Information Hiding

Steganography and Watermarking

- ♦ It employs technologies offered by numerous science disciplines:
    - Digital Signal Processing (Images, Audio, Video)
- ♦ Information Hiding is a branch of computer science that deals with concealing the existence of a message.
- ♦ It is related to cryptography whose intent is to render messages unreadable except by the intended recipients.

    - Cryptography
    - Information Theory\Coding Theory
    - Data Compression
    - Human Visual/Auditory perception

- ♦ There are two important sub-disciplines of Information Hiding
    - Steganography
    - Watermarking

Information Hiding is applied to: (or carrier files) Images (Most frequently)

- Audio
- Video
- Text
- Executable programs

Steganography

- ♦ Steganography literally means “covered writing”.
- ♦ Steganography’s primary goal is to hide data within some other data (carrier file) such that the hidden data cannot be detected even if it is being sought.

Steganography is the science that serves to hide a specific message in a suitable cover file without making a noticeable changing with the cover that bring an attention of HSS (Human Sense Systems). Steganography simply takes one piece of information and hides it within another Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information. The files can then be exchanged without anyone knowing what really lies inside of them.

Steganography types:

There are three basic types of Steganography:

1- ***Pure Steganography:*** Pure Steganography does not require the prior exchange of a stego-key, so both sender and receiver have to access the embedding and extraction algorithms.If an outsider knows the extraction algorithm, he can extract the secret message out of every cover sent between the two parties

1. The embedding process can be described as the mapping:
   E: C x M C., where C is Cover, M is Message
2. The Extraction process consists of mapping:
   D: C M

2- ***Secret Key Steganography:*** Secret key Steganography uses stego-key to embed the secret message into a cover and extracts the secret message using the same stego-key. Both parties could agree on the key before sending the secret message.

1. The embedding process can be described as :
   EK: C x M x K C
   (where K is the key and M is the Message and C is Cover).
2. The Extraction process consists of:
   DK: C x K M

Secret Key Steganography requires the exchange of some keys, although transmission of additional secret information subverts the invisible communication.

3- ***Public Key Steganography:*** Public key Steganography requires a public key to embed the secret message and a private key in reconstruct process.

Least significant bit (LSB) insertion.

It is a common, simple approach to embedding information in image.

24-bit images: These images have a 24 bit value for each pixel in which each 8 bit value refer to the colors RED BLUE and GREEN. We can embed 3 bits of information in each pixel one in each LSB position of the three 8 bit values in 24 bit value. Increase or decrease of the value by changing the Least Significant bit doesn’t change the appearance of the image much so the resulted Stego image looks exactly same as the cover image.

8-bit images: In these images 1 bit of information can be hidden in each pixel. The pointers to entries in the palette are changed. A change of even one bit could mean the difference between a shade of red and a shade of blue. Such a change would be noticeable on the displayed image, for this reason data-hiding experts recommend using grey-scale palettes.

Example of LSB

insertion : hide the letter G in a carrier file

G in ASCII is the binary string

01000111 suppose a sequence of 8 bytes

had the values

01010100 11010101 11001100 11110001 00011101 01010001 11001100

11001000 hiding the 8 bits representing G in the LSB of the eight carrier bytes

results in

0101010**0** 1101010**1** 1100110**0** 1111000**0** 0001110**0** 0101000**1** 1100110**1**

1100100**1** - this changed 4 bits (in italics); in general, about 50% of the bit values

change

Watermarks

1. Watermarks have been proposed for Copyright Protection of digital images, audio and video and, extensively, multimedia products.
2. Watermarks are digital signals that are embedded into other digital signals (carriers file).
3. The carrier signal is not affected strongly by such an embedding (watermarks are invisible).
4. A watermark should represent exclusively the copyright owner of the product and can be detected only by him/her.

About A-PDF Watermark

A-PDF Watermark is a fast desktop utility program that lets you add images, texts, shape, and PDF (style) watermark to a batch of Acrobat PDF documents.

With A-PDF Watermark, you can create, edit and manage the text, image, shape, PDF watermark. Text watermark support either static or dynamic text, with dynamic text, you can use PDF file name, metadata information, and date time as the watermark. Image watermark support almost all of image formats includes TIFF, JPEG, JPEG 2000, GIF, BMP, PNG, ICO, WMF, EMF etc. You can create watermark using company logos, signatures, product pictures or any artwork in image formats.

A-PDF Watermark features include adding multiple watermarks to multiple PDF files in one pass, placing watermark in fixed position or tile, on top or bottom of content, making watermark rotation and transparent. A command line version is included also.

A-PDF Watermark does NOT require Adobe Acrobat, and produces documents compatible with Adobe Acrobat Reader Version 5 and above.

5. Watermarks must be robust to any product modification that does not degrade its quality.
6. Resistance against any intentional attack is required
7. In a watermarking scheme can distinguish between ***<u>three fundamental stages</u>***
   - Watermark generation, aims at producing the watermark pattern.
   - Watermark embedding, can be considered as a superposition of watermark signal on the original image.
   - Watermark detection, performed using watermark correlators or hypothesis testing

What are the differences between watermarking and steganography?

♦ Digital watermarking is a concept closely related to steganography, in that they both hide a message inside a carrier file.

♦ However, what separates them is their goal.

- Watermarking tries to hide a message related to the actual content of the carrier file,
- while in steganography the carrier file has no relation to the message, and it is merely used as a cover to hide its existence.

Steganography/Watermarking versus Cryptography

The purpose of both is to provide secret communication.

Cryptography hides the contents of the message from an attacker, but not the existence of the message.

Steganography / watermarking even hide the very existence of the message in the communicating data.

Consequently, the concept of breaking the system is different for cryptosystems and stegosystems (watermarking systems).

♦ cryptographic system is broken when the attacker can read the secrete message.

♦ Breaking of a steganographic /watermarking system has two stages:

1. The attacker can detect that steganography/watermarking has been used.
2. The attacker is able to read, modify or remove the hidden message.

A steganography/watermarking system is considered as insecure already if the detection of steganography/watermarking is possible.

.