

# Στεγανογραφία

Σε αυτό το εργαστήριο θα χρησιμοποιήσουμε τα λογισμικά **s-tools** και **MP3Stego** για την μελέτη της στεγανογραφίας εικόνας και ήχου αντίστοιχα.

## 1. Στεγανογραφία εικόνας και ήχου

Στεγανογραφία ονομάζεται η επιστήμη της απόκρυψης πληροφοριών μέσα σε άλλες πληροφορίες. Ιστορικά, υπήρξαν τεχνικές που χρησιμοποιούσαν αόρατο μελάνι, λεπτές εγκοπές σε έγγραφα, ακόμα και μηνύματα σε tattoos κάτω από το τριχωτό της κεφαλής του αγγελιοφόρου.

Στην σημερινή ψηφιακή εποχή, η επιστήμη της στεγανογραφίας παρέχει τεχνικές απόκρυψης μηνυμάτων σε ψηφιακά αρχεία ήχου, σε ψηφιακές εικόνες, ακόμα και τεχνικές παραγωγής ψευδο-μηνυμάτων κειμένου τα οποία στην ουσία κωδικοποιούν άλλα μηνύματα.

Ιδανικά, στη στεγανογραφία στο αρχικό μήνυμα δεν θα πρέπει να διακρίνεται η ύπαρξη του κρυμμένου μηνύματος. Γι' αυτό και χρησιμοποιούνται σαν αρχικά μηνύματα κυρίως αρχεία που περιέχουν πλεονασμό (redundancy) δεδομένων (π.χ. απλά αρχεία ήχου και εικόνας). Γενικότερα, η στεγανογραφία λειτουργεί αποτελεσματικότερα με συμπιεσμένα αρχεία όπως είναι τα JPEG και MPEG. Κάποια εργαλεία στεγανογραφίας μπορείτε να βρείτε στο παρακάτω link:

<http://www.jjtc.com/Steganography/tools.html>

### 1.1. Στεγανογραφία εικόνας

Η πιο αποτελεσματική μέθοδος για αυτούς τους είδους την στεγανογραφία είναι η μέθοδος λιγότερο σημαντικού bit - **least significant bit** (LSB) method. Σε αυτήν την μέθοδο το κρυμμένο μήνυμα τροποποιεί το τελευταίο bit του εκάστοτε byte της εικόνας. Με αυτόν τον τρόπο, το χρώμα των pixels της εικόνας τροποποιείται ελάχιστα επομένως δεν μπορεί να διακριθεί η αλλαγή που έχει πραγματοποιηθεί στην εικόνα και δυσκολεύει την ανίχνευση του κρυμμένου μηνύματος. Ο πιο κατάλληλος τύπος εικόνας για την περίπτωση αυτής της στεγανογραφίας είναι οι 24 bit Bitmap εικόνες. Αυτό οφείλεται στο μεγάλο μέγεθος των εικόνων αυτών αλλά και στην υψηλή τους ποιότητα.

Η παρακάτω ακολουθία από 24 bits αντιπροσωπεύει ένα pixel μιας εικόνας. Τα 3 bytes που καθορίζουν το χρώμα παρέχουν 256 διαφορετικές τιμές για κάθε χρώμα (red, green and blue) και επομένως μπορούν να αναπαραστήσουν συνολικά 16.7 εκατομμύρια χρώματα. Η τιμή που φαίνεται στην πιο κάτω εικόνα αντιστοιχεί στο χρώμα **dark green**:

Byte 1 - Red	Byte 2 - Green	Byte 3 - Blue
0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0

Εμείς θα πάρουμε 11 τέτοια pixels τα οποία αντιπροσωπεύουν μέρος ενός μονόχρωμου background.

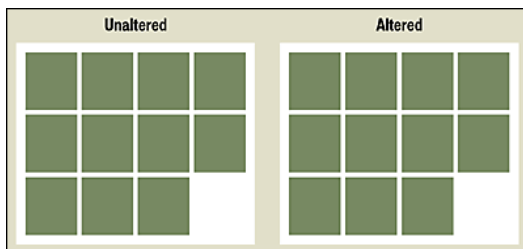
Στην παρακάτω εικόνα φαίνεται το μήνυμα που θέλουμε να κρύψουμε στην εικόνα τέσσερις χαρακτήρες **Aha! (4 bytes)** —σε κώδικα ASCII:

0 1 0 0 0 0 0 1	0 1 1 0 1 0 0 0
0 1 1 0 0 0 0 1	0 0 1 0 0 0 0 1

Στην επόμενη εικόνα τα λιγότερο σημαντικά (τα πιο δεξιά) bit του κάθε byte έχουν χρησιμοποιηθεί για να κρύψουν το κρυμμένο μήνυμα κειμένου. Το κρυμμένο μήνυμα «φιλοξενείται» σε 32 από τα 264 bits (περίπου 12%). Το μπορντώ και το κίτρινο χρώμα αντιπροσωπεύουν τα bit τα οποία αλλάζουν τιμή έτσι ώστε να συμπεριλάβουν το κρυμμένο μήνυμα. Παρατηρήστε ότι μόνο τα 15 από τα 264 bits (λιγότερα από 6%) θα πρέπει να τροποποιηθούν και μόνο οχτώ από τα 11 pixels.

Pixel	Byte 1 - Red	Byte 2 - Green	Byte 3 - Blue
1	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
2	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 0
3	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
4	0 1 0 1 0 1 1 1	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0
5	0 1 0 1 0 1 1 1	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 0
6	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 1
7	0 1 0 1 0 1 1 1	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 0
8	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 1
9	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 1
10	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 0	0 0 0 1 1 1 1 0
11	0 1 0 1 0 1 1 0	0 1 1 1 1 0 1 1	0 0 0 1 1 1 1 0

Οι εικόνες παρακάτω αντιπροσωπεύουν τα 11 pixels που έχουν τροποποιηθεί. Η αριστερή εικόνα είναι η αρχική. Η δεξιά είναι η τροποποιημένη, βάσει όσων περιγράφηκαν παραπάνω. Βλέπετε καμία διαφορά;



Αν αντί για 11 pixels (33Bytes) bitmap εικόνας είχαμε μια 300KB bitmap εικόνα file, αυτή θα μπορούσε να «φιλοξενήσει» μήνυμα των 36KB, ή αλλιώς περίπου 6,000 λέξεις.

1. Κατεβάστε από την ηλεκτρονική τάξη το **steg.zip**, αποσυμπίεστε τα αρχεία σε έναν υποκατάλογο, και εκτελέστε το **S-Tools.exe**
2. Κατεβάστε την εικόνα <http://tinyurl.com/hh6n2ec>. Ανοίξτε την με το εργαλείο S-Tools επιλέγοντας και σύροντάς τη στο παράθυρο του εργαλείου S-Tools.
3. Δημιουργήστε ένα αρχείο **hidden.txt** και γράψτε κάτι σε αυτό.
4. Για να κρύψετε το **hidden.txt** πίσω από την εικόνα, επιλέξτε και σύρετέ το πάνω στην εικόνα. Δώστε έναν κωδικό ως στεγανο-κλειδί και παρατηρήστε την εικόνα με το ένθετο αρχείο. Βλέπετε κάποια αλλαγή στην εικόνα; Υπάρχει διαφορά ως προς το μέγεθος του αρχείου;
5. Δοκιμάστε να ενθέσετε άλλα, πολύ μεγαλύτερα αρχεία. Υπάρχει κάποιο πρόβλημα;
6. Αφού ανοίξετε ένα στεγανο-φορέα (αρχική εικόνα), με δεξί κλικ επιλέξτε **“Reveal”** για να εμφανιστεί το κρυμμένο αρχείο.
7. Με βάση τα συμπεράσματά σας ως τώρα, μπορείτε να σκεφτείτε έναν τρόπο απόκρυψης του αρχείου «πίσω» από την εικόνα έτσι ώστε: i) να μην αλλάζει το μέγεθος του αρχείου και ii) να μην υπάρχει αισθητή αλλαγή στην εικόνα;

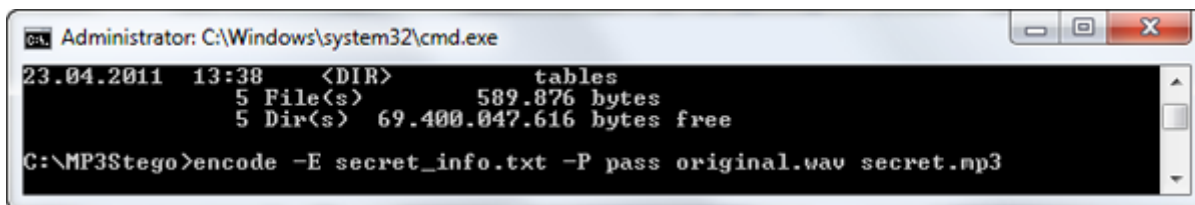
## 1.2. Στεγανογραφία ήχου

Η στεγανογραφία ήχου αναφέρεται στην προσθήκη θορύβου ή ηχούς που θα μπορούσαν να προέρχονται από τη διαδικασία του recording. Ένα από τα πιο δημοφιλή εργαλεία είναι το [Mp3stego](#). Αντί να χρησιμοποιεί την τεχνική Least Significant Bit (LSB), το MP3Stego κρύβει την πληροφορία στην «καρδιά» του αρχείου MP3 – στο “inner loop”.

Το MP3Stego προσθέτει το TXT αρχείο με το κρυμμένο μήνυμα σε ένα WAV file και το μετατρέπει σε αρχείο MP3. Τα δεδομένα που κρύβονται είναι σχεδόν αδύνατον να ανιχνευτούν.

Το MP3Stego είναι ένα απλό command line tool. Υποστηρίζει μόνο απλά TXT μηνύματα και το αρχικό audio stream θα πρέπει να είναι σε WAV format.

(The MP3Stego developer, Fabien A.P. Peticolas, co-wrote a huge piece on [steganography and its mathematic challenges](#))

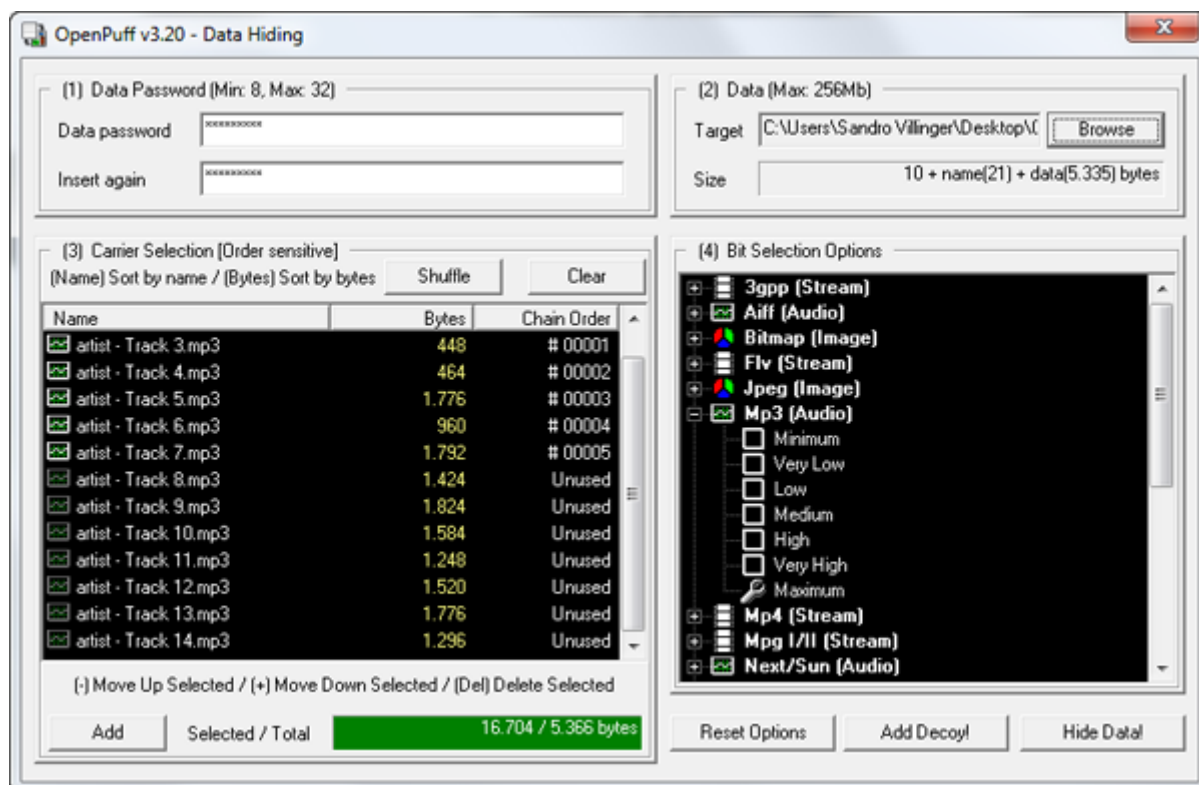


```
Administrator: C:\Windows\system32\cmd.exe
23.04.2011 13:38 <DIR>          tables
                5 File(s)          589.876 bytes
                5 Dir(s)  69.400.047.616 bytes free

C:\MP3Stego>encode -E secret_info.txt -P pass original.wav secret.mp3
```

1. Κατεβάστε από την ηλεκτρονική τάξη το **MP3Stego\_1\_1\_18.zip** και αποσυμπίστε τα αρχεία σε έναν υποκατάλογο. Επιπλέον, κατεβάστε και αποσυμπίστε τα αρχεία ήχου **original\_file.zip** και **not\_encrypted.zip**.
2. Δημιουργήστε στον προηγούμενο υποκατάλογο ένα αρχείο **hidden.txt** και γράψτε κάτι σε αυτό.
3. Ανοίξτε ένα **cmd** και μπειτε στον υποκατάλογο.
4. Χρησιμοποιήστε στο cmd την εντολή:  
`encode -E hidden.txt -P aT123 original_file.wav encrypted.mp3`  
Η εντολή αυτή συμπιέζει το αρχείο ήχου **original\_file.wav** και κρύβει σε αυτό το **hidden.txt** χρησιμοποιώντας σαν password το **aT123**  
Το αποτέλεσμα αυτής της διαδικασίας βρίσκεται στο **encrypted.mp3** που δημιουργείται.
5. Συγκρίνετε τον ήχο του **encrypted.mp3** με αυτόν του **not\_encrypted.mp3** που κατεβάσατε από την ηλεκτρονική τάξη. Μπορείτε να καταλάβετε διαφορά στα δυο αρχεία; Υπάρχει διαφορά στο μέγεθος των δυο αρχείων;
6. Για να αποκρυπτογραφήσετε το κείμενο από ένα αρχείο ήχου χρησιμοποιήστε στο **cmd** την αντίστοιχη εντολή:  
`decode -X -P aT123 encrypted.mp3`  
Η εντολή αυτή θα επιδιώξει να αποσυμπίσει αρχικά το **.mp3** αρχείο στο αρχείο **encrypted.mp3.pcm** και στη συνέχεια να εντοπίσει (αν υπάρχει) το κρυπτογραφημένο κείμενο. Σε αυτή την περίπτωση, το κρυμμένο κείμενο αποκρυπτογραφείται και αποσυμπίζεται στο αρχείο **encrypted.mp3.txt**

Ένα άλλο εργαλείο είναι το [OpenPuff 3.2](#)-. Υποστηρίζει MP3, 3gpp, Aiff, Wave και άλλες μορφές ήχου. Προσέξτε: Για να εξασφαλίσουμε ότι το αρχείο ήχου δεν θα παραμορφωθεί, το κρυφό μήνυμα θα πρέπει να έχει περιορισμένο αριθμό από bytes.



Στο παραπάνω παράδειγμα, έπρεπε να επιλέξουμε πολλαπλά MP3 files (το κάθε ένα με διαθέσιμο χώρο «αποθήκευσης» περίπου 450 Bytes έως 1.8 Kbytes) έτσι ώστε να κρύψουμε ένα 5.4 Kbyte Excel αρχείο. Παρόλο που αυτό κάνει το σύνολο των δεδομένων ογκώδες, επίσης ενδυναμώνει το αποτέλεσμα της στεγανογραφίας: Κάποιος τρίτος θα χρειαζόταν όλα τα αρχεία MP3 για να μπορέσει να ανιχνεύσει ότι υπάρχει κρυμμένη πληροφορία.

Μόλις πατήσουμε “Hide Data!”, είμαστε έτοιμοι.

*Σημείωση: Τα Easter Eggs που περιγράφηκαν δεν λειτουργούν σε όλες τις εκδόσεις του Office.*