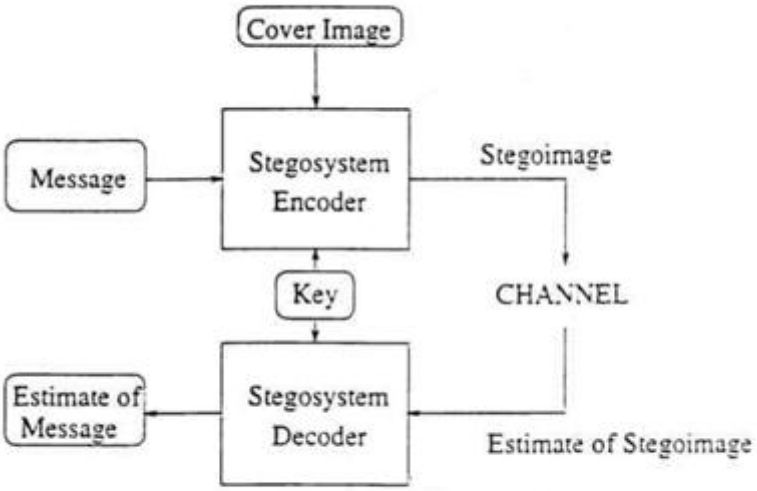
Εργασία στο μάθημα της Κρυπτογραφίας με τίτλο :

Στεγανογραφία



Εργασία : Βεζέρης Δημήτριος , ΜΔΕ (296)
Λευκίππου 6, 67100 Ξάνθη, Τηλ.-Fax 2541–084–084, e-mail: leader@cosmos4u.com
www.vezeris.gr

Επιβλέπων : Επ. Καθηγητής : Διαμαντίδης Δημήτριος
Πολυτεχνική Σχολή, Ξάνθη Ελλάδα 67100, Τηλέφωνα: +30 2541079261 (εσ.71261),
Fax:+30 2541079260 (εσ.71260) , Email: diam@duth.gr

ΠΕΡΙΕΧΟΜΕΝΑ

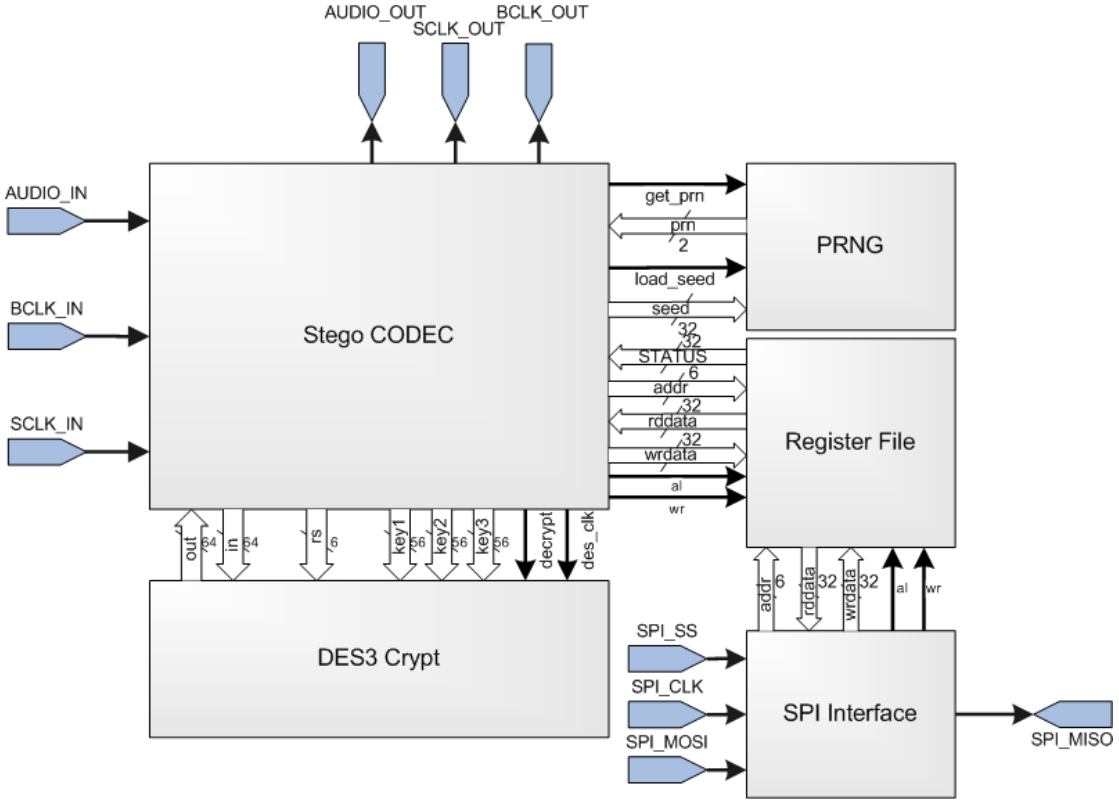
Πρόλογος

Σε έναν ιδανικό κόσμο πιθανό να μη χρειαζόταν ποτέ να ορίσουμε έννοιες όπως η στεγανογραφία ή η κρυπτογραφία γενικά. Πολλά βέβαια μηνύματα , από τους αρχαιοτάτους χρόνους είναι κρυπτογραφημένα και μερικά ακόμα και σήμερα μη αποκρυπτογραφημένα. Ενώ ξεκίνησε με απλές και έξυπνες ιδέες η κρυπτογραφία σήμερα έχει γίνει ολόκληρη επιστήμη και μάλιστα πολύ πολύπλοκο ώστε να είναι επεξεργάσιμη από τον ανθρώπινο εγκέφαλο. Στην παρούσα εργασία θα εκθέσουμε πληροφορίες σχετικά με τη στεγανογραφία από πληροφορίες που αντλήθηκαν από το διαδίκτυο. Ευχαριστώ όλους αυτούς που στηρίζουν τη συνέχεια των σπουδών μου σε ανώτερο επίπεδο.

Ξάνθη Φεβρουάριος 2010.

Εισαγωγή

Σήμερα στις τεχνολογίες των τηλεπικοινωνιών οι οποίες έχουν ασύρματες και ασύρματες μορφές, σταθερές και κινητές συσκευές, ζούμε την εποχή της επικοινωνίας και της μεταφοράς της πληροφορίας. Είτε βρίσκοντας εμείς τον τόπο ή τον χώρο που εμπιστευόμαστε αντλώντας την πληροφορία είτε επικοινωνώντας με κάποιον που εμπιστευόμαστε και πληροφορούμαστε από ζωντανή πηγή. Στο παρόν με τον όρο τηλεπικοινωνία εννοούμε και το διαδίκτυο και τα κινητά και τα σταθερά κλπ. Η μεταφορά αυτή συνήθως γίνεται χωρίς κρυπτογράφηση ή όχι τουλάχιστον σε όλη τη διαδρομή της, από την αφετηρία στον προορισμό της. Υπάρχουν σήμερα αρκετοί αλγόριθμοι κρυπτογράφησης που μπορούν να εφαρμοστούν πάνω στις πληροφορίες ενός καναλιού επικοινωνίας, και να μεταφέρονται κρυπτογραφημένα μηνύματα από τον αποστολέα στον παραλήπτη. Σε όλες τις περιπτώσεις κωδικοποιούμε την πληροφορία και η πληροφορία μεταφέρεται μέσα στα κανάλια.
Υπάρχει όμως και η περίπτωση της στεγανογραφίας. Στην περίπτωση αυτή κωδικοποιούμε την πληροφορία αλλά ο φορέας είναι άλλο σύνολο πληροφοριών, ασύνδετα με την πληροφορία. Μπορούμε λοιπόν να κρυπτογραφήσουμε ένα μήνυμα ή όχι, αλλά να το κρύψουμε μέσα σε μία άλλη άσχετη πληροφορία.
Η Στεγανογραφία τροποποιεί ένα κομμάτι πληροφορίας και το κρύβει μέσα σε άλλη. Τα αρχεία υπολογιστών (εικόνες, ήχοι, ακόμη και οι αποθηκευτικοί δίσκοι) περιέχουν αχρησιμοποίητους ή ασήμαντους τομείς δεδομένων. Η τέχνη της Στεγανογραφίας εκμεταλλεύεται αυτές τις περιοχές, αντικαθιστώντας τις με χρήσιμες πληροφορίες. Τα αρχεία αυτά μπορούν να ανταλλαχθούν χωρίς κανένας να ξέρει τι βρίσκεται πραγματικά μέσα τους. Μια φωτογραφία μας μπορεί εύκολα να περιέχει μια προσωπική επιστολή στον παραλήπτη. Η καταγραφή μιας σύντομης πρότασης μπορεί να περιέχει τα σχέδια της επιχείρησής μας για ένα νέο προϊόν. Η Στεγανογραφία μπορεί επίσης να χρησιμοποιηθεί για να τοποθετήσει ένα κρυμμένο "εμπορικό σήμα" στις εικόνες, τη μουσική, και το λογισμικό, μια τεχνική που θα δούμε παρακάτω με την ονομασία υδατογράφημα.


AUDIO_OUT
SCLK_OUT
BCLK_OUT
AUDIO_IN
BCLK_IN
SCLK_IN
Stego CODEC
get_prn
prn
2
load_seed
seed
32
STATUS
32
addr
6
rddata
32
wrdata
32
al
wr
PRNG
Register File
out
64
in
64
rs
6
key1
56
key2
56
key3
56
decrypt
des_clk
DES3 Crypt
addr
6
rddata
32
wrdata
32
al
wr
SPI_SS
SPI_CLK
SPI_MOSI
SPI Interface
SPI_MISO

1. Στεγανογραφία

1.1. Ορισμοί

Η Στεγανογραφία δεν είναι ακριβώς Κρυπτογραφία αλλά είναι οπωσδήποτε ένα μέσο προστασίας της πληροφορίας στον τομέα της ασφάλειας. Αντίθετα με την Κρυπτογραφία όπου σκοπός μας είναι να αλλάξουμε την πληροφορία που θέλουμε να ασφαλίσουμε από οποιουδήποτε είδους επίθεση, έτσι ώστε ο επιτιθέμενος να μην μπορεί να βγάλει νόημα από τα στοιχεία που έχει, ενώ στην Στεγανογραφία σκοπός μας είναι να κρύψουμε την ίδια την ύπαρξη της πληροφορίας.
Θα μπορούσαμε να πούμε ότι η Στεγανογραφία είναι ευρύτερη έννοια της Κρυπτογραφίας (στην περίπτωση που κρυπτογραφούμε αλλά και κρύβουμε).
Η Στεγανογραφία προέρχεται από τις λέξεις **Στεγανό** = προστατευμένο - καλυμμένο & **Γραφή** = γραφή, κείμενο ή σχέδιο, που σημαίνει η γραφή "που καλύπτεται" ή αλλιώς " προστατευμένη" γραφή.
Στεγανογραφία είναι η επιστήμη που σκοπό έχει να κρύψει την πληροφορία έτσι ώστε τα μηνύματα να μπορούν να περάσουν χωρίς να υπάρχει η παραμικρή υποψία ότι υπάρχουν.
Στη σημερινή "ψηφιακή εποχή" ως μέσο (φέρον) για το κρύψιμο των πληροφοριών, λαμβάνονται οι ψηφιακές εικόνες και τα αρχεία ήχου.
Με τη στεγανογραφία επιτρέπεται η μετάδοση καλυμμένης πληροφορίας με ασφάλεια μεταξύ δύο προορισμών ενώ μπορεί να μην κρυπτογραφεί το μήνυμα, αλλά αντί αυτού στηρίζεται στο ότι ο εχθρός δεν θα ανακαλύψει ποτέ τη μετάδοση της πληροφορίας σε σχέση με την κρυπτογράφηση που κρύβει το περιεχόμενο του μηνύματος. Βέβαια δεν κρύβει την επικοινωνία μεταξύ δύο προορισμών. Θα μπορούσε όμως και η επικοινωνία να μην υπάρχει αλλά κάποιος να επισκέπτεται ένα χώρο και να διαβάζει μηνύματα, χωρίς να φαίνεται κάποια αποστολή.

Εδώ λοιπόν μπορούμε να διαφοροποιήσουμε και την κρυπτογραφία που είναι η μορφή μυστικής πληροφορίας από την στεγανογραφία που είναι μυστική επικοινωνία.

1.2. Μορφές εμφάνισης

Καθ' όλη τη διάρκεια της ιστορίας, ένα πλήθος μεθόδων και παραλλαγών έχουν χρησιμοποιηθεί για να κρύψουν πληροφορίες. Τα πρώτα σημάδια εμφάνισης της Στεγανογραφίας είναι από την εποχή του Ηρόδοτου στην αρχαία Ελλάδα, ο οποίος περιγράφει πως οι έλληνες έκρυβαν ένα μήνυμα σε ειδικές ξύλινες πλάκες που χρησιμοποιούσαν για γραφή και μετά το κάλυπταν με κερί. Σε μια ιστορία του ο Δημήρατος θέλησε να ειδοποιήσει τη Σπάρτη ότι ο Ξέρξης σκόπευε να εισβάλει στην Ελλάδα. Για να αποφύγει τη σύλληψη, έξυσε το μήνυμα στην ξύλινη πλάκα και έπειτα κάλυψε την πλάκα με κερί. Οι πλάκες εμφανίστηκαν να είναι κενές και αχρησιμοποίητες ,έτσι πέρασαν τον έλεγχο από τους φρουρούς χωρίς καμία υποψία.

Μια άλλη έξυπνη μέθοδος ήταν να ξυριστεί το κεφάλι ενός αγγελιοφόρου και να του κάνουν τατουάζ ένα μήνυμα ,μια εικόνα ή και ένα χάρτη (π.χ. πειρατές) στο κεφάλι του. Μετά από λίγο χρόνο αφού μακρύνουν τα μαλλιά του , το μήνυμα θα ήταν μη ορατό έως ότου ξυρίσει πάλι το κεφάλι.

Μια άλλη κοινή μορφή αόρατου μηνύματος είναι μέσο της χρήσης των ‘‘αόρατων μελανιών’’. Τέτοια μελάνια χρησιμοποιήθηκαν με πολλή επιτυχία τον δεύτερο παγκόσμιο πόλεμο. Μια αθώα επιστολή μπορεί να περιέχει ένα πολύ διαφορετικό μήνυμα που γράφεται μεταξύ των γραμμών. Νωρίς στον δεύτερο παγκόσμιο πόλεμο η τεχνολογία της Στεγανογραφίας αποτελούταν σχεδόν αποκλειστικά από τα αόρατα μελάνια. Τα κοινά υλικά για τα αόρατα μελάνια είναι γάλα, ξίδι, χυμοί φρούτων και ούρα. Όλοι αυτά σκουραίνουν όταν θερμαίνονται. Με τη βελτίωση της τεχνολογίας και την ευκολία ως προς την αποκωδικοποίηση των αόρατων μελανιών, περιπλοκότερα μελάνια αναπτύχθηκαν στο να αντιδρούν μόνο σε συγκεκριμένες χημικές ουσίες. Μερικά μηνύματα έπρεπε επεξεργαστούν κατάλληλα όπως οι φωτογραφίες αναπτύσσονται με διάφορες χημικές ουσίες στα εργαστήρια .

Μηνύματα ως Null Ciphers (όχι κρυπτογράφημα) χρησιμοποιήθηκαν επίσης. Το πραγματικό μήνυμα είναι καμουφλαρισμένο σε ένα αθώο μήνυμα. Λόγω της "φήμης" πολλών ανοικτών κωδικοποιημένων μηνυμάτων, οι ύποπτες επικοινωνίες ανιχνεύθηκαν από διάφορα αντικατασκοπικά φίλτρα . Εν ολίγης αρκετά "αθώα" μηνύματα μπόρεσαν να διαπεράσουν. Ένα παράδειγμα ενός μηνύματος null cipher περιέχει κρυμμένο ένα μήνυμα τέτοιας μορφής:

Π.χ.: Fi**s**hing fr**e**shwater be**n**ds an**d** sal**t**water
co**a**sts re**w**ards an**y**one fe**e**ling st**r**essed.
Re**s**ourceful an**g**lers us**u**ally fi**n**d ma**s**terful
le**a**pers fu**n** an**d** ad**m**it sw**o**rdfish ra**n**k
ov**e**rwhelming an**y**day.

Διαβάζοντας το τρίτο γράμμα από κάθε λέξη το μήνυμα που προκύπτει είναι :

Send Lawyers, Guns, and Money.

Το ακόλουθο μήνυμα είναι ένα αληθινό γεγονός που στάλθηκε στον δεύτερο παγκόσμιο πόλεμο :

A**p**parently n**e**utral's p**r**otest i**s** t**h**oroughly d**i**scounted
a**n**d i**g**nored. I**s**man h**a**rd h**i**t. B**l**ockade i**s**sue a**f**fects
p**r**etext f**o**r e**m**bargo o**n** b**y**-products, e**j**ecting s**u**ets a**n**d v**e**getable o**i**ls.

Διαβάζοντας το δεύτερο γράμμα από κάθε λέξη το μήνυμα που προκύπτει είναι :

Pershing sails from NY June 1.

Η ανίχνευση μηνυμάτων βελτιωνόταν, παράλληλα νέες τεχνολογίες αναπτύχθηκαν που θα μπορούσαν να περάσουν περισσότερες πληροφορίες και να είναι λιγότερο ευδιάκριτες. Οι Γερμανοί ανέπτυξαν τα Microdots (μικροσκοπική τεχνολογία) στην οποία ο κάποτε διευθυντής του FBI J.Edgar Hoover χαρακτήρισε ως " the enemy's masterpiece of espionage." Τα Microdots είναι μικροσκοπικές φωτογραφίες που περιέχουν δεδομένα στο μέγεθος μιας τυπωμένης κουκίδας σε μία δακτυλογραφημένη σελίδα. Τα πρώτα Microdots ανακαλύφθηκαν μεταμφιεσμένα σε έναν δακτυλογραφημένο φάκελο που μεταφέρθηκε από έναν γερμανό πράκτορα το 1941. Το μήνυμα δεν ήταν κρυμμένο, ούτε

κρυπτογραφημένο. Ήταν ακριβώς τόσο μικρό ώστε να μην τραβήξει ποτέ τη παραμικρή προσοχή . Παρά το μέγεθος τους, τα Microdots επέτρεψαν τη διαβίβαση μεγάλων σε όγκο πληροφοριών συμπεριλαμβανομένων και διαφορών σχεδίων και φωτογραφιών.

Μετά από πολλές μεθόδους που ανακαλύφθηκαν και που καταδιώχτηκαν, διάφορες κυβερνήσεις έλαβαν ακραία μέτρα που μπορεί να μας φαίνονται πολύ αστεία σήμερα όπως στις ΗΠΑ η απαγόρευση των γρίφων, σταυρολέξων, οδηγίες πλεξίματος, αποκόμματα εφημερίδων, ακόμα και παιδικές ζωγραφιές δεδομένου ότι μπορούν όλα να περιέχουν μυστικά μηνύματα. Οι αρμόδιες αρχές ενέργησαν ακόμη και στην αντικατάσταση των γραμματοσήμων στους φακέλους. Απαγορεύτηκαν επίσης όλες οι διεθνείς παραγγελίες παραδόσεων συγκεκριμένων τύπων λουλουδιών που περιείχαν συγκεκριμένες ημερομηνίες παράδοσης από τις κυβερνήσεις των ΗΠΑ και Βρετανίας. Στην ΕΣΣΔ όλες οι διεθνείς ταχυδρομικές επιστολές απαγορεύτηκαν στην προσπάθεια να εμποδίσουν οποιαδήποτε εχθρική δραστηριότητα.

Με κάθε ανακάλυψη ενός μηνύματος που κρύβεται χρησιμοποιώντας μια υπάρχουσα τεχνολογική εφαρμογή, μια νέα Στεγανογραφική τεχνική επινοείται. Υπάρχουν ακόμη και τάσεις για επαναχρησιμοποίηση παλαιών μεθόδων. Τα σχέδια και οι ζωγραφιές έχουν χρησιμοποιηθεί συχνά για να κρύψουν ή να αποκαλύψουν πληροφορίες. Είναι απλό να κωδικοποιηθεί ένα μήνυμα με την ποικιλία γραμμών, χρωμάτων ή άλλων στοιχείων μίας εικόνας. Οι υπολογιστές φέρνουν μια τέτοια μέθοδο σε νέες διαστάσεις όπως θα δούμε αργότερα.

Ακόμη και το σχεδιάγραμμα ενός εγγράφου μπορεί να παρέχει πληροφορίες για το ίδιο έγγραφο. Ο Brassil και άλλοι, σε μια σειρά δημοσιεύσεων εξετάζουν τον προσδιορισμό εγγράφων και το χαρακτηρίζουν σύμφωνα με τη διαμόρφωση της θέσης των γραμμών και των λέξεων. Παρόμοιες τεχνικές μπορούν επίσης να χρησιμοποιηθούν για να παρέχουν κάποιες άλλες "συγκαλυμμένες" πληροφορίες ακριβώς σαν το 0,1 που είναι πηγές πληροφορίας σε έναν υπολογιστή. Όπως σε ένα από τα παραδείγματά τους, η λέξη-μετατόπιση μπορεί να χρησιμοποιηθεί για να βοηθήσει να προσδιοριστεί ένα έγγραφο. Μια παρόμοια μέθοδος μπορεί να εφαρμοστεί για να εμφανίσει ένα εξ ολοκλήρου διαφορετικό μήνυμα. Η ακόλουθη πρόταση:

Το παρόν αποτελεί μία εργασία όχι για την κρυπτογραφία αλλά για μία συγγενής έννοια. Την χρησιμοποίησε ο Γερμανικός Στρατός κατά τη διάρκεια του Β' παγκοσμίου πολέμου και ονομάζεται στεγανογραφία.

Αν πριν από κάθε λέξη που θέλουμε να περάσουμε αυξήσουμε το κενό διπλάσια από ότι το κανονικό τότε το αποτέλεσμα του αλγορίθμου θα μπορούσε να είναι:

Το παρόν αποτελεί μία εργασία όχι για την κρυπτογραφία αλλά για μία συγγενής έννοια. Την χρησιμοποίησε ο Γερμανικός Στρατός κατά τη διάρκεια του Β' παγκοσμίου πολέμου και ονομάζεται στεγανογραφία.

Οι προτάσεις που περιέχουν τις κρυμμένες λέξεις εμφανίζονται αβλαβείς καθώς και όλο το μήνυμα φαίνεται αθώο, αλλά ο συνδυασμός αυτός με τον συγκεκριμένο αλγόριθμο παράγει ένα διαφορετικό μήνυμα:

όχι κρυπτογραφία χρησιμοποίησε στεγανογραφία.

2. Σύγχρονη στεγανογραφία

2.1. Στεγανογραφία και υπολογιστές.

Η Στεγανογραφία στους υπολογιστές είναι βασισμένη σε δύο παραδοχές - αρχές. Η πρώτη είναι ότι τα αρχεία που περιέχουν εικόνες ή ήχο μπορούν να αλλάξουν κατά μία ορισμένη επέκταση χωρίς καμία αλλοίωση της λειτουργικότητάς τους αντίθετα από άλλους τύπους δεδομένων (π.χ. τα προγράμματα) που πρέπει να είναι ακριβή προκειμένου να λειτουργήσουν .
Η άλλη αρχή στηρίζεται στην ανικανότητα του ανθρώπου να διακρίνει τις ελάχιστες αλλαγές στο χρώμα μίας εικόνας ή στην ποιότητα του ήχου, το οποίο είναι ιδιαίτερα εύκολο να χρησιμοποιηθεί και να εφαρμοστεί στα δεδομένα που περιέχουν περιττές πληροφορίες, είτε πρόκειται για ήχο 16-bit , 8-bit ή ακόμα καλύτερα μιας εικόνας 24-bit. Η τροποποίηση που γίνεται στις ψηφιακές εικόνες, αλλάζοντας την τιμή του λιγότερου σημαντικού bit (LSB) του χρώματος του εικονοστοιχείου (Pixel) δεν γίνεται αντιληπτή από το ανθρώπινο μάτι.

2.2. Στεγανάλυση

Ένα από τα μειονεκτήματα της Στεγανογραφίας και άξιο προσοχής είναι το μέγεθος του αρχικού αρχείου και αυτού τού οποίου προκύπτει μετά από κάποια Στεγανογραφική μέθοδο που εφαρμόσαμε πάνω του. Κάποιος μπορεί να δει τη διαφορά μεταξύ του αρχικού και του τροποποιημένου αρχείου μόνο συγκρίνοντας τα μεγέθη τους. Έτσι ο αναλυτής εάν κατέχει μόνο το τροποποιημένο αρχείο (και όχι το αρχικό), τότε θα φαίνεται το αρχείο αθώο. Η τεχνική κατά την οποία με διάφορες διαδικασίες προσπαθούμε να ανιχνεύσουμε κάποιο κρυμμένο μήνυμα ή δεδομένο μέσα σε μία "αθώα" πληροφορία λέγεται Στεγανάλυση και είναι ουσιαστικά η απάντηση στην Στεγανογραφία όπως η αποκρυπτογράφηση στην κρυπτογράφηση.
Για την καλύτερη ασφάλεια συνιστάται κάποιος να χρησιμοποιεί εικόνες με πολλές διαβαθμίσεις χρωμάτων και κατά προτίμηση να μην είναι συνηθισμένο αρχείο ώστε να μην είναι γνωστό στο κοινό επειδή οι ελάχιστες αλλαγές θεωρούνται έως και αδύνατων να παρατηρηθούν. Η χρησιμοποίηση π.χ. μίας εικόνας ενός διάσημου ζωγράφου που είναι ευρέως γνωστή δεν είναι και μια πολύ καλή ιδέα, επειδή ο καθένας (τουλάχιστον οι ειδικοί στο χώρο) θα ξέρουν πως είναι η εικόνα αρχικά, εκτός από τα σημεία ίδιου χρώματος. Καλύτερα αποτελέσματα θα έχουμε αν εφαρμόσουμε σε μία άσχετη φωτογραφία. Γενικά αφού κρύψουμε ένα μήνυμα σε ένα αρχείο προτιμάτε να καταστρέψουμε το πρωτότυπο για καλύτερη ασφάλεια.
Όπως είδαμε η Στεγανογραφία χρησιμοποιείτε για την ασφάλεια της πληροφορίας ώστε να μην μπορεί να εντοπιστεί η ύπαρξή της. Όμως η επιστήμη της Στεγανογραφίας δημιούργησε και άλλους υποκλάδους όπως η τεχνική του Watermarking (υδατογραφήματος) και Fingerprint (αποτυπώματος) η οποία είναι μία μέθοδος που κρύβει πληροφορίες ταυτότητας ή άδειες αντικειμένων όπως serial numbers.

2.3. Υδατογράφημα

Αν μιλήσουμε για εμπορικές Στεγανογραφικές εφαρμογές που υπάρχουν στο δίκτυο θα πρέπει σίγουρα να αναφέρουμε το ψηφιακό υδατογράφημα που έχει πάρει μια νέα σημασία στην σύγχρονη ψηφιακή εποχή. Ακόμα και οι εικόνες, το βίντεο, η μουσική, το κείμενο, και το λογισμικό, όλα αντιγράφονται εύκολα και διανέμονται παράνομα, αναγκάζοντας τους συντάκτες να χάνουν μεγάλο μερίδιο πωλήσεων και σε πολλές περιπτώσεις τα πνευματικά τους δικαιώματα. Το υδατογράφημα είναι μια ειδική τεχνική που εγκαθιστά αόρατα ψηφιακά σημάδια στις εικόνες και στα αρχεία ήχου τα οποία φανερώνουν πληροφορίες πνευματικών δικαιωμάτων. Αυτά τα σημάδια ανιχνεύονται από ειδικά προγράμματα που μπορούν να αντλήσουν πολλές χρήσιμες πληροφορίες από αυτό το ειδικό σήμα (υδατογράφημα).

Όταν το αρχείο δημιουργείται, ταυτόχρονα κρατά τα πνευματικά δικαιώματα , το πώς να έρθει σε επαφή με το συντάκτη κλπ.... Όπως ξέρουμε χιλιάδες γνήσια προϊόντα αναπαράγονται παράνομα και κλέβονται από το δίκτυο κάθε μέρα ώστε να καθίσταται αυτή τη τεχνολογία απαραίτητη και χρήσιμη εάν θέλουμε να προστατέψουμε τα πνευματικά μας δικαιώματα από την πειρατεία.
Υπάρχουν πολλές εταιρίες στο δίκτυο που πωλούν προϊόντα υδατογραφήματος. Μία από τις ηγετικές είναι η Digimarc (http://www.digimarc.com) τις οποίας οι πωλήσεις προγραμμάτων ξεπερνούν το ένα εκατομμύριο. Προσφέρει ελεύθερα το πρόγραμμα PictureMarc το οποίο είναι ένα plug-in στο Photoshop και στο CorelDraw, ή το αυτόνομο ReadMarc. Μόλις εγκατασταθεί, μπορούμε αφού ανοίξουμε ένα αρχείο να διαβάσουμε το κρυμμένο υδατογράφημα που είναι ενσωματωμένο (αν υπάρχει). Για πιο απαιτητικές περιπτώσεις η Digimarc προσφέρει το individual Creator ID (με άδεια ενός έτους) που μας επιτρέπει να ενσωματώνουμε υδατογράφημα στις εικόνες, προτού τις βγάλουμε στον Internet. Έπειτα εταιρικοί χρήστες μπορούν να χρησιμοποιήσουν το MarcSpider το οποίο ψάχνει όλο το δίκτυο για παράνομες εικόνες και αναφέρει οποιαδήποτε παράνομη αναπαραγωγή τους.

Είναι δυνατόν συντάκτες, σχεδιαστές, δημιουργοί να μην πάσχουν πλέον από κλοπές κλπ ; Η ιστορία μας έχει μάθει ότι σε κάθε πρόβλημα υπάρχει μία λύση αλλά και αντιθέτως, σε κάθε λύση υπάρχει ένα πρόβλημα! Όπως πολλά άλλα προγράμματα που σπάζουν τους καθιερωμένους μηχανισμούς ασφάλειας, υπάρχουν προγράμματα που προορίζονται να καταδείξουν την αδυναμία των τρεχόντων αλγόριθμων έτσι ώστε οι επιχειρήσεις να παρακινηθούν και να αναπτύξουν ακόμα πιο γερές υδατογραφικές τεχνολογίες.
Παρά τις προσπάθειες των κατασκευαστών το υδατογράφημα δεν αποδείχθηκε αρκετά γερό. Το υδατογράφημα μπορεί να επιζήσει πολλών πραγμάτων όπως ρυθμίσεις φωτεινότητας και αντίθεσης, που εφαρμόζουν τα ειδικά φίλτρα ακόμα και εκτύπωση η σάρωση, αλλά δεν μπορεί να επιζήσει από ειδικά προγράμματα όπως το StirMark (http://www.cl.cam.ac.uk/users/fapp2/steganography /image_watermarking/stirmark) και UnZign (http://www.altern.org/watermark) τα οποία είναι δύο παραδείγματα λογισμικού που εμφανίστηκαν στο δίκτυο αμέσως μετά την ανακάλυψη κάθε τεχνολογίας υδατογραφήματος και μπορούν να αφαιρέσουν πληροφορίες πνευματικών δικαιωμάτων από αρχεία. Προφανώς αυτά τα εργαλεία δεν στοχεύουν ενάντια σε κάποιο αλγόριθμο Στεγανογραφίας , αλλά μάλλον σε συγκριτικές μετρήσεις επιδόσεων που μας βοηθούν να ξεχωρίσουμε ώστε να επιλέξουμε το πιο αξιόπιστο για υδατογράφημα λογισμικό. Τα συμπεράσματα στα οποία οδηγούμαστε είναι: μερικά υδατογραφήματα αφαιρούνται εύκολα ή καταστρέφονται με το χειρισμό των διάφορων

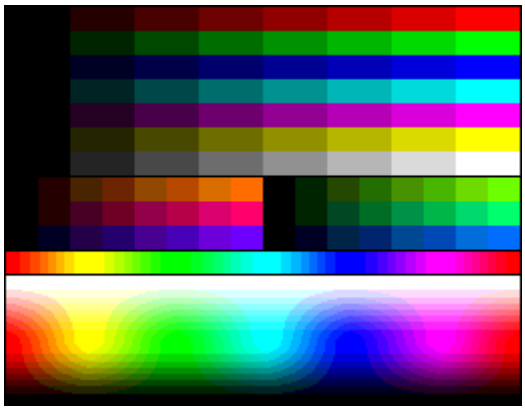
χαρακτηριστικών του αρχείου, δυστυχώς σήμερα όλα τα υδατογραφήματα μπορούν να καταστραφούν χωρίς σημαντική απώλεια στην ποιότητα της εικόνας.

2.4. Στεγανογραφία με ψηφιακή εικόνα

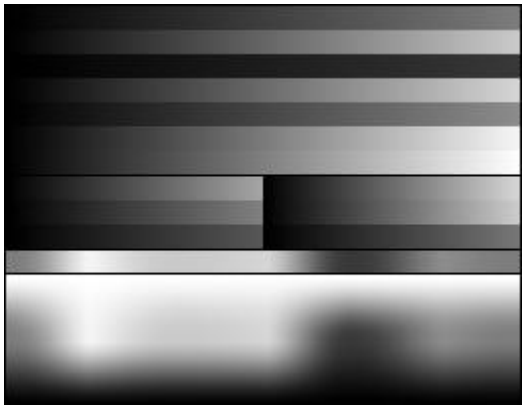
Σήμερα, κατά τη μετατροπή μιας εικόνας από αναλογική μορφή σε ψηφιακή ,έχουμε την επιλογή συνήθως μεταξύ τριών διαφορετικών ειδών χρωμάτων :

- 24-bit χρωματισμό: κάθε pixel μπορεί να έχει 2^{24} χρώματα, και αυτά αντιπροσωπεύουν διαφορετικές ποσότητες των τριών βασικών χρωμάτων: κόκκινο (R), πράσινο (G), μπλε (B), που δίνονται από 8-bit (256 τιμές) το κάθε ένα.
- 8-bit χρώμα: κάθε pixel μπορεί να έχει 256 (2^8) χρώματα, που επιλέγονται από μια παλέτα ή αλλιώς από ένα πίνακα χρωμάτων.
- 8-bit κλίμακα του γκρίζου : κάθε pixel μπορεί να έχει 256 (2^8) σκιές της κλίμακας του γκρίζου.

Εικόνα 1 24bit palette



Εικόνα 2 8bit palette



Εικόνα 3 8bit grayscale

Θα δούμε τη μέθοδο του λιγότερου σημαντικού ψηφίου. Η μέθοδος εισαγωγής LSB τροποποιεί το LSB κάθε χρώματος στις εικόνες 24-bit ή

8-bit.

Παράδειγμα:

Το γράμμα "A" σε κώδικα ASCII είναι το 65 (δεκαδικό), το οποίο είναι το 10000001 στο δυαδικό.

Χρειάζονται τρία διαδοχικά pixel σε μια εικόνα 24-bit για να αποθηκεύσει ένα "A":

Ας θεωρήσουμε ότι τα pixel πριν από την εισαγωγή είναι:

Πρώτο pixel :10000000.10100100.10110101,
Δεύτερο pixel:10110101.11110011.10110111,
Τρίτο pixel:11100111.10110011.00110011

Οι τιμές κάθε pixel μετά από την εισαγωγή ενός "A" θα είναι:

*1000000**1**.10100100.1011010**0**,*
*1011010**0**.1111001**0**.1011011**0**,*
*1110011**0**.1011001**0**.00110011*

(Οι τιμές σε **bold** είναι αυτές που τροποποιήθηκαν από το μετασχηματισμό)

Στο ίδιο παράδειγμα για μια 8-bit εικόνα θα χρειαστούν 8 pixel:

10000000, 10100100, 10110101, 10110101, 11110011,
10110111, 11100111, 10110011

Οι τιμές τους μετά από την εισαγωγή ενός "A" θα ήταν:

*1000000**1**, 10100100, 1011010**0**, 1011010**0**, 1111001**0**,*
*1011011**0**, 1110011**0**, 10110011*

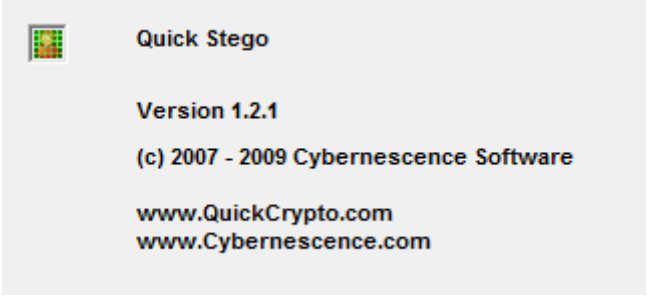
Παρατήρηση :Από τα παραπάνω παραδείγματα συμπεράνουμε ότι η εισαγωγή ενός LSB έχει συνήθως πιθανότητα 50% να αλλάξει για κάθε 8-bit, προσθέτοντας πολύ λίγο θόρυβο στην αρχική εικόνα.

Για εικόνες 24-bit η τροποποίηση μπορεί να επεκταθεί μερικές φορές και στο δεύτερο ή ακόμα και τρίτο LSB χωρίς να είναι ορατή η αλλαγή. Οι 8-bit εικόνες έχουν άντ' αυτού ένα περιορισμένο διάστημα πού μπορούν να επιλεγούν τα χρώματα, έτσι είναι συνήθως δυνατό να αλλαχτεί μόνο το LSB σε αυτά χωρίς η τροποποίηση να είναι ανιχνεύσιμη.

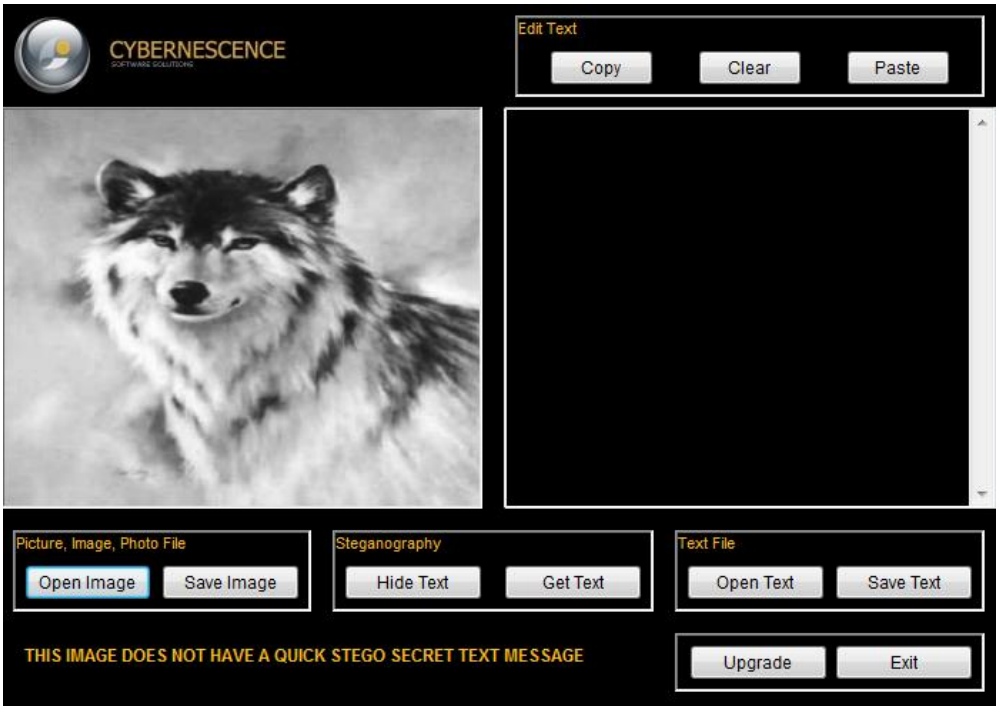
Θεωρούμε το παρακάτω κείμενο ένα μήνυμα που θέλουμε να κρύψουμε :

Θα πρέπει όλοι μαζί να συμβάλουμε στην ανασυγκρότηση του κράτους. Για το λόγω αυτό θα πρέπει ήσυχα να σταματήσουμε τις εισαγωγές, να ασχοληθούμε με την Ναυτιλία, Αλιεία & Γεωργία για την εγχώρια αγορά, να στραφούμε προς τη Ρωσία και να πουλήσουμε ότι μεταχειρισμένο πήραμε έως σήμερα.

Το παραπάνω κείμενο θα το κρύψουμε στην εικόνα με το λύκο, με τη βοήθεια του προγράμματος



Η εικόνα χωρίς το μήνυμα, μόλις έχει φορτωθεί και χωρίς αλλοίωση είναι η παρακάτω.



Στη συνέχεια δίνουμε το μήνυμα ώστε να αποθηκευτεί μέσα στην εικόνα.

Εκτελούμε τον αλγόριθμο για την απόκρυψη του μηνύματος και αποθηκεύουμε την εικόνα με το κρυμένο μήνυμα μέσα της. Παρακάτω δίνουμε τις δύο φωτογραφίες. Αριστερά την φωτογραφία χωρίς το κείμανο και δεξιά αυτή με το κείμενο.


2.5. Στεγανογραφία με ψηφιακό ήχο

Στοιχεία που κρύβονται σε ακουστικά σήματα είναι ιδιαίτερα προκλητικά, επειδή το ανθρώπινο ακουστικό σύστημα δεν λειτουργεί πέρα από ένα δυναμικό εύρος συχνοτήτων. Μπορεί να αντιλαμβάνεται ένα εύρος της δύναμης πάνω από ένα δισεκατομμύριο προς ένα και ένα εύρος συχνοτήτων μεγαλύτερο από χίλια προς ένα.
Η ευαισθησία σε κάθε πρόσθετο τυχαίο θόρυβο είναι επίσης έντονη. Οι διαταραχές σε ένα αρχείο ήχου μπορεί να εντοπίζονται τόσο χαμηλά όπως ένα bit προς δέκα εκατομμύρια (80 DB κάτω από το επίπεδο περιβάλλοντος).
Εντούτοις, υπάρχουν μερικές "ευαισθησίες" της αντίληψης διαθέσιμες. Το ανθρώπινο ακουστικό σύστημα ενώ έχει μεγάλο δυναμικό εύρος συχνοτήτων , έχει επίσης έναν αρκετά μικρό διαφορικό εύρος. Κατά συνέπεια, οι δυνατοί ήχοι τείνουν να καλύψουν πιο ασθενείς ήχους . Επιπλέον το ανθρώπινο ακουστικό σύστημα είναι ανίκανο να αντιληφθεί την απόλυτη φάση αλλά μόνο τη σχετική φάση. Τέλος, υπάρχουν μερικές περιβαλλοντικές διαστρεβλώσεις τέτοιες ώστε να αγνοούνται από τον ακροατή στις περισσότερες περιπτώσεις.
Εκμεταλλευόμαστε πολλά από αυτά τα γνωρίσματα στη παρακάτω μέθοδο καθώς έχουμε λάβει υπόψη προσεκτικά τις ευαισθησίες του ανθρώπινου ακουστικού συστήματος.
Μία ακουστική ακολουθία σε αναλογική μορφή για να την επεξεργαστούμε σε ψηφιακή μορφή θα πρέπει πρώτα να ορίσουμε την συχνότητα δειγματοληψίας από την οποία όσο πιο πολλά δείγματα έχουμε τόσο μεγαλύτερο το μέγεθος του αρχείου αλλά και καλύτερη η ποιότητα του ήχου. Τα βήματα που ακολουθούμε για να κρύψουμε δεδομένα σε ένα ηχητικό αρχείο δεν διαφέρουν και πολύ από αυτά που κάναμε για την εικόνα. Δηλαδή πάλι σκοπός μας είναι να αλλάξουμε το τελευταίο σημαντικό ψηφίο (LSB).
Παράδειγμα :
Έχουμε ένα αρχείο ήχου σε wav μορφή με τα ακόλουθα χαρακτηριστικά :
44100 Hz 16-bit stereo του ενός λεπτού.

Διαστάσεις αρχείου = (16-bit x 44100 Hz x 60sec) x 2 (το stereo είναι δικάναλο)
= 84672000 bit
Έχουμε συνεπώς μέγεθος για να κρύψουμε στο αρχείο (χρησιμοποιώντας τα 2 τελευταία LSB) = 84672000 bit / 16 x 2 = 10584000 bit
προσοχή : Ποτέ δεν κρύβουμε μία πληροφορία σε ένα wav ή bmp αρχείο και μετά το συμπιέζουμε η ακόμα και αν αλλάξουμε τη μορφή του διότι υπάρχει μεγάλος κίνδυνος να χαθούν αυτά που είχαμε κρύψει.

Τα ηχητικά δείγματα είναι από την φύση τους ανακριβείς εκτιμήσεις της σωστής αξίας τιμών σε μια δεδομένη χρονική στιγμή. Τα ηχητικά δείγματα σε μορφή WAV αποθηκεύονται είτε σαν 8-bit είτε σαν 16-bit που περνούν τελικά από το μετατροπέα της κάρτας ήχου. Για τα δείγματα 8-bit σημαίνει ότι οι τιμές μπορούν να κυμανθούν μεταξύ 0 και 255 δείγματα , για τα 16-bit κυμαίνονται μεταξύ 0 και 65535. Στο συγκεκριμένο παράδειγμα αυτό που θα κάνουμε είναι να διαμοιράσουμε τα bit-pattern που αντιστοιχούν στο αρχείο που θέλουμε να κρύψουμε στα λιγότερα σημαντικά bit του ηχητικού δείγματος.

- παραδείγματος χάριν ας υποθέσουμε ότι ένα ηχητικό δείγμα έχει κάπου τα ακόλουθα οκτώ bytes πληροφορίας: 132 134 137 141 121 101 74 38

Σε δυαδικό αυτά θα είναι :
10000100 10000110 10001001 10001101 01111001 01100101 01001010 00100110
(το LSB κάθε αριθμού σε κόκκινο)

- Ας υποθέσουμε ότι θέλουμε να κρύψουμε το δυαδικό 11010101 (213) εσωτερικά σε αυτή την ακολουθία. Αντικαθιστούμε απλά το LSB (λιγότερο σημαντικό bit) κάθε byte δείγματος με το αντίστοιχο κομμάτι byte που προσπαθούμε να κρύψουμε. Έτσι η παραπάνω ακολουθία θα αλλάξει ως εξής:
  133 133 137 142 121 100 74 39
  Στο δυαδικό αυτό είναι :
  10000101 10000101 10001001 10001110 01111001 01100100 01001010 00100111
- Παρατηρούμε ότι η τιμή του ηχητικού δείγματος έχει αλλάξει το πολύ κατά μια μονάδα για το καθένα . Αυτή ή αλλαγή δεν θα είναι αντιληπτή από το ανθρώπινο αυτί και ταυτόχρονα έχουμε κρύψει πάλι 8-bit πληροφορίας μέσα στο δείγμα.

2.6. Εν κατακλείδι

Η Στεγανογραφία είναι μια αρχαία τέχνη που έχει διαδοθεί και αναπτυχθεί με την εμφάνιση του διαδικτύου και γενικά από τα ψηφιακά μέσα. Δεν είναι πλέον μια μέθοδος που περιορίζεται στη μυστική επικοινωνία μεταξύ δύο κατασκόπων ή κάποια άλλη χρήση της σε διάρκεια πολέμου. Τα εργαλεία είναι τώρα προσιτά στους χρήστες και σε αρκετές περιπτώσεις δωρεάν μέσω του διαδικτύου, τα οποία πολλές φορές δεν απαιτούν καμία ειδική γνώση για τη λειτουργία τους.
Θα μπορούσαμε να χρησιμοποιούμε την στενογραφία παράλληλα με τη κρυπτογραφία. Αυτό έχει διάφορα πλεονεκτήματα και μειονεκτήματα. Πλεονέκτημα είναι ότι αυξάνει την δυνατότητα προστασίας της μυστικότητάς μας, ή την επικοινωνία μας όταν το απαιτούν οι συνθήκες. Μειονέκτημα είναι η αυξανόμενη δυνατότητα για τους εγκληματίες και τους τρομοκράτες να επικοινωνούν μεταξύ τους χωρίς να ανιχνεύονται από την δικαιοσύνη. Η απαγόρευση της τεχνολογίας δεν είναι επαρκής για να σταματήσει την εγκληματική χρήση. Η Στεγανάλυση ενώ κατευθύνεται στο να γίνει αποτελεσματική, αντιμετωπίζει πολλά εμπόδια για να γίνει μια αξιόπιστη μέθοδος ανίχνευσης στεγανογραφικής δραστηριότητας.

Η Στεγανογραφία και η Στεγανάλυση είναι ακόμα σε στάδια έρευνας και ανάπτυξης. Δεδομένου ότι οι τεχνικές για το κρύψιμο πληροφορίας βελτιώνονται, το ίδιο ισχύει και για την ανίχνευση. Στην πραγματικότητα, η Στεγανογραφία είναι μέρος του ίδιου κύκλου με την επιβολή του νόμου και της εγκληματικότητας.
Δεδομένου ότι η ικανότητα της επιβολής του νόμου αυξάνεται, έτσι και η ικανότητα της εγκληματικότητας αυξάνεται. Η μόνη επιλογή είναι η συνεχής πρόοδος. Η Συνεχής πρόοδος και η έρευνα είναι ο μόνος τρόπος στο για να μην σταματήσει ο κύκλος υπέρ εκείνων που κάνουν κακή χρήση της τεχνολογίας.

3. Αναφορές.

1. Από το site της Wikipedia (http://en.wikipedia.org/wiki/Steganography)
2. Από το site της Wikipedia (http://en.wikipedia.org/wiki/Security_through_obscurity)
3. Από το site της Wikipedia (http://en.wikipedia.org/wiki/Cryptography)
4. Πτυχιακή εργασία στη στεγανογραφία Γεωργακόπουλου Νικόλαου , Κρήτη, 2001
5. DATA HIDING: STEGANOGRAPHY AND COPYRIGHT MARKING, Stefano Cacciaguerra & Stefano Ferretti, Department of Computer Science, University of Bologna,