Chapter 8
Multimedia Security

Digital Watermarks for Multimedia

Digital Watermarking

- Watermarking is a method to hide secret information in a multimedia content
- The signal may be audio, pictures or video
- If the signal is copied, then the information is also carried in the copy

- Roots in Steganography
  Stegano for “covered” and graphos “to write”
Steganography - Hiding Information

- Goal
  hide secret communication
  hide secret messages in regular messages
  attacker should not see second secret message
  secret messages are "invisible"
  "invisible writing"

Simple Example 1

Taking the first letter in each word

Weather tonight increasing snow.
Unexpected precipitation smothers Eastern towns. Be extremely cautious and use snow tires especially heading East. The highways are dangerously slippery. Highway evacuation is suspected. Police report emergency situation. Should avoid the area today.

Newt is upset because he thinks he is President.

Simple Example 2

Taking the second letter in each word

Currently, many feel test is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Pershing sails from NY June 1.
Information Hiding

- Distinguished but imperceptible marks
  - Contain a hidden copyright notice or serial number
  - Help to prevent unauthorized copying directly

- Example
  - Military Communications System
    Conceal its sender, its receiver or its very existence
  - Mobile Phone System, DVD Player, Digital Election, Cash

Definition of Digital Watermarking

- Digital Watermarking technology
  allows users to embed some data into digital contents such as
  still image,
  movie and
  audio data.

- When data is embedded,
  it is not written at header part but embedded directly into
digital media itself by changing media contents data.

Multimedia and security

- Video Conferencing:
  Only allowed participants in a video conferencing session
- Pay-TV (Pay per View)
  Only allowing paying customers to listen to a live broadcast
- Video on Demand
  Only allowing paying customers to listen to a recording or file
- Restricting where, when or how a recording is accessed
How It Works?

Overall Model

Crypto & Digital Watermarking
Applications of Watermarks

- Rights management
  - Copyrights protection
  - Content distribution, tracking and monitoring
- Contents management
  - Captioning
  - Annotation
- Access/copy control
  - Prevent unauthorized copy, playback of multimedia contents
- Authentication
  - Assure contents integrity
  - Prevent unauthorized alternation of contents
  - Detect alternation location in the contents

Why? - Copyrighting

- Watermarking preserves intellectual property unlike encryption
  - Permanent proof of originality for paper media.
  - Verifies ownership of media suspected of misappropriation
- Usage Control:
  - Permanent proof of ownership for digital media.
  - Preventing people making illegal copies
- Content protection for preview
  - Digital detection of the watermark would indicate the source of the image

Why? - Authentication

- Authentication
  - Keeping things secret
  - Making sure only the right people get access to things
  - (Making sure the applications don’t have security flaws)
  - A watermark will be destroyed when the image is manipulated digitally in any way.
  - Proves authenticity of media.
    - If the watermark is still intact, then the image has not been “doctored.”
    - If the watermark has been destroyed, then the image has been tampered with.
Types of Watermarks (I)

– Visible
   A visible translucent image which is overlaid on the primary image
   Example: Visible corporate logo to protect copyrights

– Invisible
   An overlaid image which cannot be seen, but which can be detected algorithmically
   Embedding level is too small to notice
   Can be retrieved by extraction software
   Applications:
   Authentication
   Copyrighting

Visible Watermark

– Logo or seal of the organization which holds the rights to the primary image, it allows the primary image to be viewed, but still marks it clearly as the property of the owning organization.
– Overlay the watermark in a way which makes it difficult to remove, if the goal of indicating property rights is to be achieved.

Invisible Watermark

Watermarks: Secret Code for Protection

Depending on the chosen technology, one or several degrees of protection can be applied.

Watermark is embedded in the digital data, invisible to the naked eye.

Watermark is used to prevent unauthorized distribution or reproduction.
Types of Watermarks (II)

- Robust watermarks:
  - There should be no way of removing the embedded information without rendering the cover object unusable
  - Visible watermarks
  - Unperceivable watermarks
  - Fingerprinting:
    - a unique watermark in each object
  - Applications:
    - To resolve original owner/creator disputes
    - Detect copies copyrighted material
    - Fingerprinting
    - Traitor tracing – detect who leaked a copy

Types of Watermarks (II)

- Fragile watermarks
  - Any manipulation of the cover object removes the watermark
  - Can detect changed objects, compressed copies, etc.
  - Also useful with fingerprinting
  - Applications:
    - Only allow devices to play watermarked objects
    - No copies
    - Fingerprinting
    - Only allow objects to be played on one, unique device

Properties/Features of Digital Watermarks

- Invisible/Inaudible
  Information is embedded without digital content degradation, because of the level of embedding operation is too small for human to notice the change.

- Inseparable
  The embedded information can survive after some processing, compression and format transformation.

- Unchanging data file size
  Data size of the media is not changed before and after embedding operation because information is embedded directly into the media.
Image watermark

– Spatial Watermarks
  Watermark is inserted in the spatial domain
  Has low bit capacity
  Not robust to geometric distortions
– Spectral Watermarks
  Watermark is inserted in the frequency domain
  Watermark is generated using the principle of Direct Sequence Spread Spectrum (DS-SS)
  » Image Adaptive DCT Watermarking
  » Image Adaptive DWT Watermarking

Invisible Watermarking for Multimedia

– E.g. Secure Spread Spectrum
– Non-visible watermarking using random vector
– Computation of spectral components using DCT
  Discrete cosine transformation
– Computation of various frequency bands according to luminance and chroma values

Secure Spread Spectrum

– Selection of n significant points
– Change values of these points by adding watermark
  E.g. \( v'_i = v_i + \alpha x_i \)
Secure Spread Spectrum

- Identification of watermark:
  - Computing the difference between original picture and test picture
  - Comparing difference with embedded watermark
- Robust against JPEG and MPEG compression
- Robust against scaling
- Robust against changing luminance and contrast

Adaptive & Non-Adaptive Watermarking

1. Non-adaptive DCT watermarking
2. Image-adaptive watermarking using DCT
3. Image-adaptive watermarking using WT (Wavelet Transform)

Video Watermarking

- Watermark is added to I frames only
- Drift compensation signal is needed to compensate for watermark signals from previous frames
- Scene adaptive watermarking can prevent removal of watermark by inter-frame collusion
- There are mainly 3 copy protection states:
  - “one-copy”
  - “no-more-copy”
  - “never-copy”
Broadcasting of Video with Watermarking

Audio Watermarking

- Watermarking in audio signal is a challenge due to Human Auditory System (HAS)
- Two main areas considered for modification,
  - Digital representation
    - WAV, AIFF or low quality 1-law format, etc
    - Signal’s transmission pathway
      - Digital, resampled, analog and over the air
- Watermarking
  - Low bit coding
  - Phase coding
  - Spread spectrum, etc

Audio - Watermarking - Integrity

Spread spectrum: Direct Sequence Spread Spectrum encoding (DS-SS)
Watermarking 3D Objects

– Research on digital watermarking of 3D objects is becoming important as more and more 3D data is entering the World Wide Web.
– Problems:
  One must deal with low volume of data.
  Handling and editing may involve a variety of complex geometrical or topological operations.
  No unique representation of model data exists.
– The embedded watermark should be robust and resist all/most of the following modifications:
  Rotation
  Translation
  Uniform Scaling
  Polygon simplification
  Randomization of points
  Re-meshing
  Mesh smoothing operation
  Shearing

Requirements for 3D Object Watermarking

– Geometry is the best candidate for watermarking, being the least likely to be removed
– List of embedding primitives invariant to different geometrical transformations:

<table>
<thead>
<tr>
<th>Invariant to Translation &amp; Rotation</th>
<th>length of line, area of polygon, volume of polyhedron</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invariant to Rotation, Uniform Scaling &amp; Translation</td>
<td>angle, ratio of areas of two polygons</td>
</tr>
<tr>
<td>Invariant to affine transformation</td>
<td>ratio of lengths of 2 segments of a line, ratio of volumes of 2 polyhedrons</td>
</tr>
</tbody>
</table>

Triangle Similarity Quadruple (TSQ) Embedding
Tetrahedral Volume Ratio (TVR) Embedding
Mesh Density Pattern Embedding

TSQ Algorithm

- TSQ (Triangle Similarity Quadruple) Watermark Embedding

1. Find a set of triangles to be used as a Macro-Embedding Primitive (MEP)
2. Embed Marker value pair in the center triangle by changing \( e_{14}/e_{24}, h_{12}/e_{12} \)
3. Embed Subscript in the pair \( e_{02}/e_{01}, h_{0}/e_{12} \) by displacing vertex \( v_0 \)
4. Embed the two Data symbols similarly, displacing \( v_3 \) and \( v_5 \)
5. Repeat steps 1-4 until all data symbols of the message are embedded
Watermarking Standards

- Being a new field no standards so far
- Application environment is just like Compression where there are too many compression algorithms
- Users prefer to use a single best-of breed technique for each application
- Standard benchmark tests are necessary to test robustness, unintentional/intentional attacks, etc
- Standard watermark application and extraction interface would allow users to create a plug and play environment that could select a watermarking scheme out of many

Attacks: unintentional

- There are a number of unintentional and intentional attacks:
- Unintentional attacks:
  - Image: compression, transcoding, printing/scanning, filtering, noise, geometric transforms, cropping, compositing/mosaicing,...
  - Video: AD/DA conversion, compression, transcoding, text/logo insertion, geometric transformations, jitter, cropping,...

Attacks: Intentional

- Intentional attacks:
  - watermark removal/interference:
    - denoising, compression, quantization, remodulation, blurring, averaging,...
  - Desynchronization (detector disabling):
    - cropping, affine and projective transforms, jittering, mosaicing, collage,...
  - Cryptographic:
    - key determination (brute force), Oracle attack (i.e., generate unmarked data by trial and error)
  - Protocol:
    - copy attack, printing/rescanning,...

→ Watermark research must include work on attacks!
LAW

- DMCA - Digital Millennium Copyright Act
- EU copyright directive

... "Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective." ..

"..."technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter..."

Summary

- Watermarking
  - Image, Video, 3-D models, Audio and Text
  - No watermarking technique is proven robust so far
  - Study of attacks leads to intensive evaluations of different watermarking techniques
  - Need for a standard to make watermarking systems interoperable

- Who is Interested:
  - Military and intelligence agencies
  - Criminals
  - Law enforcement and counter intelligence
  - Secret communication without encryption
  - Media companies

Case studies
Case Study - Example (I)

- Digital Commerce
  - Publications
  - Digital TV, DVD
  - Digital Information (Digital Library)
  - Game
  - Music/Image/Movie
  - E-Book (Digital Book)
  - Cyber Education (E-Learning)
  - Digital Cash (Electronic Payment Protocol)

- Core
  - Digital Contents (eContents)

Nevertheless, the evolution from traditional publishing towards multimedia rich web-based publishing is underway.

1st-Generation e-publishing:
- B2B services

2nd-Generation e-publishing:
- e-commerce

3rd-Generation e-publishing:
- B2C web-based services

- Buying books online
- Buying books online (amazon.com)
- Online catalogues

Source: Arthur D. Little, GigaPort

Retailer

Distributor (incl. storage)

Printer

Publisher

Writer

Tailoring

Re-use emphasis on optimisation of the value chain

Focus on development of new services

$direct$-to-$plate$ printing

Fall 2008, Mohamad Eid ELG 5121/CSI7631-41
Case Study - Example (II)

3. Attacks

- Original
- Wavelet compr 94%
- Crumple & scan

Composition of wavelet compressed house and warped bear

Fall 2008, Mohamad Eid ELG 5121/CSI7631-43