Multimedia Security: So What’s the Big Deal?

Edward J. Delp

Purdue University
School of Electrical and Computer Engineering
Video and Image Processing Laboratory (VIPER)
West Lafayette, Indiana

email: ace@ecn.purdue.edu
http://www.ece.purdue.edu/~ace
Multimedia Security

• “Everything” is digital these days - a copy of a digital media element is identical to the original
• How can an owner protect their content?
• Are images still “fossilized light”?
• What does all of this mean in terms of law?
  – What does it mean to own “bits”?
• Does any security system really work or does it just make us feel good!
What Do We Want From a Security System?

- Access Control
- Copy Control

- Auditing (fingerprinting)
  - Who did what and when?

Playback Control
Record Control
Generation Control
What Do Users Want?

• Time-shifting
• Format-shifting
• Single copy (back ups?)

If you do not like the owner of the content or disagree with the way it is distributed, should you steal it?
Digital Millennium Copyright Act

- Will it be illegal to remove security features from a data element?
- Will reverse engineering still be legal?
- What constitutes distribution?
  - Can I give a data element to my 10,000 closest friends?

http://lcweb.loc.gov/copyright/
Digital Communication System

- Digital Information Source
- Source Encoder
- Encrypt
- Channel Encoder
- Channel
- User
- Source Decoder
- Decrypt
- Channel Decoder
Typical Cryptography System: Trusted Users
Cryptography System: User Not Trusted

Source -> Insecure Channel -> User

Authentication
Media Elements

- Audio
- Video
- Documents (including HTML documents)
- Images
- Graphics
- Graphic or Scene Models
- Programs (executable code)
Multimedia Security - Tools Set

• Encryption

• Authentication

• Hashing

• Time-stamping

• Watermarking
Multimedia Security Applications

- Privacy
- Forgery Detection ⇒ watermarking
- Copyright Protection ⇒ watermarking
- Proof of Purchase (non-deniable)
- Proof of Delivery (non-deniable)
- Intruder Detection

How do you do this over a noisy wireless channel?
What is Watermarking?

• The use of perceptually invisible authentication techniques
  – “controlled” distortion is introduced in a multimedia element
• Visible watermarks also exists
Watermarking Scenario

• Scenario
  – an owner places digital images on a network server and wants to “protect” the images

• Goals
  – verify the owner of a digital image
  – detect forgeries of an original image
  – identify illegal copies of the image
  – prevent unauthorized distribution
Where are Watermarks Used?

- Watermarks have been used or proposed in:
  - digital cameras
  - DVD video
  - audio (SDMI $\Leftarrow$ dead on arrival)
  - broadcast video (in US - ATSC)
    - visible watermarks now used
      - metadata “binding” mechanism
      - key distribution systems
      - preventing forgery of bank notes
      - digital cinema
      - “analog hole”
Steganography

Steganography - *(covered writing)* techniques used to hide information within other information to conceal the very existence of the message

Used much longer than cryptography

Different than cryptography in that an illegal user may intercept the message
Watermarking

• The use of perceptually invisible authentication techniques is one form of watermarking
  – distortion is introduced in the data
• Other forms include visible watermarks
A Review of Watermarking Techniques

- Spatial watermarking
- Sub-band (wavelet) watermarking
- DCT coefficient modulation
- Visible watermarks
Components of a Watermarking Technique

• The watermark, W
  – each owner has a unique watermark

• The marking algorithm
  – incorporates the watermark into the image

• Verification algorithm
  – an authentication procedure (determines the integrity / ownership of the image)
Watermark Detection

- The tradeoff of detectability vs. visibility (host signal interference)
- Do you need the original image for detection?
  - If not ⇒ blind detection

- What about the “key?”
  - private or public?
- These are very important when with video
Main Principles

• Transparency - the watermark is not visible in the image under typical viewing conditions

• Robustness to attacks - the watermark can still be detected after the image has undergone linear and/or nonlinear operations (this may not be a good property - fragile watermarks)

• Capacity - the technique is capable of allowing multiple watermarks to be inserted into the image with each watermark being independently verifiable
Fragile Watermarks

- Changes to image easily detected and localized
- Used for authentication, rather than copy detection
Attacks

- Compression
- Filtering
- Printing and rescanning
- Geometric attacks - cropping, resampling, rotation
- Collusion - spatial and temporal
- Conversion to analog
Spread Spectrum
DCT Watermark

• $W$ is a sequence of random numbers
  – bipolar binary sequence, or $N(0,1)$
• $X_D$ and $Y_D$ are DCT of $X$ and $Y$
• $a = $ scaling factor:

$$Y_D(i) = X_D(i)(1 + aW)$$
DCT Watermark

• $W^*$ is the extracted version of the watermark
• Verification:

$$S(W, W^*) = \frac{W \cdot W^*}{\sqrt{W^* \cdot W^*}}$$

• $T = \text{user-defined threshold}$
• If $S > T$, image is authentic
Fixed-length DCT Watermark

\[ a = 0.1 \]
Fixed-length DCT Watermark

\[ a = 0.5 \]
Fixed-length DCT Watermark

\[ a = 1.0 \]
Fixed-length DCT Watermark

\[ a = 5.0 \]
Digital Image Steganography

- Example cover and stego images produced by S-Tools 4.0
  - Message: This is a test message demonstrating the S-Tools 4.0 steganography software.
  - Stego key: STEGO

Cover Image (8 bits/pixel)  Stego Image (8 bits/pixel)
Purdue Research Efforts

- Robust Image-Adaptive Watermarks
- Fragile and Semi-Fragile Watermarks for Forensic Imaging
- Robust Video Watermarking
- Digital Cinema
- Watermark Evaluation
- Document Protection and Forensic Analysis
- Error resilient cryptography
- Security in Consumer Electronic Devices and Home Networks
Image Adaptive Watermarks (DCT)
Image Adaptive Watermarks (DCT)
Image Adaptive Watermarks (DCT)
VW2D Difference Image
Results - Girls

← Original “Girls”

Altered “Girls” →
Watermark Embedding Protocol

- **Input Frame** $X(t)$
- **Watermark Generator**

  - Watermark $W(t)$

  - Watermark Key for Next Frame $K(t+1)$

- **Embed**

- **Frame Analyzer**

  - Feature Values

- **Temporal Redundancy Control**

- **Finite State Machine**

- **Watermarked Frame** $Y(t)$
Watermark Detection Protocol

Test Picture $Z(t)$

Watermark Detector

Frame Analyzer

Watermark Generator

Memory (Queue)

State, Key

UT March 21, 2003 Slide 40
Conclusions

• The “secure” multimedia system is evolving
• Simple add-ons will not work (not like the text-based systems)
• Exploit the unique nature of the type of data
• Digital watermarking may be crucial to secure networked multimedia systems
• Time stamping is important
• New techniques tolerate changes to images, and are compatible with compression
Conclusions

• Watermarking is still an interesting research area with many interesting problems
  – where will it be useful?
  – will watermarking only be used a second-tier security system?
  – will there be significant theoretical developments?

• Is watermarking the “feel good” technology of multimedia?