

TEMA 10

Metode steganografice de
protecție a informației

Cuprins

- Ce este steganografia?
- Implementări ale steganografiei
- Detectarea steganografiei
- Combaterea steganografiei
- Concluzii
- Întrebări

Ce este steganografia?

“stegos” - *acoperit, ascuns, protejat*

“graphia” - *scris*

Ce este steganografia?

Arta de a ascunde informația
în interiorul altei informații

*Deoarece toată lumea poate citi, codarea
textului în propoziții neutre este în mod
incontestabil eficace*

Ce este steganografia?

*Since everyone can read, encoding text
in neutral sentences is doubtfully effective*

*Since **E**veryone **C**an **R**ead, **E**ncoding **T**ext
In **N**eutral **S**entences Is **D**oubtfully **E**ffective*

⇒ Secret inside

Ce este steganografia?

La ce folosește?

- Ascunderea faptului de transmitere a mesajului
- Ascunderea unor mesaje în interiorul datelor
- Watermark (filigran) digital
- Diferit de criptografie
- Nu se cunoaște cantitatea de date stocate

Ce este steganografia?

Watermark-ul digital

- Nu ascunde informația
- Important: nu se poate modifica
- Utilizează proprietatea de a ascunde a Steganografiei
- Recent: MPAA ascunde watermark-urile în filme

Implementări

Ascunderea informației

- Text / Pagini Web
- Imagini
- Audio
- Video

Implementări

Text / Pagini Web

- Utilizează cartea de coduri
- Aspectul textelor
- Fiecare al n -lea caracter
- Utilizarea spațiilor și a liniilor noi
- Poate fi dificil de detectat sau decodat

Implementări

Text / Pagini Web

In the midway of this our mortal life,
I found me in a gloomy wood, astray
Gone from the path direct: and e'en to tell
It were no easy task, how savage wild
That forest, how robust and rough its growth,
Which to remember only, my dismay
Renews, in bitterness not far from death.
Yet to discourse of what there good befell,
All else will I relate discover'd there.
How first I enter'd it I scarce can say

Implementări

Text / Pagini Web

In the midway of this our mortal life,
I found me in a gloomy wood, astray
Gone from the path direct: and e'en to tell
It were no easy task, how savage wild
That forest, how robust and rough its growth,
Which to remember only, my dismay
Renews, in bitterness not far from death.
Yet to discourse of what there good befell,
All else will I relate discover'd there.
How first I enter'd it I scarce can say

06081913030629170827 ⇒ *meet at dawn*

Implementări

Imagini

- Imaginea container
- Identificarea datelor redundante
- Înlocuirea (unei submulțimi) de biți redundanți cu date

Implementări

Imagini

- JPEG utilizează Transformarea Cosinus Discretă DCT
- Transformă blocul de pixeli în coeficienți DCT
- Obține bitul de semnificație minimă (LSB - least significant bit) al fiecărui coeficient DCT
- Înlocuiește LSB cu bitul mesajului secret
- Inserează DCT-ul modificat în imaginea-rezultat

Implementări

Imagini



Imaginea originală



Imaginea cu date incorporate

Implementări

Images

- JPEG stegencrytion
 - Operates in transformation space
 - No visual changes
- GIF and BMP stegencrytion
 - Operates in low bit planes
 - Subject to visual attacks

Implementări

Imagini



Imaginea originală



Imaginea cu date incorporate

Implementări

Audio

- Folosește frecvențe nepercepute de oameni
- Incorporează date folosind LSB
- Codifică tonurile muzicale

Implementări

Video

- Semnale vizibile (gesturi, mișcări)
- Aceleași tehnici ca la imagini
- Aceleași tehnici ca la audio

Detectarea steganografiei

Text

- Look for (disturbings of) patterns
- Odd use of language
- Line heights and whitespaces

Detectarea steganografiei

Imagini

- Analiza paletei de culori
- Marimea fișierului imagine
- Diferențe:
 - Format
 - Data *Ultimei modificări*

Detectarea steganografiei

Imagini

- Analiza statistică
- Analiza frecvenței coeficienților DCT
- Entropia datelor redundante
- Conținut ascuns \Rightarrow entropie mai mare

Detectarea steganografiei

Imagini

- Aplicarea filtrelor în steganograme
- Reprezentarea vizuală a datelor statistice

Detectarea steganografiei

Filtrare



Imaginea originală



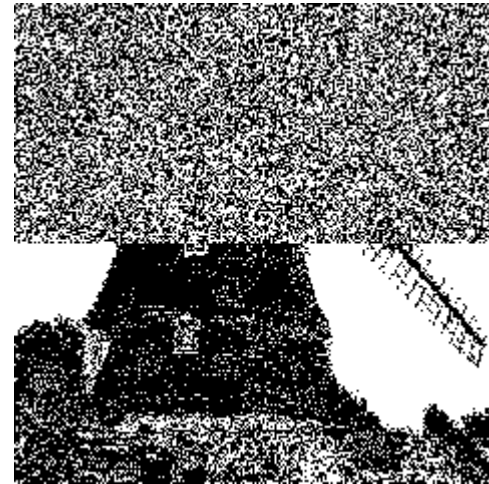
Date incorporate

Detectarea steganografiei

Filtrare



Imaginea originală



Date incorporate

Detectarea steganografiei

Audio

- Analiza statistică
- Analiza pattern-elor zgomotului de fond
- Distorsiuni
- Măsurarea frecvențelor neauzite

Detectarea steganografiei

Video

- Căutarea mișcărilor distinctive
- Aceleași tehnici ca și în cazul imaginilor
- Aceleași tehnici ca și la audio

Combaterea steganografiei

Text

- Modificarea spațiilor, punctuația
- Modify line heights, layout
- Add or remove words
- Modificarea înălțimii liniilor, a aspectului
- Adăugarea sau eliminarea cuvintelor

Combaterea steganografiei

Imagini

- Comprimare cu pierdere de date
- Conversia în alt format
- Redimensionarea imaginii
- Modificarea culorilor

Combaterea steganografiei

Audio

- Comprimare cu pierdere de date
- Modificarea bitrate-ului
- Modificarea / limitarea spectrului frecvenței

Combaterea steganografiei

Video

- Aceleași tehnici ca pentru imagini
- Aceleași tehnici ca pentru audio

Relația cu Criptografia

- Steganografia și Criptografia nu e același lucru
 - Criptografia încearcă să modifice conținutul mesajului în așa fel încât să nu poată fi citit fără cheia corespunzătoare
 - Steganografia încearcă să ascundă complet existența mesajului
- Ambele concepte pot fi utilizate împreună
 - Ordinea operațiilor este relevant
 - Un mesaj ascuns care este criptat mai întâi
 - Un mesaj criptat care conține un mesaj ascuns

Steganografie vs Criptografie

Steganografie	Criptografie
Necunoașterea transmiterii mesajului	Cunoașterea transmiterii mesajului
Previne descoperirea existenței mesajului	Previne descoperirea conținutului mesajului de către o entitate neautorizată
Tehnologii puțin obișnuite	Tehnologii obișnuite
Tehnologia se dezvoltă încă pentru anumite formate	Majoritatea algoritmilor cunoscuți de toți
Mesajul o dată detectat devine cunoscut	Algoritmii moderni sunt rezistenți la atacuri
Nu modifică structura mesajului secret	Modifică structura mesajului secret

Concluzii

- Ascunde datele practic oriunde
 - Detectarea Steganografiei
 - posibilă, dar poate fi dificilă
 - dificilă când corepunde principiului
- Kerckhoff
- Combaterea steganografiei nu este dificilă

Sarcini

- Analiza metodei LSB pentru imagini
- Analiza transformării DCT
- Studiu despre domeniile de aplicare a steganografiei

Întrebări???

