2-Layer Security System for Hiding Sensitive Text Data on Personal Computers

Nouf Al-Otaibi and Adnan Gutub

Umm Al-Qura University (UQU)
Makkah, Saudi Arabia
Outline

• Introduction
• Motivation & Methods
• Cryptography & Steganography
• System Overview
• System Implementation Interface
• Testing
• Results & Comparison
Motivation:

- Secure Text Storage on Personal Computer (PC)
- Use 2-layers
  - PC independent (Cryptography Layer)
  - PC data dependant (Steganography Layer)
Methods

• Cryptography
  ▫ Converting secret data to unreadable forms...
  Unconverting it back to the readable form

• Steganography
  ▫ Hiding existence of a secret data (from observation)
Cryptography

Hiding

Key = Z

Same

Key = Z

Retrieve

Secret Data

Lock

Secret Data

Z

Key

Z

Key
Steganography model

Basic Steganography System

Cover Object → Input

Secret Object → Input

Steganography Algorithm (Embedding Part) → Output

Stego Object

Communication Channel

Cover Object

Secret Object

Stego Object

Steganography Algorithm (Detection Part) → Output

Cover Object

Secret Object
Steganography & Cryptography

- Overlapping usages for information hiding
- Steganography security hides the knowledge that there is information in the cover medium
- Cryptography reveals this knowledge but encodes the data as cipher-text and disputes decoding it without permission
- Cryptography concentrate the challenge on the decoding process while steganography adds the search of detecting if there is hidden information or not.
Process flow graph of the 2-Layer security system

Storing sensitive secret text data

Retrieving back secret text data
Overview: 2-layer security system

- Sensitive Secret Text Data
- Cover Stego Image
- Secret Encryption/Decryption Key

2-Layer Security System
- AES Symmetric Cryptography Layer
- Image Base
- Steganography Layer

Output: Stego-Image
Hiding Sensitive Secret Text Data on Personal Computers
Cryptography: AES
Steganography: Image based

- Hiding in LSBs
- Example: embedding 200 => (11001000)

  - Pixel 1: 00101101 00011101 11011100
  - Pixel 2: 10100110 11000101 00001101
  - Pixel 3: 11010011 10101100 01100011
System interface

showing: bits statistics
process of hiding sensitive text:

AES encryption
image based steganography
retrieve sensitive data
Image changes cannot be observed

Original image

Stego image
Stego Tests: Capacity Improvement

Changing: 1-LSB → 7-LSB

Steganography acceptable number of bits = 1-LSB & 2-LSB
Testing: 30 images

security relation to data dependency

Compare: 1LSB and 2LSB.
Testing Results: 30 images
security relation to data dependency
Compare: 1LSB & 2LSB.
Remarks

• Implemented visual basic platform of 2-layer security system ==> hiding sensitive text data on personal computers (PC)
• AES Crypto layer: PC independent security
• Image Based Stego layer: fully dependant on the PC data available
• Capacity improved by Stego layer accepting security of 2LSB as well as 1LSB
köszönöm! ที่ดี! děkuji
mahalo 고맙습니다
thank you
merci 谢谢 danke
Ευχαριστώ شكرا
どうもありがとうございます  gracias
2-Layered Security System for Hiding Sensitive Text Data on Personal Computers

Nouf Al-Otaibi and Adnan Gutub
Umm Al-Qura University (UQU), Makkah, Saudi Arabia