Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Εργαστήριο Ηλεκτρονικής Διακυβέρνησης

Στεγανογραφία

Δρ. Κωνσταντίνος Παπαπαναγιώτου
conpap@di.uoa.gr

G.J. Simmons (1984): “**The Prisoners' Problem and the Subliminal Channel**”

Δύο εγκληματίες φυλακίζονται σε απομονωμένα κελιά

Επικοινωνούν ανταλλάσσοντας μηνύματα

Ο διευθυντής των φυλακών διαβάζει και μπορεί να τροποποιήσει κατά βούληση κάθε μήνυμα

Εάν θεωρήσει κάποιο μήνυμα ύποπτο αφαιρεί το δικαίωμα επικοινωνίας

Πώς θα οργανωθεί η απόδραση;

Ιστορικά:

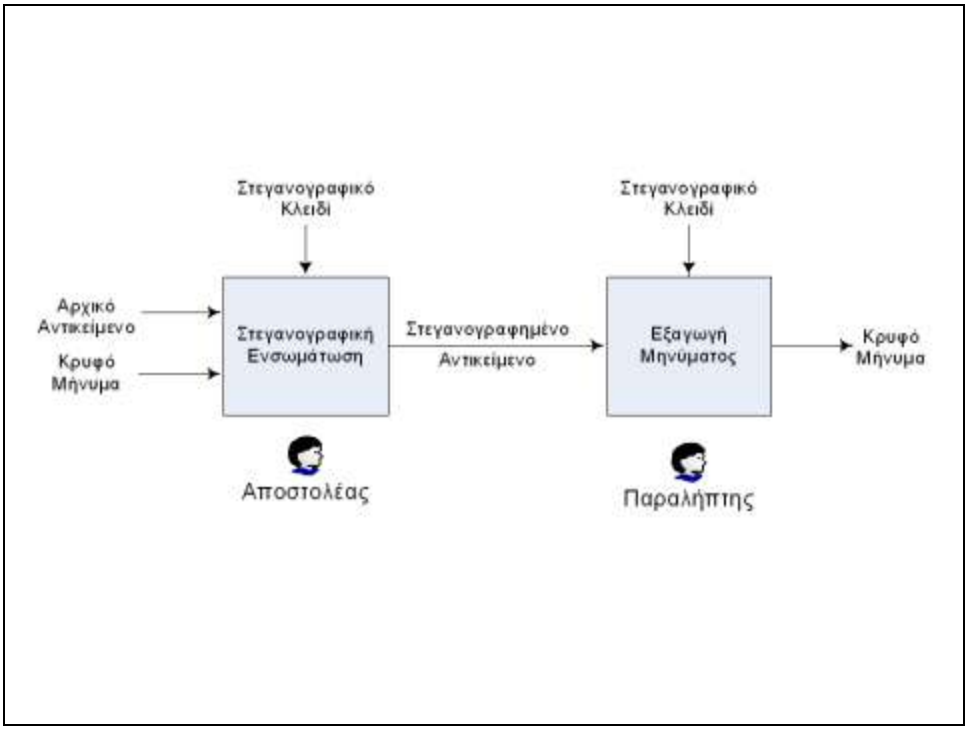
- Ηρόδοτος, 440 π.Χ.
- «Αόρατο μελάνι»
- Μικροκουκίδες (microdots)
- Τρομοκρατία

Στεγανογραφία: Ενσωμάτωση μυστικής πληροφορίας σε ένα **αρχικό αντικείμενο** (cover object)

Στεγανογραφικό **κλειδί** (stego key)

Στεγανογραφημένο αντικείμενο (stego object)

Στεγανογραφική **χωρητικότητα** (stego capacity)


Στεγανογραφικό Κλειδί
Στεγανογραφικό Κλειδί
Αρχικό Αντικείμενο
Κρυφό Μήνυμα
Στεγανογραφική Ενσωμάτωση
Στεγανογραφημένο Αντικείμενο
Εξαγωγή Μηνύματος
Κρυφό Μήνυμα
Αποστολέας
Παραλήπτης

Διαφορά με κρυπτογραφία

- Διαφέρει από την κρυπτογραφία
  - Κρυπτογραφία: Μετασχηματίζει το μήνυμα έτσι ώστε να το καθιστά ακατανόητο σε οποιονδήποτε τρίτο
  - Πολλές φορές η προστασία αυτή δεν είναι αρκετή
  - Στεγανογραφία: αποκρύπτει την ύπαρξη του μηνύματος
- Συνδυασμός κρυπτογραφίας-στεγανογραφίας
  - Το κρυφό μήνυμα κρυπτογραφείται πριν ενσωματωθεί στο αρχικό αντικείμενο

Προστασία Πνευματικών Δικαιωμάτων

- Ψηφιακή υδατογραφία
  - Ένα αντικείμενο σημαδεύεται με τέτοιο τρόπο ώστε να μη μπορεί να αντιγραφεί ή να αποδεικνύεται η ταυτότητα του ιδιοκτήτη σε περίπτωση διαφωνίας
  - Εφαρμογή υδατογραφίας σε ψηφιακά μέσα
- Fingerprinting
  - Διαφορετικά σημάδια τοποθετούνται σε αντίγραφα του ίδιου αντικειμένου (κρυφός σειριακός αριθμός)
- Στην υδατογραφία δε ενδιαφέρει τόσο η απόκρυψη του μηνύματος, όσο το να μη μπορεί να καταστραφεί ή να αλλαχθεί

Εφαρμογές

- Πρακτικά σε οτιδήποτε παρουσιάζει πλεονασμό:
  - Εικόνα
  - Ήχος
  - Video
  - Δικτυακά πρωτόκολλα (π.χ. δρομολόγησης)
  - Κείμενα φυσικής γλώσσας

Το πιο διαδεδομένο πεδίο εφαρμογής

Εκμετάλλευση των αδυναμιών του ανθρώπινου οπτικού συστήματος

- π.χ. το ανθρώπινο μάτι διακρίνει περίπου 1Μ χρώματα

Απλούστερος Αλγόριθμος: LSB (Least Significant Bit)

- το κρυφό μήνυμα αποθηκεύεται στα LSB των pixels
- π.χ. στο LSB ενός χρώματος RGB
- 2 ή και 3 bit μπορούν να αλλαχτούν
- Οι αλλαγές αυτές μπορούν να θεωρηθούν θόρυβος και δεν επιφέρουν σημαντικές οπτικές αλλαγές στην εικόνα.

Εφαρμογή σε πεδία μετασχηματισμών

- DCT (Discrete Cosine Transform)
- Πεδίο συχνοτήτων (μετασχηματισμός Fourier)

Τεχνικές masking

- συνήθως χρησιμοποιούνται στην υδατογραφία
- ο παρατηρητής αδυνατεί να ξεχωρίσει ένα σήμα παρουσία ενός άλλου
- π.χ. φωτεινές ή σκοτεινές περιοχές

Εκμετάλλευση των αδυναμιών του ανθρώπινου αυτιού

Εφαρμογή του LSB σε ηχητικά δείγματα

Τεχνικές masking

π.χ. ασθενέστερος ήχος παρουσία ενός πολύ δυνατότερου

Απόκρυψη σε ηχώ (echo hiding)

Πεδία Μετασχηματισμών (π.χ. FFT)

Στεγανογραφία σε γλώσσες markup

- π.χ.
  <image src='test.jpg', alt='test', width='85', height='85'>
- Αλλαγή στη σειρά εμφάνισης των πεδίων
  - π.χ.
    <image src='test.jpg', alt='test', height='85', width='85'>
- Εισαγωγή κενών (white space steganography)
  - π.χ.
    <image src='test.jpg', alt='test', width='85', height='85'>
  - χρήση πολλαπλών κενών ή και TAB
- Χρήση του χαρακτήρα τέλους (/)
  - π.χ.
    <image src='test.jpg', alt='test', width='85', height='85'/>
  - <image src='test.jpg', alt='test', width='85', height='85'></image>

Στεγανογραφία σε φυσική γλώσσα

- Η συντακτική φύση της γλώσσας καθιστά δύσκολη την εφαρμογή παραδοσιακών αλγορίθμων στεγανογραφίας
- Απαιτείται ανάλυση της σημασιολογικής και συντακτικής δομής της πρότασης
- Chomsky: είναι δυνατή η παραγωγή πολλαπλών προτάσεων από τη βαθεία δομή, με γλωσσικούς μετασχηματισμούς (Μετασχηματιστική Γραμματική - Transformational Grammar)
- Συμβολικός Μετασχηματισμός
  - πιο διαδεδομένος μετασχηματισμός
  - αντικατάσταση συνωνύμων ή λεξική στεγανογραφία
- Συντακτικός Μετασχηματισμός
  - π.χ. παθητικοποίηση, κ.λ.π.
- Σημασιολογικός Μετασχηματισμός
  - π.χ. συναναφορά, κ.λ.π.

Στεγανάλυση

- Επίθεση σε στεγανογραφικούς αλγορίθμους
- Οπτικές επιθέσεις
  - Εμπειρία
  - Αλγόριθμοι φιλτραρίσματος
  - Εξαιρετικά χρονοβόρα και δαπανηρή διαδικασία
- Στατιστικές επιθέσεις
  - π.χ. κατανομή χρώματος ή συχνοτήτων

Τέλεια Στεγανογραφία;

- Υπάρχει τέλεια στεγανογραφία, όπως υπάρχει τέλεια κρυπτογραφία (one time pad)
- Ο διευθυντής της φυλακής δε θα πρέπει να μπορεί να ξεχωρίσει ένα κανονικό μήνυμα από ένα που περιέχει στεγανογραφημένη πληροφορία
- Θεωρούμε ότι ένα σύστημα στεγανογραφίας έχει παραβιαστεί αν κάποιος κακόβουλος χρήστης αντιληφθεί την ύπαρξη συγεκαλυμμένης επικοινωνίας
  - ανεξάρτητα από το αν αποκαλυφθεί το κρυφό μήνυμα
- Πρόβλημα της Θεωρίας Πληροφορίας
- Πρακτικά: Στατιστικές μέθοδοι και εμπειρία επιβεβαιώνουν την ασφάλεια ενός στεγανογραφικού συστήματος