprint, 2008.

[12] M. Talagrand. “Selecting a proportion of characters.” Israel J. Math., 108:173–191, 1998.

[13] The method Truncated Newton interior – point http://cslgreenhouse.csl.illinois.edu /allertonarchives/allerton07/PDFs/papers/0013.pdf

Κεφάλαιο 5

Εφαρμογή Στεγανογραφίας

5.1 Εισαγωγή

Στο κεφάλαιο αυτό θα αναλύσουμε τα αποτελέσματα που προέκυψαν από τα πειράματα που πραγματοποιήσαμε χρησιμοποιώντας μια υψηλού επιπέδου γλώσσα αυτή της Matlab. Αρχικά θα κάνουμε μια εισαγωγή στους τύπους εικόνας που χρησιμοποιήσαμε στα πειράματα μας και στην συνέχεια θα αναλύσουμε τον κώδικα και τον αλγόριθμο που χρησιμοποιήσαμε. Τέλος θα συγκεντρώσουμε τα αποτελέσματα μας τα οποία θα τοποθετηθούν σε πίνακες και θα εξάγουμε τα συμπεράσματά μας δίνοντας παράλληλα λύσεις σε τυχών αδυναμίες που προέκυψαν.

5.2 Τύποι εικόνων

Στα πειράματα που θα πραγματοποιήσουμε παρακάτω χρησιμοποιούμε δύο ειδών εικόνες: τις grayscale εικόνες και τις RGB εικόνες. Παρακάτω θα κάνουμε μια μικρή αναφορά για αυτούς τους δύο τύπους εικόνας.

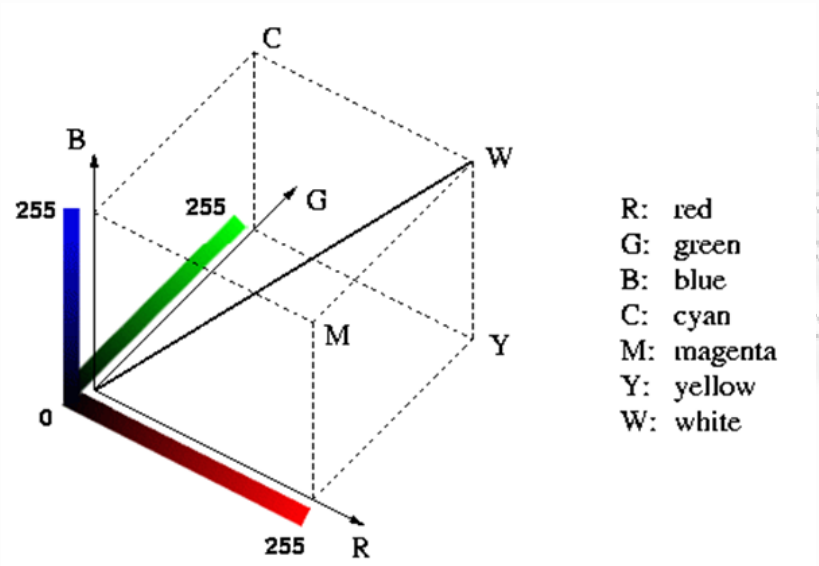
5.2.1 Grayscale εικόνες

Μια grayscale εικόνα είναι μια εικόνα της οποίας τα χρώματα είναι στις αποχρώσεις του γκρι. Αυτό το οποίο κάνει τις grayscale εικόνες να διαφέρουν από όλες τις άλλες έγχρωμες είναι ότι χρειάζονται πολύ λίγη πληροφορία για την αναπαράσταση του κάθε εικονοστοιχείου (pixel). Μια grayscale εικόνα είναι ένας πίνακας δεδομένων, του οποίου οι τιμές του αντιπροσωπεύουν την ένταση του κάθε pixel μέσα στο διάστημα τιμών από 0 έως 1.

Το MatLab αποθηκεύει μια grayscale εικόνα σαν ένα μονοδιάστατο πίνακα με κάθε στοιχείο του πίνακα να αντιπροσωπεύει ένα εικονοστοιχείο της εικόνας. Ο πίνακας μπορεί να είναι της τάξεως double, unit8 ή unit16. Τα στοιχεία στον πίνακα δεδομένων της εικόνας αντιπροσωπεύουν διάφορες εντάσεις ή αλλιώς αποχρώσεις του γκρι, όπου η ένταση 0 συνήθως αντιπροσωπεύει το μαύρο, και η ένταση 1 το άσπρο.

5.2.2 RGB εικόνες

Μία μονόχρωμη (ή γκρι) ψηφιακή εικόνα είναι ένας πίνακας από αριθμούς που αντιπροσωπεύουν τη φωτεινότητα κάθε εικονοστοιχείου (pixel). Η ένταση του κάθε pixel κλιμακώνεται σε 28 = 256 επίπεδα του γκρι, έτσι ώστε κάθε pixel να απαιτεί 8 bits για αποθήκευση στη μνήμη, γι' αυτό άλλωστε και λέγεται εικόνα 8-bit. Οι έγχρωμες εικόνες αναπαρίστανται από 3 σύνολα πινάκων, ένα για κάθε βασικό χρώμα : κόκκινο, πράσινο, μπλε. Η βασική ιδέα είναι ότι κάθε χρώμα μπορεί να αναπαρασταθεί αναμιγνύοντας ποσότητες βασικών χρωμάτων [1]. Παρατηρήστε τον κύβο RGB που δείχνει την κατανομή των χρωμάτων στο χώρο:



Εικόνα 5.1 Σχηματική αναπαράσταση κύβου RGB.

Πηγή: (Grokking the GIMP)

Σε κάθε άξονα τα χρώματα κυμαίνονται από μηδενική έως πλήρη συνεισφορά. Ο κύβος είναι στερεός και κάθε σημείο μέσα του καθορίζεται από τρία νούμερα (rgb). Η διαγώνιος από το μαύρο (0,0,0) προς το λευκό (1,1,1) αναπαριστά όλα τα γκρι, που σημαίνει ότι εδώ όλα τα κόκκινα, πράσινα και μπλε στοιχεία είναι ίσα. Πρακτικά τα διαφορετικά συστήματα υλικού και λογισμικού χρησιμοποιούν διαφορετικές κλίμακες για τα χρώματα με πιο κοινές τις 0 - 256 και 0 – 65536 για κάθε στοιχείο. Σημαντικό είναι το γεγονός ότι ο RGB χώρος αναπαριστά λιγότερα χρώματα απ' όσα μπορεί ο άνθρωπος να δει.

Στο Matlab η αναπαράσταση μιας RGB εικόνας διαστάσεων M x N γίνεται με έναν πίνακα τριών διαστάσεων M x N x 3 που περιέχει pixel χρώματος. Κάθε pixel είναι μια τριπλέτα χρωμάτων που αντιστοιχεί στις συνιστώσες του κόκκινου, του πράσινου και του μπλε για το συγκεκριμένο σημείο. Μια RGB εικόνα, δηλαδή, μπορεί να αναπαρασταθεί ως μια «στοίβα» από τρείς gray-scale εικόνες οι οποίες όταν τροφοδοτηθούν στις εισόδους για κόκκινο, πράσινο και μπλε μιας έγχρωμης οθόνης παράγουν μια έγχρωμη εικόνα. Οι RGB εικόνες αποθηκεύονται σαν 24-bit εικόνες , όπου καθεμία από τις χρωματικές συνιστώσες είναι 8-bit. Αυτό αποδίδει περίπου 16 εκατομμύρια χρώματα. Η ακρίβεια με την οποία μια κανονική εικόνα αναπαρίσταται μας οδήγησε στον όρο «εικόνα πραγματικών χρωμάτων». Ένας πίνακας RGB στο MatLab μπορεί να είναι της τάξεως double, unit8, ή unit16

Παρακάτω δίνεται ένας πίνακας από την Matlab με τις αντιστοιχίες των χρωμάτων με τις RGB τιμές τους:

RGB Τιμή	Χρώμα
[1 1 0]	κίτρινο
[1 0 1]	φούξια
[0 1 1]	κυανό
[1 0 0]	κόκκινο
[0 1 0]	πράσινο
[0 0 1]	μπλε
[1 1 1]	λευκό
[0 0 0]	μαύρο
[0.5 0.5 0.5]	γκρι
[0.5 0 0]	βαθύ κόκκινο

[1 0.62 0.4]	χάλκινο
[0.49 1 0.83]	κυανοπράσινο

5.3 Παρουσίαση κώδικα υλοποίησης

Στην συγκεκριμένη υποενότητα θα παρουσιάσουμε αναλυτικά τον κώδικα Matlab που χρησιμοποιήσαμε με σκοπό να παρατηρήσουμε το ποσοστό των σωστών εικονοστοιχείων μεταξύ της αρχικής εικόνας και της στεγο-εικόνας η οποία βελτιώθηκε μέσω του λογισμικού BM3D που θα δούμε στην επόμενη υποενότητα. Θα πρέπει να επισημάνουμε ότι υπάρχουν δύο ξεχωριστοί κώδικες ένας για τις εικόνες grayscale και ένας για τις RGB εικόνες. Και στους δύο κώδικες το αποτέλεσμα είναι μια εικόνα που δείχνει την αρχική εικόνα, την στεγο-εικόνα και την διορθωμένη εικόνα. Επίσης στο Command Window του Matlab εκτυπώνεται κάθε φόρα και το ποσοστό.

5.3.1 Κώδικας για τις grayscale εικόνες

Ο κώδικας για τις grayscale εικόνες είναι ο εξής:

```
% Matlab script for comparing initial image and a compressive sensing image
% using the algorithm MB3D. In order to do this we create a stego image
% importing into the initial image the random message and then we use BM3D
% to create the compressive sensing image. Finally we implement xor
% between initial and compressive sensing image and produce the percent of
% right pixels.

close all; clc; clear perc;

files = dir('*.gif'); % select between .pgn or .tiff or .gif

for k = 1:numel (files) % start the loop

rand('state',0); randn('state',0);

% input original image
y = im2double(imread(files(k).name)); %convert a grayscale image to a double matrix
y_uint8 = uint8(256*y); %convert image to a uint8 form
y_uint8_mod2 = mod(y_uint8,2); % implement mod2 to the image

% create a random message
message =round(rand(size(y)));%grayscale image
message_uint8 = uint8(message);

% parameters
sigma = 0.1;   % noise standard deviation

%create the staganography image
z = y+sigma*message; %grayscale image
z_1 =mat2gray(z); %convert the matrix to a grayscale image

%run the function to create compressive sensing image
[PSNR, y_est] = BM3D(y, z, sigma); %grayscale image

%xor the compressive sensing image with the initial
y_est_uint8 = uint8(256*y_est); %grayscale image
y_est_uint8_mod2 = mod(y_est_uint8,2); % implement mod2 to the image
```

```
K = bitxor(y_uint8_mod2, y_est_uint8_mod2); %implement xor
K_uint8 = uint8(K);
K = bitxor(K_uint8, message_uint8); %implement xor

% Find the percent of right pixels
final = find(K==0); %find the zeros
final_number = length(final(:,1));%count the length of the zeros
[b1, b2] = size(y); % find the dimension of the picture
total =  b1*b2; %count the size of the image
perc(k) = final_number/total; %find the percent

%display figure
figure(k)
subplot(k,3,1), imshow(y), title('Original image');
subplot(k,3,2), imshow(z_1),  title('Steganography image');
subplot(k,3,3), imshow(y_est),  title('Fixed image');

end %end of the loop

%display the perscent
disp('The percent of right pixels between initial images and fixed is in the matrix perc at
workspace')
```

Ο παραπάνω κώδικας ξεκινάει με την εντολή close all; clc; clear perc; η οποία κλείνει όλα τα ανοιχτά παράθυρα του Matlab, καθαρίζει το Command Window του Matlab και τέλος μηδενίζει τον πίνακα perc στο οποίο αποθηκεύονται κάθε φορά τα αποτελέσματα. Έπειτα υπάρχει η εντολή files = dir('*.gif'); η οποία μπορεί να μετατραπεί είτε σε files = dir('*.tiff'); είτε σε files = dir('*.png');. Η εντολή αυτή φορτώνει όλες τις εικόνες που υπάρχουν μέσα στο φάκελο Steganography με σκοπό να τις χρησιμοποιήσει στο loop που υπάρχει παρακάτω.

Στην αρχή του κώδικα υπάρχει ένας βρόγχος (loop) ο οποίος χρησιμοποιείται για να λαμβάνει κάθε φορά τις εικόνες που χρειάζονται για την εκτέλεση του πειράματος και να εξάγει τα αποτελέσματα. Με την εντολή for k = 1:numel (files) ξεκινάει το loop και «τραβάει» μια-μια τις εικόνες ξεκινώντας από την 1 μέχρι την τελευταία. Ο σκοπός για τον οποίο βάλαμε numel στην παραπάνω εντολή είναι γιατί κάθε φορά έχουμε διαφορετικό πλήθος εικόνων. Με τον βρόγχο αυτό εκτελούνται όλες οι εντολές που βρίσκονται μέσα στο σώμα του βρόγχου για κάθε εικόνα. Το αποτέλεσμα που προκύπτει αποθηκεύεται μέσα στο πίνακα perc. Ο βρόχος τελειώνει με την εντολή end.

Στην συνέχεια θα αναφερθούμε στις εντολές που υπάρχουν μέσα στο βρόγχο Αρχικά εισάγουμε την πρώτη εικόνα με την βοήθεια της εντολής y = im2double(imread(files(k).name)); η οποία ουσιαστικά αφού διαβάσει την εικόνα την μετατρέπει σε ένα πίνακα με στοιχεία της μορφής double. Έπειτα μετατρέπουμε τον πίνακα που προέκυψε από την εισαγωγή της εικόνας σε μορφή uint8 με την εντολή y_uint8 = uint8(256*y); πράγμα το οποίο θα μας βοηθήσει να εκτελέσουμε την πράξη XOR πιο κάτω. Θα πρέπει εδώ να επισημάνουμε ότι πολλαπλασιάζουμε τον πίνακα y με το 256 έτσι ώστε να πάρουμε την τιμή κάθε εικονοστοιχείου της εικόνας. Τέλος εφαρμόζουμε mod2 στον πίνακα y_uint8 για να πάρουμε το 1 ή το 0 που είναι τα τελευταία μικρής σημαντικότητας bits του κάθε εικονοστοιχείου.

Στην συνέχεια δημιουργούμε ένα τυχαίο μήνυμα χρησιμοποιώντας την εντολή message =round(rand(size(y))); Το μήνυμα αυτό θα εισαχθεί μέσα στην εικόνα με αποτέλεσμα να δημιουργηθεί η στεγο-εικόνα. Παρατηρούμε εδώ ότι ο πίνακας που δημιουργήθηκε για το τυχαίο μήνυμα χρησιμοποιεί την συνάρτηση size() της Matlab με σκοπό να δημιουργηθεί ο πίνακας message ο οποίος να έχει τις ίδιες διαστάσεις με την εικόνα. Αυτό είναι λογικό διότι το μήνυμα θα εισαχθεί στην εικόνα με την πράξη της πρόσθεσης και όπως καλά γνωρίζουμε για να προσθέσουμε δύο πίνακες γραμμικά, θα πρέπει να είναι των ίδιων διαστάσεων. Τέλος με την εντολή message_uint8 = uint8(message); μετατρέπουμε τον πίνακα message σε πίνακα της μορφής uint8.

Για την δημιουργία της στεγο-εικόνας χρησιμοποιούμε την εντολή z = y+sigma*message;. Η εντολή z_1 = mat2gray(z); που ακολουθεί απλά μετατρέπει τον πίνακα που προέκυψε σε εικόνα τύπου grayscale. Αφού λοιπόν έχουμε παράγει την στεγο-εικόνα εφαρμόζουμε πάνω της την συνάρτηση BM3D(y, z, sigma) με σκοπό την βελτίωση της ποιότητας της εικόνας. Για την λειτουργία αυτής της συνάρτησης θα μιλήσουμε στην επόμενη υποενότητα. Η εντολή sigma = 0.1; είναι μια παράμετρος θορύβου που προστίθεται στην εικόνα.

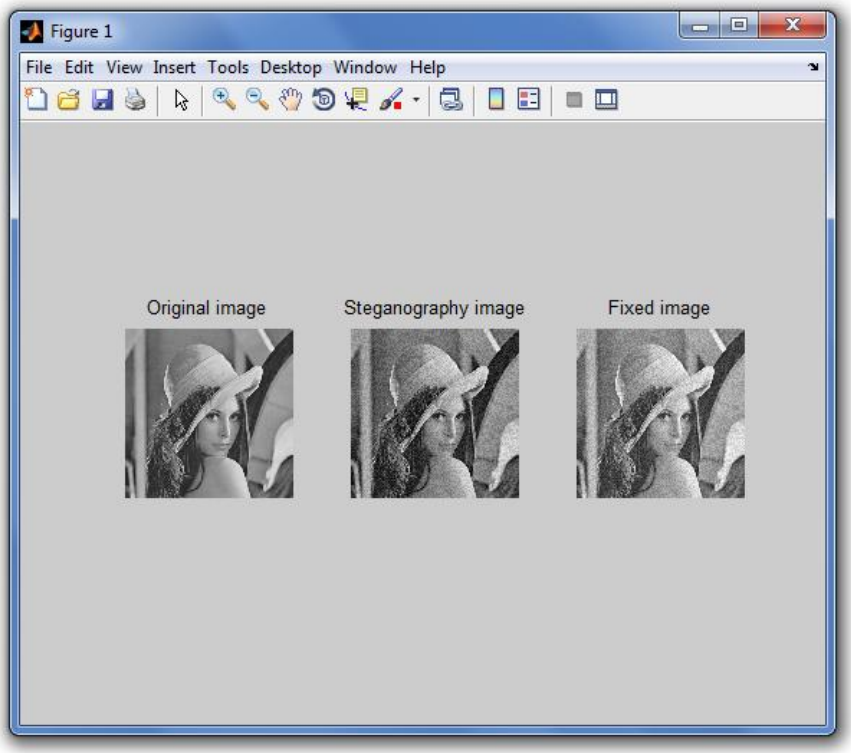
Η βελτιωμένη εικόνα μας, η οποία είναι η y_est μετατρέπεται πια σε πίνακα της μορφής uint8 με την βοήθεια της εντολής y_est_uint8 = uint8(256*y_est);.Θα πρέπει εδώ να επισημάνουμε ότι πολλαπλασιάζουμε τον πίνακα y_est με το 256 έτσι ώστε να πάρουμε την τιμή κάθε εικονοστοιχείου της βελτιωμένης εικόνας. Τέλος εφαρμόζουμε mod2 στον πίνακα y_est_uint8 για να πάρουμε το 1 ή το 0 που είναι τα τελευταία μικρής σημαντικότητας bits του κάθε εικονοστοιχείου. Αυτό πραγματοποιείται με την εντολή y_est_uint8_mod2 = mod(y_est_uint8,2);.

Τώρα πια έχοντας την αρχική εικόνα κα την εικόνα βελτίωσης θα εκτελέσουμε την πράξη XOR. Αυτό πραγματοποιείται με την εντολή K = bitxor(y_uint8_mod2, y_est_uint8_mod2); Στην συνέχεια μετατρέπουμε τον πίνακα K σε μορφή uint8 με την εντολή K_uint8 = uint8(K);. Αυτό το πραγματοποιούμε επειδή θέλουμε να κάνουμε XOR τον πίνακα αυτό με το μήνυμα έτσι ώστε να βρούμε τα εικονοστοιχεία που είναι ίδια στην αρχική και την τελική εικόνα.

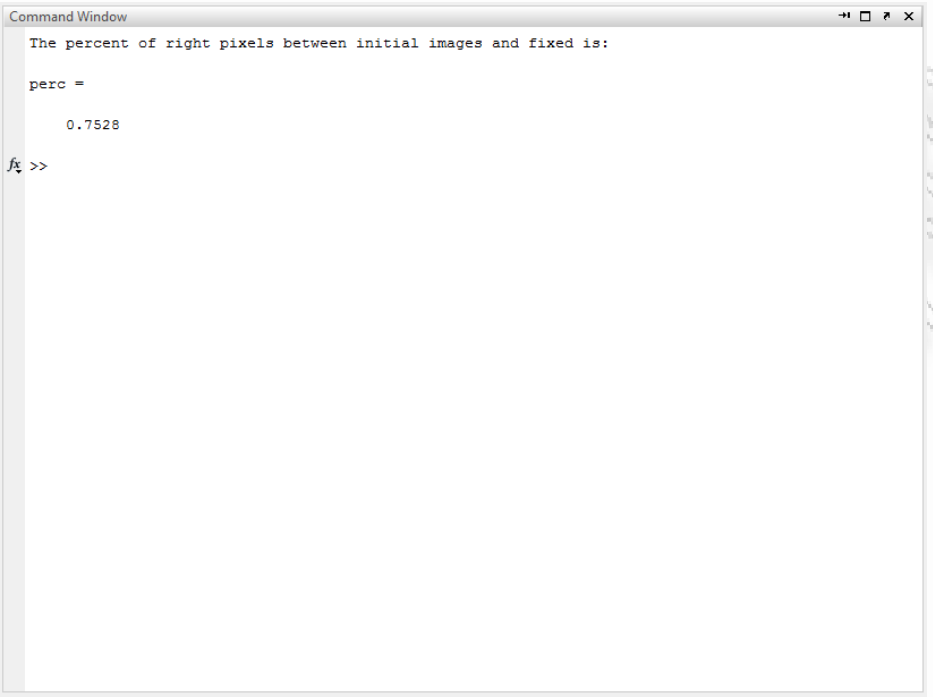
Αφού λοιπόν έχουμε πραγματοποιήσει την πράξη εκτελούμε τις εντολές final = find(K==0); και final_number = length(final(:,1)); που σκοπό έχει να εντοπίσει και να καταμετρήσει τα μηδενικά που υπάρχουν στο πίνακα της πράξης XOR. Καταμετρούμε τα μηδενικά και όχι τους άσσους γιατί τα μηδενικά είναι αυτά που λένε πόσα pixels είναι ίδια μεταξύ της αρχικής και της διορθωμένης εικόνας.

Τέλος με τις εντολές figure(1) subplot(1,3,1), imshow(y), title('original image'); subplot(1,3,2), imshow(z_1), title('steganography image'); subplot(1,3,3), imshow(y_est), title('Fixed image'); απλά εξάγουμε και τις τρεις εικόνες σε μια.

Ένα παράδειγμα υλοποίησης του παραπάνω κώδικα φαίνεται στην αμέσως επώνυμη εικόνα**.**



Εικόνα 5.2 Αποτέλεσμα κώδικα για grayscale εικόνα.



Εικόνα 5.3 Εμφάνιση ποσοστού στο Command Window.

Όπως μπορούμε να παρατηρήσουμε από την παραπάνω εικόνα το ποσοστό των σωστών pixels είναι 75,28%. Πράγμα το οποίο σημαίνει ότι το μήνυμα που κρύβεται πίσω από την αρχική εικόνα αλλοιώνει σε ποσοστό περίπου 25%. Ο θόρυβος ο οποίος παρουσιάζεται στη διορθωμένη εικόνα δεν θα πρέπει να μας ανησυχεί μιας και εμείς ενδιαφερόμαστε για τα εικονοστοιχεία του background και όχι της εικόνας.

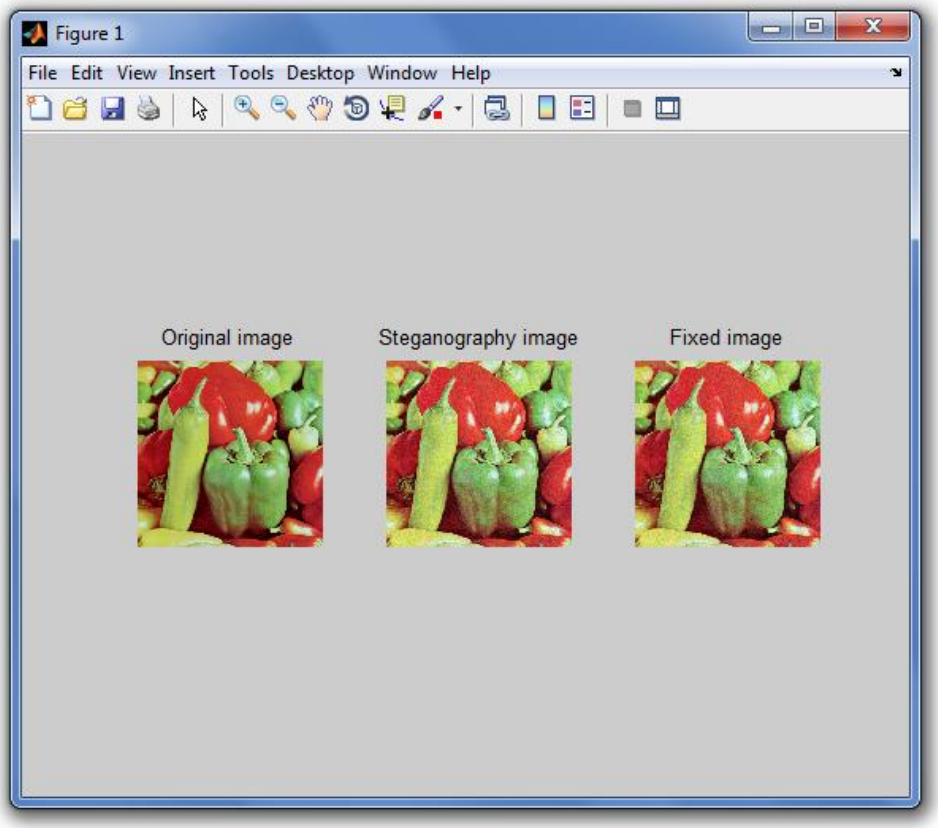
5.3.2 Κώδικας για τις RGB εικόνες

Ο κώδικας για RGB εικόνες είναι ο εξής:

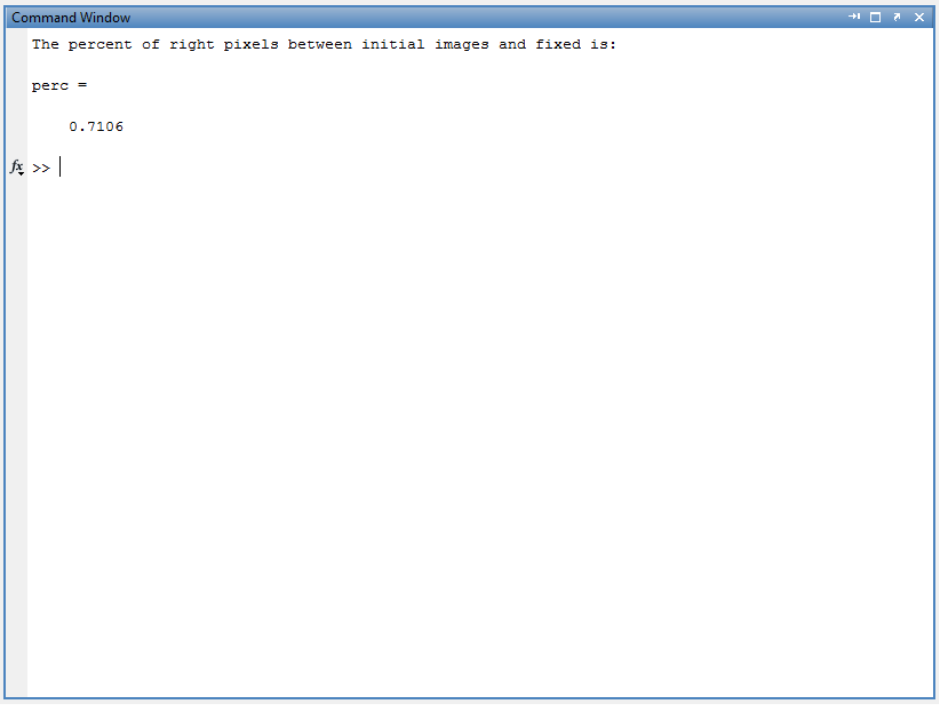
```
% Matlab script for comparing initial image and a compressive sensing image
% using the algorithm MB3D. In order to do this we create a stego image
% importing into the initial image the random message and then we use BM3D
% to create the compressive sensing image. Finally we implement xor
% between initial and compressive sensing image and produce the percent of
% right pixels.

close all; clc; clear perc;

files = dir('*.tiff'); % select between .pgn or .tiff

for k = 1:numel (files) % start the loop

rand('state',0); randn('state',0);

% input original image
yRGB = im2double(imread(files(k).name));%convert a rgb image to a double matrix
y_uint8 = uint8(256*yRGB); %convert image to a uint8 form
y_uint8_mod2 = mod(y_uint8,2); % implement mod2 to the image
```

```
% create a random message
message = round(rand(size(yRGB))); %rgb image
message_uint8 = uint8(message);

% parameters
sigma = 0.1;   % noise standard deviation

%create the steganography image
zRGB = yRGB+sigma*message; %rgb image


%run the function to create compressive sensing image
[PSNR, yRGB_est] = CBM3D(yRGB, zRGB, sigma); %rgb image

%xor the compressive sensing image with the initial
y_est_uint8 = uint8(256*yRGB_est); %rgb image
y_est_uint8_mod2 = mod(y_est_uint8,2); % implement mod2 to the image
K = bitxor(y_uint8_mod2, y_est_uint8_mod2); %implement xor
K_uint8 = uint8(K);
K = bitxor(K_uint8, message_uint8); %implement xor

% Find the percent of right pixels
final = find(K==0); %find the zeros
final_number = length(final(:,1));%count the length of the zeros
[b1, b2, b3] = size(yRGB); % find the dimension of the picture
total = b1*b2*b3; %count the size of the image
perc (k) = final_number/total; %find the percent

%display figure
figure(k)
subplot(k,3,1), imshow(yRGB), title('Original image');
subplot(k,3,2), imshow(zRGB),  title('Steganography image');
subplot(k,3,3), imshow(yRGB_est),  title('Fixed image');

end  %end of the loop

%display the perscent
disp('The percent of right pixels between initial images and fixed is in the matrix perc at
workspace')
```

Όπως μπορούμε να παρατηρήσουμε οι δύο κώδικες μοιάζουν πολύ μεταξύ τους. Η βασική διαφορά υπάρχει στην συνάρτηση που χρησιμοποιούμε που σε αυτή την περίπτωση είναι η CBM3D την οποία θα αναλύσουμε στην παρακάτω υποενότητα. Στην συνέχεια ακολουθεί ένα παράδειγμα υλοποίησης.



Εικόνα 5.4 Αποτέλεσμα κώδικα για RGB εικόνα.



Εικόνα 5.5 Εμφάνιση ποσοστού στο Command Window.

Όπως μπορούμε να παρατηρήσουμε από την παραπάνω εικόνα το ποσοστό των σωστών pixels είναι και εδώ 71,06%. Πράγμα το οποίο σημαίνει ότι το μήνυμα που κρύβεται πίσω από την αρχική εικόνα αλλοιώνει σε ποσοστό περίπου 29%. Ο θόρυβος ο οποίος παρουσιάζεται στη διορθωμένη εικόνα δεν θα πρέπει να μας ανησυχεί μιας και εμείς ενδιαφερόμαστε για τα εικονοστοιχεία του background και όχι της εικόνας.

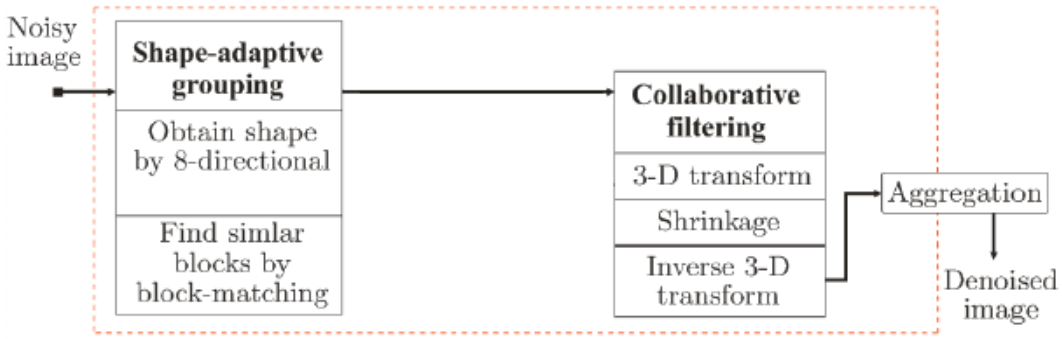
5.4 Ανάλυση αλγορίθμου BM3D

Ο αλγόριθμος BM3D είναι μια καινοτόμος στρατηγική απαλοιφής του θορύβου από μια εικόνα ο οποίος βασίζεται στην ενίσχυση της διεσπαρμένης (sparse) αναπαράστασης σε μια τροποποιημένη περιοχή. Η ενίσχυση της διασποράς επιτυγχάνεται από την ομαδοποίηση όμοιων τμημάτων 2D εικόνας (δύο διαστάσεων) σε 3D πίνακες δεδομένων οι οποίοι ονομάζονται «groups» [2].

Το συνεργατικό φιλτράρισμα (collaborative filtering) είναι μια ειδική διαδικασία που αναπτύχθηκε με σκοπό να χειριστεί αυτά τα 3D groups. Αυτό πραγματοποιείται χρησιμοποιώντας τρία διαδοχικά βήματα: 3D μετασχηματισμός των 3D groups, μείωση φάσματος μετασχηματισμού και ανάποδος 3D μετασχηματισμός. Το αποτέλεσμα είναι μια 3D εκτίμηση η οποία αποτελείται από κοινά φιλτραρισμένα ομαδοποιημένα blocks εικόνας. Με την μείωση του θορύβου, το συνεργατικό φιλτράρισμα αποκαλύπτει ακόμα και τις πιο μικρές κοινές λεπτομέρειες που υπάρχουν στα ομαδοποιημένα blocks (grouped blocks) ενώ ταυτόχρονα διατηρεί τα ουσιώδη μοναδικά χαρακτηριστικά κάθε μεμονωμένου block. Έπειτα τα φιλτραρισμένα blocks επιστρέφουν στις αρχικές του θέσεις [2].

Επειδή αυτά τα blocks επικαλύπτονται, για κάθε εικονοστοιχείο λαμβάνουμε πολλές διαφορετικές εκτιμήσεις οι οποίες πρέπει να συνδυαστούν. Η συγκέντρωση (aggregation) είναι μια ιδιαίτερη διαδικασία μέσου όρου η οποία αξιοποιείται με σκοπό να εκμεταλλευτεί αυτόν τον πλεονασμό [2].

Μια σημαντική βελτίωση επιτυγχάνεται από ένα ειδικό συνεργατικό φίλτρο το collaborative Wiener filtering [2].



Εικόνα 5.6 Σχηματική αναπαράσταση BM3D.
Πηγή: (BM3D Image Denoising with Shape-Adaptive Principal Component Analysis)

Παρακάτω παραθέτουμε τον κώδικα του BM3D για grayscale εικόνες μαζί με κάποια σχόλια.

```
function [PSNR, y_est] = BM3D(y, z, sigma)

%%%%  Quality/complexity trade-off profile selection

%%%%  'np' --> Normal Profile (balanced quality)
%%%%  'lc' --> Low Complexity Profile (fast, lower quality)
%%%%
%%%%  'high' --> High Profile (high quality, not documented in [1])
%%%%
```

```
%%%%  'vn' --> This profile is automatically enabled for high noise
%%%%          when sigma > 40
%%%%
%%%%  'vn_old' --> This is the old 'vn' profile that was used in [1].
%%%%          It gives inferior results than 'vn' in most cases.

if (exist('profile') ~= 1)
   profile        = 'np'; %% default profile/choose a profile
end

%%%% Specify the standard deviation of the corrupting noise

if (exist('sigma') ~= 1),
   sigma              = 25; %% default standard deviation of the AWGN
end

%%%% Following are the parameters for the Normal Profile (np).

%%%% Select transforms ('dct', 'dst', 'hadamard')
transform_2D_HT_name = 'bior1.5'; %% transform used for the HT filtering of size N1 x N1
transform_2D_Wiener_name = 'dct'; %% transform used for the Wiener filtering of size
N1_wiener x N1_wiener
transform_3rd_dim_name = 'haar';  %% transform used in the 3-rd dim, the same for HT and
Wiener filt.

%%%% Hard-thresholding (HT) parameters:

N1 = 8; %% N1 x N1 is the block size used for the hard-thresholding (HT) filtering
Nstep = 3; %% sliding step to process every next reference block
N2 = 16; %% maximum number of similar blocks (maximum size of the 3rd dimension of a 3D
array)
Ns = 39; %% length of the side of the search neighborhood for full-search block-matching (BM),
must be odd
tau_match = 3000; %% threshold for the block-distance (d-distance)
lambda_thr2D = 0; %% threshold parameter for the coarse initial denoising used in the d-
distance measure
lambda_thr3D = 2.7; %% threshold parameter for the hard-thresholding in 3D transform domain
beta = 2.0; %% parameter of the 2D Kaiser window used in the reconstruction

%%%% Wiener filtering parameters:

N1_wiener          = 8;
Nstep_wiener       = 3;
N2_wiener          = 32;
Ns_wiener          = 39;
tau_match_wiener   = 400;
beta_wiener        = 2.0;

%%%% Block-matching parameters:

stepFS = 1; %% step that forces to switch to full-search BM, "1" implies always full-search
smallLN = 'not used in np'; %% if stepFS > 1, then this specifies the size of the small local
search neighb.
stepFSW = 1;
smallLNW = 'not used in np';
```

```
thrToIncStep = 8; %% if the number of non-zero coefficients after HT is less than thrToIncStep, than the sliding step to the next reference block is incresed to (nm1-1)

if strcmp(profile, 'lc') == 1,

    Nstep             = 6;
    Ns                = 25;
    Nstep_wiener      = 5;
    N2_wiener         = 16;
    Ns_wiener         = 25;

    thrToIncStep      = 3;
    smallLN           = 3;
    stepFS            = 6*Nstep;
    smallLNW          = 2;
    stepFSW           = 5*Nstep_wiener;

end

if (strcmp(profile, 'vn') == 1) | (sigma > 40),

    N2                = 32;
    Nstep             = 4;

    N1_wiener         = 11;
    Nstep_wiener      = 6;

    lambda_thr3D      = 2.8;
    thrToIncStep      = 3;
    tau_match_wiener  = 3500;
    tau_match         = 25000;

    Ns_wiener         = 39;

end

% The 'vn_old' profile corresponds to the original parameters for strong noise proposed in [1].

if (strcmp(profile, 'vn_old') == 1) & (sigma > 40),

    transform_2D_HT_name = 'dct';

    N1                = 12;
    Nstep             = 4;

    N1_wiener         = 11;
    Nstep_wiener      = 6;

    lambda_thr3D      = 2.8;
    lambda_thr2D      = 2.0;
    thrToIncStep      = 3;
    tau_match_wiener  = 3500;
    tau_match         = 5000;

    Ns_wiener         = 39;
```

```
end

decLevel = 0;  %% dec. levels of the dyadic wavelet 2D transform for blocks (0 means full
decomposition, higher values decrease the dec. number)
thr_mask = ones(N1); %% N1xN1 mask of threshold scaling coeff. --- by default there is no
scaling, however the use of different thresholds for different wavelet decompoistion subbands
can be done with this matrix

if strcmp(profile, 'high') == 1, %% this profile is not documented in [1]

   decLevel     = 1;
   Nstep        = 2;
   Nstep_wiener = 2;
   lambda_thr3D = 2.5;
   vMask = ones(N1,1); vMask((end/4+1):end/2)= 1.01; vMask((end/2+1):end) = 1.07; %% this
allows to have different threhsolds for the finest and next-to-the-finest subbands
   thr_mask = vMask * vMask';
   beta         = 2.5;
   beta_wiener  = 1.5;

end

%%%% Create transform matrices

 [Tfor, Tinv]   = getTransfMatrix(N1, transform_2D_HT_name, decLevel);     %% get
(normalized) forward and inverse transform matrices
[TforW, TinvW] = getTransfMatrix(N1_wiener, transform_2D_Wiener_name, 0); %% get
(normalized) forward and inverse transform matrices

if (strcmp(transform_3rd_dim_name, 'haar') == 1) | (strcmp(transform_3rd_dim_name(end-
2:end), '1.1') == 1),
   %%% If Haar is used in the 3-rd dimension, then a fast internal transform is used, thus no
need to generate transform
   %%% matrices.
   hadper_trans_single_den         = {};
   inverse_hadper_trans_single_den = {};
else
   %%% Create transform matrices. The transforms are later applied by
   %%% matrix-vector multiplication for the 1D case.
  for hpow = 0:ceil(log2(max(N2,N2_wiener))),
     h = 2^hpow;
     [Tfor3rd, Tinv3rd]   = getTransfMatrix(h, transform_3rd_dim_name, 0);
     hadper_trans_single_den{h}         = single(Tfor3rd);
     inverse_hadper_trans_single_den{h} = single(Tinv3rd');
   end
end

%%%% 2D Kaiser windows used in the aggregation of block-wise estimates

if beta_wiener==2 & beta==2 & N1_wiener==8 & N1==8 % hardcode the window function so
that the signal processing toolbox is not needed by default
   Wwin2D = [ 0.1924   0.2989   0.3846   0.4325   0.4325   0.3846   0.2989   0.1924;
      0.2989   0.4642   0.5974   0.6717   0.6717   0.5974   0.4642   0.2989;
      0.3846   0.5974   0.7688   0.8644   0.8644   0.7688   0.5974   0.3846;
      0.4325   0.6717   0.8644   0.9718   0.9718   0.8644   0.6717   0.4325;
      0.4325   0.6717   0.8644   0.9718   0.9718   0.8644   0.6717   0.4325;
```

```
        0.3846    0.5974    0.7688    0.8644    0.8644    0.7688    0.5974    0.3846;
        0.2989    0.4642    0.5974    0.6717    0.6717    0.5974    0.4642    0.2989;
        0.1924    0.2989    0.3846    0.4325    0.4325    0.3846    0.2989    0.1924];
    Wwin2D_wiener = Wwin2D;
else
    Wwin2D = kaiser(N1, beta) * kaiser(N1, beta)'; % Kaiser window used in the aggregation of
the HT part
    Wwin2D_wiener = kaiser(N1_wiener, beta_wiener) * kaiser(N1_wiener, beta_wiener)'; %
Kaiser window used in the aggregation of the Wiener filt. part
end

%%%% If needed, read images, generate noise, or scale the images to the [0,1] interval

if (exist('y') ~= 1) | (exist('z') ~= 1)
    y       = im2double(imread(image_name));  %% read a noise-free image and put in intensity
range [0,1]
    randn('seed', 0);                         %% generate seed
    z = y+sigma*message; %% create an image with message instead of a noisy
else

    image_name = 'External image';

    % convert z to double precision if needed
    z = double(z);

    % convert y to double precision if needed
    y = double(y);

    % if z's range is [0, 255], then convert to [0, 1]
    if (max(z(:)) > 10), % a naive check for intensity range
        z = z / 255;
    end

    % if y's range is [0, 255], then convert to [0, 1]
    if (max(y(:)) > 10), % a naive check for intensity range
        y = y / 255;
    end
end

if (size(z,3) ~= 1) | (size(y,3) ~= 1),
    error('BM3D accepts only grayscale 2D images.');
end
```

Όπως μπορούμε να παρατηρήσουμε από τον παραπάνω κώδικα η συνάρτηση δέχεται σαν είσοδο μια εικόνα grayscale χωρίς μήνυμα την y, μια εικόνα με μήνυμα την z, μια παράμετρο sigma για τον θόρυβο και το προφίλ που το έχουμε θέσει σαν «np» δηλαδή το κοινό προφίλ. Η έξοδος της συνάρτησης είναι μια εικόνα y_est η οποία έχει βελτιωθεί κατά πολύ σε σχέση με την εικόνα z που περιέχει το μήνυμα.

Στο σημείο αυτό θα πρέπει να αναφέρουμε ότι το προφίλ το έχουμε θέσει «np» και όχι κάποιο άλλο από τα τέσσερα που υπάρχουν στον αλγόριθμο και αυτό διότι σε πειράματα τα οποία κάναμε παρατηρήσαμε ότι το προφίλ «np» δίνει καλύτερα αποτελέσματα. Με άλλα λόγια έχουμε μικρότερο ποσοστό ανόμοιων εικονοστοιχείων μεταξύ της αρχικής εικόνας και της διορθωμένης.

Όπως αναφέραμε πιο πάνω σαν είσοδο η συνάρτηση έχει μια παράμετρο sigma για τον θόρυβο. Αυτή η παράμετρος έχει οριστεί στον κώδικα για τις grayscale εικόνες και για τις rgb εικόνες. Η τιμή της είναι sigma=0.1 και αυτό διότι από πειράματα που κάναμε δίνει τα καλύτερα αποτελέσματα.

Για τον μετασχηματισμό που πραγματοποιείται στην εικόνα χρησιμοποιούμε έναν από τους τρεις που υπάρχουν. Στη περίπτωση μας χρησιμοποιούμε τον transform_3rd_dim_name = 'haar' μιας και δίνει καλύτερα αποτελέσματα στην τελική εικόνα.

Τέλος θα πρέπει να αναφέρουμε ότι ο αλγόριθμος BM3D έχει κάποιο περιορισμό και πιο συγκεκριμένα δέχεται grayscale εικόνες δύο διαστάσεων. Στην περίπτωση όπου η εικόνα δεν είναι δύο διαστάσεων τότε εμφανίζεται μήνυμα λάθους.

Ο αλγόριθμος CBM3D που χρησιμοποιούμε για τις έγχρωμες εικόνες είναι σχεδόν ίδιος με τον BM3D με την μόνη διαφορά ότι δέχεται σαν είσοδο και μια άλλη παράμετρο την «colorspace» που χρειάζεται για να εντοπίσει αν η εικόνα της εισόδου είναι έγχρωμη ή όχι.

5.5 Παρουσίαση αποτελεσμάτων

Στην συγκεκριμένη υποενότητα θα παρουσιάσουμε τα αποτελέσματα που προέκυψαν από την εκτέλεση του κώδικα τόσο για τις grayscale εικόνες όσο και για τις RGB. Οι εικόνες που χρησιμοποιήσαμε στα πειράματα μας είναι «καθαρές», δηλαδή δεν έχουν ενσωματωμένες άλλες πληροφορίες μέσα τους. Έτσι η μόνη πληροφορία που θα ενσωματωθεί σ' αυτές είναι το τυχαίο το μήνυμα μας. Θα πρέπει επίσης να αναφέρουμε ότι χρησιμοποιήσαμε 50 εικόνες grayscale εκ των οποίων οι 10 είναι της μορφής .png, οι 20 είναι της μορφής .gif και οι άλλες 20 είναι τις μορφής .tiff. Επιλέξαμε να έχουμε τρεις διαφορετικούς τύπους έτσι ώστε να βγάλουμε ασφαλέστερα συμπεράσματα. Από την άλλη μεριά για τις RGB εικόνες χρησιμοποιήσαμε 30 εικόνες εκ των οποίων οι 10 είναι της μορφής .png και οι άλλες 20 είναι τις μορφής .tiff. Θα πρέπει εδώ να αναφέρουμε ότι δεν χρησιμοποιούμε RGB εικόνες τύπου .gif επειδή οι εικόνες τέτοιου τύπου δεν είναι πίνακες της μορφής MxNxK, δηλαδή δεν αναπαρίστανται σαν τρισδιάστατοι πίνακες.

Επίσης, οι εικόνες είναι διαφόρων μεγεθών δηλαδή 128x128, 256x256, 512x512.

Ο παρακάτω πίνακας παρουσιάζει τα αποτελέσματα που προέκυψαν από τις grayscale εικόνες.

	Ποσοστό ίδιων pixels
Εικόνα 1η	75,28%
Εικόνα 2η	68,97%
Εικόνα 3η	71,49%
Εικόνα 4η	64,92%
Εικόνα 5η	71,75%
Εικόνα 6η	84,09%
Εικόνα 7η	74,41%
Εικόνα 8η	78,43%
Εικόνα 9η	79,63%
Εικόνα 10η	74,09%

Πίνακας 5.1: Grayscale εικόνες τύπου .png

	Ποσοστό ίδιων pixels
Εικόνα 1η	85,63%
Εικόνα 2η	55,87%
Εικόνα 3η	61,77%
Εικόνα 4η	97,99%
Εικόνα 5η	73,42%
Εικόνα 6η	64,56%
Εικόνα 7η	57,44%
Εικόνα 8η	60,47%
Εικόνα 9η	86,17%
Εικόνα 10η	77,77%
Εικόνα 11η	72,85%
Εικόνα 12η	84,17%
Εικόνα 13η	77,55%
Εικόνα 14η	73,93%
Εικόνα 15η	65,03%
Εικόνα 16η	61,77%
Εικόνα 17η	77,82%
Εικόνα 18η	84,09%
Εικόνα 19η	94,25%
Εικόνα 20η	68,05%

Πίνακας 5.2: Grayscale εικόνες τύπου .tiff

	Ποσοστό ίδιων pixels
Εικόνα 1η	69,56%
Εικόνα 2η	68,53%
Εικόνα 3η	57,84%
Εικόνα 4η	60,33%
Εικόνα 5η	53,94%
Εικόνα 6η	54,54%
Εικόνα 7η	70,34%
Εικόνα 8η	64,98%
Εικόνα 9η	51,60%
Εικόνα 10η	72,77%
Εικόνα 11η	59,87%
Εικόνα 12η	67,04%
Εικόνα 13η	59,87%
Εικόνα 14η	66,28%
Εικόνα 15η	52,09%
Εικόνα 16η	52,02%
Εικόνα 17η	61,31%
Εικόνα 18η	56,83%
Εικόνα 19η	56,81%
Εικόνα 20η	55,60%

Πίνακας 5.3: Grayscale εικόνες τύπου .gif

Σύμφωνα με τα αποτελέσματα που προέκυψαν από τους παραπάνω πίνακες για εικόνες grayscale διαφόρων τύπων μπορούμε να συμπεράνουμε ότι οι εικόνες τύπου .png παρουσιάζουν τα μεγαλύτερα ποσοστά ενώ τα χειρότερα-χαμηλότερα ποσοστά παρουσιάζονται σε εικόνες τύπου .gif.

Στην συνέχεια θα παρουσιάσουμε τα αποτελέσματα από 30 καθαρές εικόνες RGB βγάζοντας και εκεί τα κατάλληλα συμπεράσματα.

	Ποσοστό ίδιων pixels
Εικόνα 1η	71,06%
Εικόνα 2η	60,79%
Εικόνα 3η	71,89%
Εικόνα 4η	92,80%
Εικόνα 5η	75,96%
Εικόνα 6η	70,98%
Εικόνα 7η	65,75%
Εικόνα 8η	87,47%
Εικόνα 9η	68,81%
Εικόνα 10η	69,13%

Πίνακας 5.4: RGB εικόνες τύπου .png

	Ποσοστό ίδιων pixels
Εικόνα 1η	54,19%
Εικόνα 2η	84,92%
Εικόνα 3η	71,89%
Εικόνα 4η	70,98%
Εικόνα 5η	92,80%
Εικόνα 6η	73,50%
Εικόνα 7η	71,06%
Εικόνα 8η	86,00%
Εικόνα 9η	73,89%
Εικόνα 10η	75,83%
Εικόνα 11η	88,32%
Εικόνα 12η	50,83%
Εικόνα 13η	79,01%
Εικόνα 14η	90,35%

Εικόνα 15η	68,14%
Εικόνα 16η	75,96%
Εικόνα 17η	74,49%
Εικόνα 18η	92,63%
Εικόνα 19η	89,42%
Εικόνα 20η	66,81%

Πίνακας 5.5: RGB εικόνες τύπου .tiff

Σύμφωνα με τα αποτελέσματα που προέκυψαν από τους παραπάνω πίνακες για εικόνες RGB των δύο τύπων μπορούμε να συμπεράνουμε ότι τόσο οι εικόνες τύπου .png όσο και αυτές του τύπου .tiff παρουσιάζουν σχεδόν ίδια ποσοστά. Πράγμα το οποίο σημαίνει ότι στις RGB εικόνες δεν παίζει ρόλο ο τύπος σε αντίθεση με τις grayscale εικόνες.

5.6 Συμπεράσματα

Το κεφάλαιο αυτό το μεταπτυχιακής διατριβής μπορεί να χαρακτηριστεί ως το πιο σημαντικό διότι παρουσιάζει τα αποτελέσματα της έρευνας που πραγματοποιήσαμε πάνω στην στεγανογραφία.

Όπως μπορούμε να παρατηρήσουμε από τους διάφορους πίνακες που προέκυψαν ύστερα από την εφαρμογή του κώδικα μας, το χαμηλότερο ποσοστό σωστών εικονοστοιχείων είτε αναφερόμαστε σε grayscale εικόνες είτε σε RGB είναι το 50,83% ενώ το υψηλότερο είναι το 97,99%.

Θα μπορούσε κανείς να πει ότι το 50,83% είναι ένα πάρα πολύ χαμηλό ποσοστό το οποίο προκαλεί αρνητική εντύπωση για την αποτελεσματική χρήση του κώδικα που υλοποιήσαμε. Με άλλα λόγια η μέθοδος που χρησιμοποιούμε δεν είναι η ενδεδειγμένη για να κρύψουμε ένα μήνυμα πίσω από μια εικόνα και αυτό γιατί μια κακόβουλη οντότητα θα καταλάβαινε αμέσως την χρήση της στεγανογραφίας σε αυτή την εικόνα της οποίας το ποσοστό σωστών εικονοστοιχείων αρχικής και βελτιωμένης είναι μόνο 50,83%. Ωστόσο απ' ότι μπορούμε να παρατηρήσουμε τέτοιο μικρό ποσοστό εμφανίζεται μόνο μια φορά ανάμεσα στις συνολικά 80 εικόνες. Επομένως η διαδικασία που περιγράψαμε στο κεφάλαιο αυτό δεν παρουσιάζει αρνητικά στοιχεία.

Τέλος ένα σημαντικό στοιχείο που προκύπτει από τους πίνακες είναι ότι οι εικόνες grayscale τύπου .png είναι οι καταλληλότερες για χρήση στεγανογραφίας μιας και απ' ότι παρατηρούμε έχουν σταθερά και μεγάλα ποσοστά σωστών εικονοστοιχείων σε σχέση με όλες τους άλλους τύπους εικόνων.

Βιβλιογραφία

[1] Rafael C. Gonzalez, Richard E, Woods, “Digital Image Processing”, Addison Wesley, 1993.

[2] Kostadin Dabov, Alessandro Foi, Vladimir Katkovnik, and Karen Egiazarian “BM3D Image Denoising with Shape-Adaptive Principal Component Analysis”, Department of Signal Processing, Tampere University of Technology.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Κεφάλαιο 6

Συμπεράσματα

Η μεταπτυχιακή αυτή διατριβή ασχολείται με το θέμα της στεγανογραφίας, τους τρόπους στεγανογραφίας που υπάρχουν στις μέρες μας και παρουσιάζει ένα κώδικα ο οποίος χρησιμοποιείται για να εντοπίζει κατά πόσο μια εικόνα είναι κατάλληλη έτσι ώστε να χρησιμοποιηθεί για να ενσωματώσει τυχαία μηνύματα.

Η στεγανογραφία είναι γενικά μια νέα μορφή απόκρυψης ανταλλασσόμενων μηνυμάτων η οποία διαφέρει σε ελάχιστα σημεία με την κρυπτογραφία και την υδατογράφηση. Αναμφισβήτητα η επιστήμη της στεγανογραφίας, παρ' όλο που ακόμα βρίσκεται σε αρχικό στάδιο, έχει σαφές «προβάδισμα» σε σχέση με τις άλλες δύο τεχνικές μιας και μπορεί να χρησιμοποιήσει για αντικείμενο κάλυψης διάφορα ψηφιακά μέσα όπως ψηφιακές εικόνες, αρχεία mp3 ή ακόμα και αρχεία βίντεο.

Η μεγάλη ανάπτυξη της οφείλεται και στους πολλούς τρόπους με τους οποίους μπορεί να πραγματοποιηθεί η στεγανογραφία. Μέχρι σήμερα τρεις είναι οι βασικότεροι: η έγχυση, η αντικατάσταση και η παραγωγή. Αυτή η οποία παρουσιάζει μεγαλύτερο ενδιαφέρον είναι αυτής της παραγωγής μιας και δεν υπάρχει ακόμα τρόπος εντοπισμού της.

Πολύ σημαντικό ρόλο στην στεγανογραφία παίζει το αντικείμενο κάλυψης. Η παρούσα μεταπτυχιακή διατριβή ασχολήθηκε περισσότερο με τις ψηφιακές εικόνες. Το συμπέρασμα λοιπόν που προέκυψε είναι το εξής: Για την καλύτερη ενσωμάτωση του μυστικού μηνύματος στη εικόνα-αντικείμενο κάλυψης, θα πρέπει το μήνυμα να είναι όσο το δυνατόν μικρότερο και η εικόνα να περιέχει όσο το δυνατόν περισσότερα δεδομένα.

Ένας σημαντικός τομέας ο οποίος παρουσιάστηκε σ' αυτή τη διατριβή είναι αυτός της συμπιεσμένης δειγματοληψίας. Πολλοί αλγόριθμοι έχουν αναπτυχθεί γύρω από αυτό το θέμα με καλύτερο αυτό που αναφέρεται στην ελαχιστοποίηση του I1. Θα πρέπει να τονίσουμε στο σημείο αυτό τον ιδιαίτερο ρόλο που διαδραμάτισε η θεωρία της συμπιεσμένης δειγματοληψίας στην ανάπτυξη του κώδικα που χρησιμοποιήσαμε. Γενικά η συμπιεσμένη δειγματοληψία «πατάει» πάνω σε διάφορους κλάδους της επιστήμης και της τεχνολογίας με αποτέλεσμα να έχει ξεχωριστή επίδραση πάνω σε αυτούς. Ωστόσο αυτή την στιγμή υπάρχουν και κάποια ανοιχτά θέματα τα οποία πρέπει να επιλυθούν.

Η νέα μέθοδο στεγανάλυσης που αναπτύξαμε στην διατριβή αυτή αποτελεί έναν νέο τρόπο για να εντοπίσει κάποιος αν μια εικόνα περιέχει κάποιο μυστικό μήνυμα το οποίο δεν φαίνεται με «γυμνό» μάτι. Η μέθοδος αυτή βασίζεται στον αλγόριθμο BM3D και CBM3D για εικόνες σε απόχρωση του γκρι και σε χρωματιστές εικόνες αντίστοιχα. Το συμπέρασμα που προέκυψε κατά την διάρκεια του πειραματισμού αυτής της μεθόδου είναι ότι οι εικόνες grayscale τύπου .png είναι οι καταλληλότερες για χρήση στεγανογραφίας.

Κλείνοντας, αυτό το οποίο θα μπορούσε να χαρακτηριστεί ως μελλοντική έρευνα πάνω σε αυτά που πραγματεύεται η παρούσα μεταπτυχιακή διατριβή είναι να εφαρμοστεί ένας καινούργιος αλγόριθμος ο οποίος δεν θα έχει περιορισμούς σαν και αυτούς που έχει τώρα ο BM3D και ο CBM3D. Έτσι θα μπορεί να δέχεται και grayscale εικόνες τριών διαστάσεων και όχι μόνο δύο όπως επίσης και να δέχεται όλους του τύπους έγχρωμών εικόνων ακόμα και αν δεν είναι της μορφής MxNxK.