Cryptography and Network Security II

Second Course

Lecture 11: Steganography and Watermarking

Cryptograpy & Steganography vs. Watermarking

Comparison

- Cryptography is about protecting the content of messages (their meaning).
- Steganography is about concealing the existence of messages
- Watermarking is about establishing identity of information to prevent unauthorized use
  - They are imperceptible
  - They are inseparable from the works they are embedded in
  - They remain embedded in the work even during transformation

Steganography

Basics

- The word steganography comes from the Greek *steganos* , meaning covered or secret, and *graphy* , meaning writing or drawing. Therefore, steganography literally means covered writing.
- 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 (encrypted mail, for instance).
  - The files can then be exchanged without anyone knowing what really lies inside of them
  - An image of the space shuttle landing might contain a private letter to a friend.
  - Rumor has it that terrorists used steganography to transmit messages to one another. (http://www.wired.com/news/politics/0,1283,41658,00.html)

Reference: http://members.tripod.com/steganography/stego.html

Steganography

Early Examples

In his history of the Persian Wars, Herodotus tells of a messenger who shaved his head and allowed a secret message to be tattooed on his scalp. He waited until his hair grew back. Then he journeyed to where the recipient awaited him and shaved his head again. The message was revealed. It was history's first use of steganography.

Steganography

Invisible Ink

Ancient Romans used to write between lines using invisible ink based on various natural substances such as fruit juices, urine, and milk. Their experience was not forgotten: even nowadays children play spies and write secret messages that appear only when heated.

Steganography

Invisible Ink

During the World War II the Germans developed the microdot. A secret message was photographically reduced to the size of a period, and affixed as the dot for the letter 'i' or other punctuation on a paper containing a written message. Microdots permitted the transmission of large amounts of printed data, including technical drawings, and the fact of the transmission was effectively hidden.

Steganography

Principles

- Computer Steganography is based on two principles.
  - The first one is that the files containing digitized images or sound can be altered to a certain extend without loosing their functionality.
  - The other principle deals with the human inability to distinguish minor changes in image color or sound quality, which is especially easy to make use of in objects that contain redundant information, be it 16-bit sound, 8-bit or even better 24-bit image. The value of the least significant bit of the pixel color won’t result in any perceivable change of that color.

Steganography

Process

- The data to be concealed is compressed and hidden within another file.
- The first step is to find a file which will be used to hide the message (also called a carrier or a container.)
- The next step is to embed the message one wants to hide within the carrier using a steganographic technique.
- Two different techniques commonly used for embedding are:
  - Replace the least significant bit of each byte in the [carrier] with a single bit for the hidden message.
  - Select certain bytes in which to embed the message using a random number generator; resampling the bytes to pixel mapping to preserve color scheme, in the case of an image...; hiding information in the coefficients of the discrete cosine, fractal or wavelet transform of an image; and applying mimic functions that adapt bit pattern to a given statistical distribution."

Steganography

Software

- EZStego (Stego Online, Stego Shareware, Romana Machado)
  - Java based software program which supports only GIF and PICT formats;
- Gif-It-Up v1.0 (Lee Nelson)
  - A stego program for Windows 95 that hides data in GIF files
- Hide and Seek (Colin Maroney)
  - can hide any data into GIF images;
- JPEG-JSTEG (Derek Upham)
  - can hide data inside a JPEG file
- MP3Stego (Fabien A.P. Petitcolas, Computer Laboratory, University of Cambridge)
  - can hide data inside MP3 sound files;
- Steganos (Demcom, Frankfurt, Germany)
  - encrypts files and then hides them within BMP, DIB, VOC, WAV, ASCII and HTML files.

Reference:http://www.antichildporn.org/steganog.html

Steganography Software

S-Tools

- S-Tools is one of the most popular steganography tools.
  - This program is Windows 95/98 compatible
  - It has the ability to conceal files within BMP, GIF and WAV files.
  - Allows you to simply point and click your way to hiding files.
  - It also has the ability to hide multiple files in one container.
  - It has been updated each year and can be easily downloaded by anyone. (http://members.tripod.com/steganography/stego/software.html)

Steganalysis

Basics

- Steganalysis is the art of discovering and rendering useless such covert messages.
- Steganalysis involves analysis of the carrier file
  - Simpler steganographic techniques produce some discernible change in the file size, statistics or both.
  - These changes can manifest themselves in color variations, loss of resolution and other distortions that are visible to the human eye.
  - This form of detection requires that you know what the original carrier image or file should look like.

Watermarking

Basics

- Watermarking is the practice of hiding a message about an image, audio clip, or other work of media within the work itself.
  - Watermark is hidden from the user in normal use
  - Watermark becomes visible as a result of a special viewing process

FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
E 94797458 E
WASHINGTON, D.C.
E
E 94797458 E
ONE
ONE DOLLAR
1
5

Watermarking

Examples

- Sending a message to a spy by marking certain letters in a newspaper using invisible ink
- Adding sub-perceptible echo at certain places in an audio recording.
- Embedding a picture of President Andrew Jackson into the paper during paper making process.

Watermarking

Examples

"In 1981, photographic reprints of confidential British Cabinet Documents were being printed in newspapers. Rumor has it that to determine the source of the leak, Margaret Thatcher arranged to distribute uniquely identifiable copies of the documents to each of the ministers. Each copy had a different word spacing that was used to encode the identity of the recipient."

- Digital Watermarking, Cox

Digital Watermarking

Basics

- A digital watermark is a digital signal or pattern inserted into a digital image.

Watermarking

Applications

- In a broadcast monitoring system identifying data is added to the video/audio signal prior to transmission
- Two kinds of monitoring systems exist
  - Passive Monitoring:
    - Recognize the content being broadcast
    - Compares received signals against a database of known content
    - Very expensive as large frames need to be compared
    - Useful for monitoring of competition
  - Active Monitoring:
    - Rely on information that is broadcast along with the content
    - Relatively easier to implement
    - Identification information is easily to interpret
    - Requires cooperation of broadcasting mechanism

Watermarking

Owner Identification

- Under US law the creator of a story, painting, song, or any other original work holds copyright the instant it is recorded in some physical form
  - Up to 1998 a copyright notice was required to be attached to each distributed copy if the owner wanted to protect his/her rights
  - Even after the change in 1998 when this is no longer required the awards are reduced significantly if the copyright information is not present with the work
- Textual Copyright notices have several limitations
  - They are easy to remove deliberately or inadvertently
  - They can be aesthetically ugly if they cover a part of the image
  - For music the copyright is only on the media not on the work
- Electronic watermarks are imperceptible and inseparable from the work they are contained and are hence superior

Watermarking

Proof of Ownership

- Textual notices can be erased and replaced by a forger
  - Image editors can be used to edit copyright notices
  - One solution is to register the image with copyright depository (expensive)
- Watermarking can prove image identity
  - Watermarks may also be altered
  - It is possible to prove that one image is derived from another indirectly proving the ownership

Watermarking

Other Applications

- Transaction Tracking
- Content Authentication
- Copy Control
- Device Control

Image Watermarking

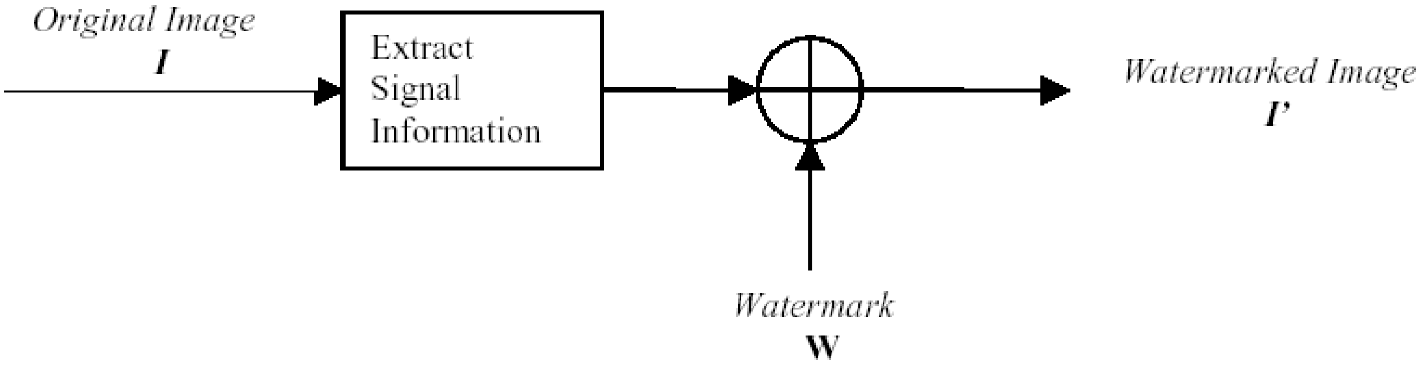
Properties

- Should be perceptually invisible to prevent obstruction of the original image.
- Statistically invisible so it cannot be detected or erased.
- Simple to extract watermark from image
  - Otherwise, the detection process requires too much computation time.
- Detection should be accurate.
  - Few false positives & false negatives
- Should be able to produce numerous watermarks.
  - Otherwise, only a limited number of images may be marked.
- Should be robust to filtering, additive noise, compression, and other forms of image manipulation.
- Should be able to determine the true owner of the image.

Watermarking

Process

Watermark Transmission:



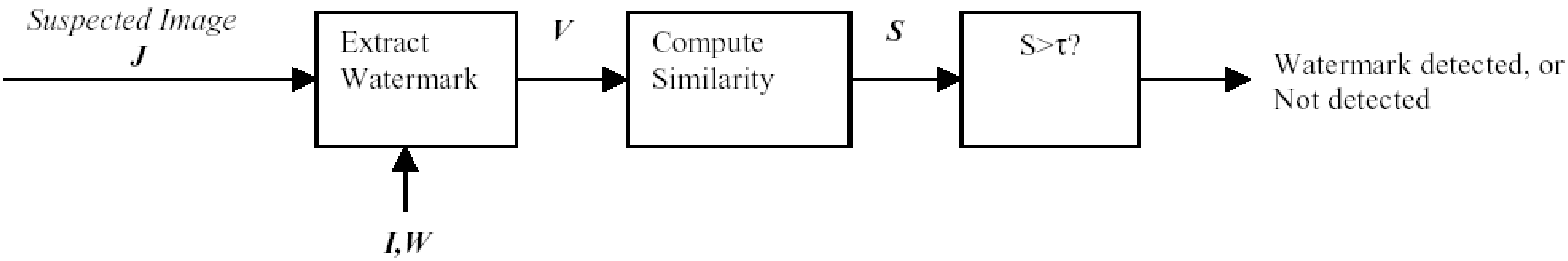
Original Image
I

Extract
Signal
Information

Watermarked Image
I'

Watermark
W

Watermark Detection:



Suspected Image
J

Extract
Watermark

I,W

V

Compute
Similarity

S

S>τ?

Watermark detected, or
Not detected

Reference: http://www.ece.utexas.edu/~bevans/courses/ee381k/projects/fall98/fu/literatureSurvey.pdf

Image Watermarking

Techniques

- M-Sequence Generator
  - Embedded or added to the last significant digit of the original image
  - Watermark was extracted by taking the least significant bits at specific locations
  - Detection was done by cross correlation of the original and extracted watermarks
- Discrete Cosine Transform (DCT)
  - Watermark was placed in perpetually significant areas of the image
  - Watermark based on 1000 random samples of a N(0,1) distribution
  - Sample was added to the 1000 largest DCT coefficients of the image
  - Inverse DCT was taken to retrieve the watermarked image
  - For detection watermark was extracted from the DCT of suspected image

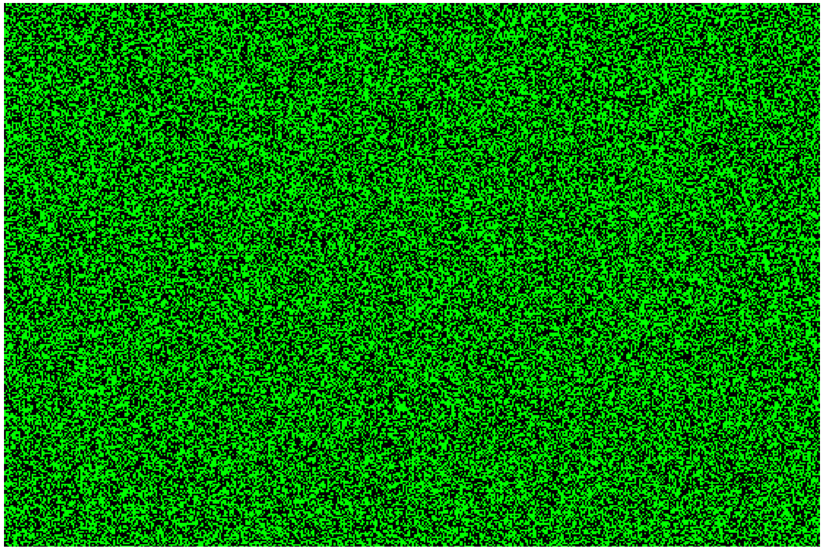
Image Watermarking

Techniques

- Discrete Wavelet Transform(DWT)
  - Watermark modeled as Gaussian noise was added to middle and high frequency bands of the image
  - Decoding process involved taking DWT of potentially marked image
- Fractal Codes
  - A collage map was composed from 8x8 blocks of original image and from image’s DCT

Watermarking

Image



Watermarking

Audio Properties

- Perceptually inaudible,
  - such that no perceptual quality degradation occurs
- Statistically undetectable
  - To ensure security
- Cannot be removed or modified by any signal processing operation (*e.g.* filtering, compression, MP3-encoding,...) without degrading perceptual quality
- Readily extractable to detect copyright information

Watermarking

Audio Techniques

- Echo Coding
- Phase Coding
- Direct-Sequence Spread Spectrum
- Frequency-Hopped Spread Spectrum
- Frequency Masking

Watermarking

Audio

Original Sound 🔈

Watermarked Sound 🔈

Echo Coding

Original Sound 🔈

Watermarked Sound 🔈

Frequency Hopped Spread Spectrum

- Wideband Audio Signal is a raw WAV file
  - Ten seconds in length
  - Sampled at 44.1 kHz
  - Quantized to 16 bits per sample