ENEE408G Lecture-9

Digital Watermarking and Fingerprinting for Digital Rights Protection of Multimedia

- *URL: http://www.ece.umd.edu/class/enee408g/*
- *Slides included here are based on Spring 2012 offering in the order of introduction, image, video, speech, and audio. © Copyrighted 2002-2012.*
- *ENEE408G course was developed @ ECE Department, University of Maryland, College Park. Inquiries can be addressed to Profs. Ray Liu (kjrliu@isr.umd.edu) and Min Wu (minwu@eng.umd.edu).*

Last Lecture

- Audio synthesis: MIDI
- Digital Audio Coding/Compression
  - Psychoacoustics properties used in perceptual audio coding
  - MPEG-1 Audio coding
- Today:
  - Digital Rights Management of Multimedia via "Watermarking"

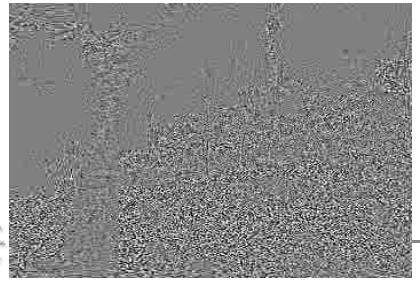
Demands on Info. Security and Protection

- Intellectual property management for digital media
  - Promising electronic marketplace for digital music and movies
  - Advantages of digital: perfect reproduction, easy transmission, …
  - Napster controversy
- Conventional encryption alone still leaves many problems unsolved
  - Protection from encryption vanishes once data is decrypted
    - *Still want establish ownership and restrict illegal re-distributions*
  - How to distinguish changes introduced by compression vs. malicious tampering?
    - *Bit-by-bit accuracy is not always desired authenticity criterion for MM*

Digital Watermarking/Data Hiding in Multimedia

- What is Digital Watermarking?
  - Examples: *Picture in picture, words in words*
    Silent message, invisible images
  - Secondary information in perceptual digital media data
- The need of watermarking: robust vs. fragile
  - Copyright protection: prove the ownership
  - Fingerprinting: trace the source
  - Copy protection: prevent illegal copying
  - Data authentication: check authenticity of data
    - *Fragile or semi-fragile watermarking*

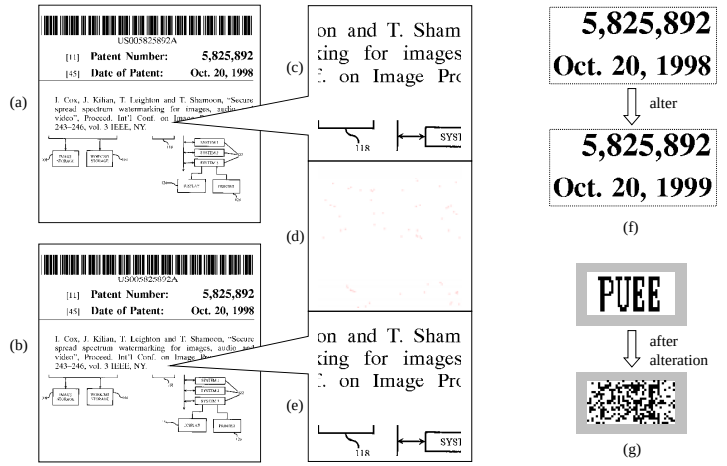
Example on Invisible and Robust Watermark



10011010 …

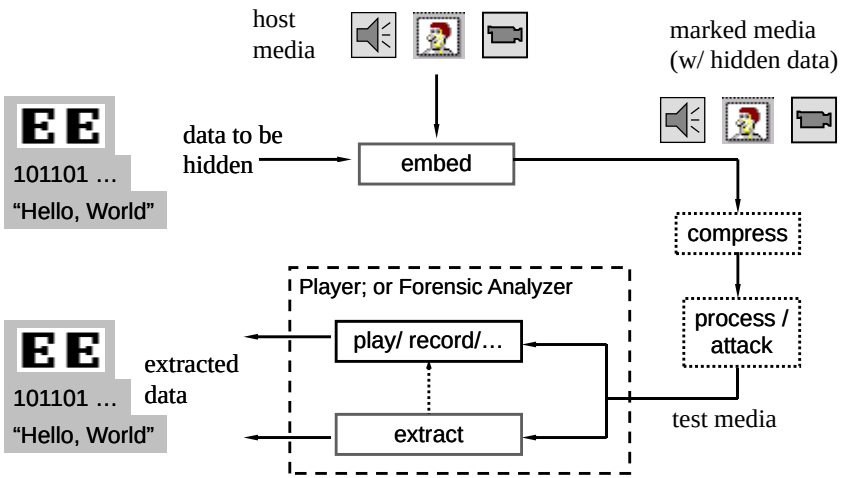
© Copyright …

Fragile Watermark Example: Document Authentication



- *Embed pre-determined pattern or content features beforehand*
- *Verify hidden data's integrity to decide on authenticity*

General Framework of Data Hiding



Basic Requirements for (Robust) Watermarking

- Imperceptibility (perceptual transparency)
- Payload
  - the amount of information that can be stored in a watermark
- Robustness
- Security – Kerckhoff Principle
  - The method used to encrypt the data is known to an unauthorized party and that the security must lie in the choice of a key.
- Blind and non-blind detection (aka Oblivious vs Non-oblivious)
  - Blind detection ~ does not use the original unmarked copy

Data Embedding by Replacing LSBs

Replace LSB with Pentagon's MSB

Data Embedding by Replacing LSBs (cont'd)

Replace 6 LSBs with Pentagon's 6 MSBs

=> See Lab Project 4 for details

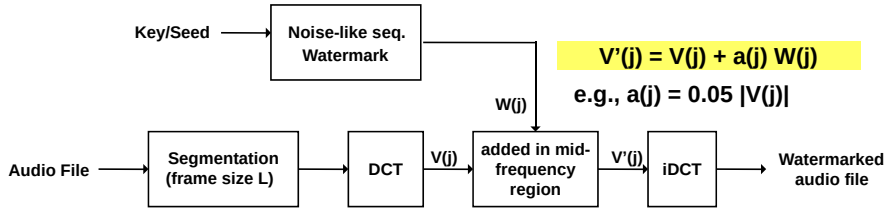
A Simple Audio Watermark in Time Domain

- Put message in the Least-Significant-Bits (LSBs)
  - Encode a message into bits
    - *e.g., represent a character string into bits using ASCII code*
  - Embedder puts in LSBs of audio samples
    - *Repeat embedding the same bit in a few samples if needed*
  - Detector retrieves embedded bits from LSBs
    - *Perform majority voting if repeated embedding is used*
  - Repack bits into message
- Tradeoff between perceptual quality and robustness
  - Compare the embedding in 1st LSBs, 2nd LSBs, …
- Security
  - Can they see/hear your message?
  - Can other people make imperceptible change to alter your message?

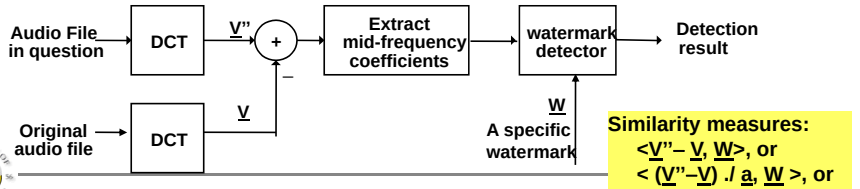
=> See Design Project 4 for details

A More Robust Watermark in Transform Domain

- Embedder: *use HAS & embed in perceptually significant freq.*



- Detector: determine the existence of a specific wmk
  - Subtract host signal, measure similarity (via correlation), & threshold it

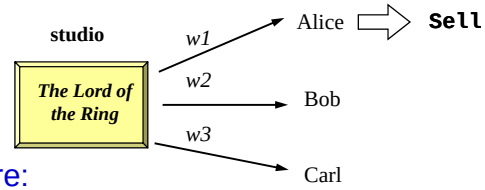


Discussions

- Why use noise-like sequence as watermark?
  - Imperceptibility
  - Confidentiality of the embedded data
  - Robustness against jamming
- Imperceptibility
  - Frequency domain embedding: can take advantage of known perceptual properties such as masking
  - Can apply sophisticated HAS models to improve perceptual quality
- Robustness and security
  - Use "attacks" to find weaknesses and improve designs
  - Case study: SDMI public challenge (Fall'00)

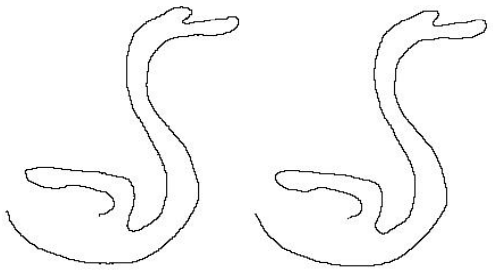
Digital Fingerprinting and Tracing Traitors

- Leak of information poses serious threats to government operations and commercial markets
  - e.g., pirated content or classified document



- Promising countermeasure: robustly embed digital fingerprints
  - Insert ID or "fingerprint" (often through robust watermarking) to identify each user
  - Purpose: deter information leakage; digital rights management
    - *provide post-delivery protection complementary to encryption*
  - Challenge: imperceptibility, robustness, tracing capability

Fingerprinting Curves

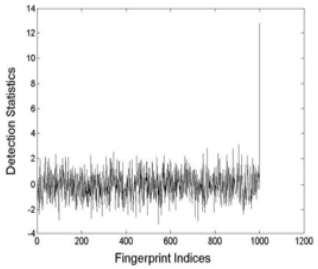


Original Curve

(captured by TabletPC)

Fingerprinted Curve

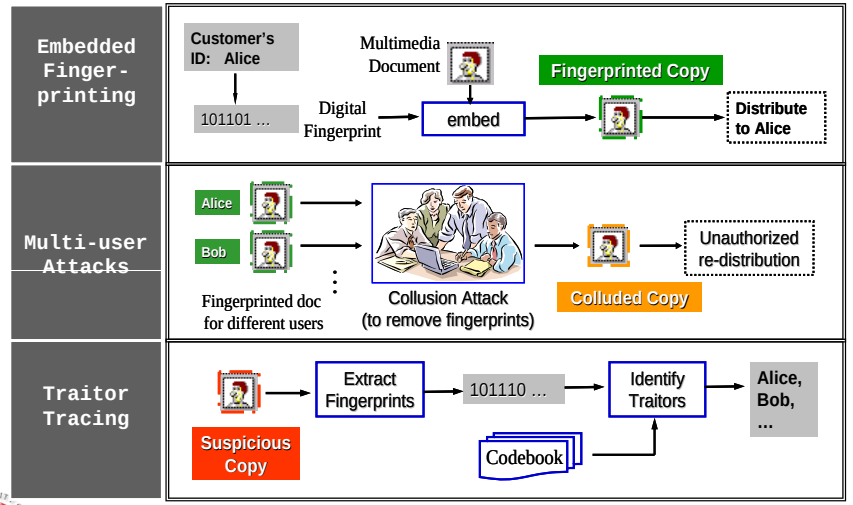
(100 control points)



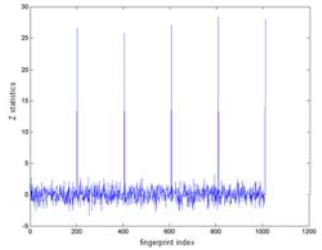
Detection Statistics

Typical threshold is 3~6 for false alarm of 10^{-3} ~ 10^{-9}

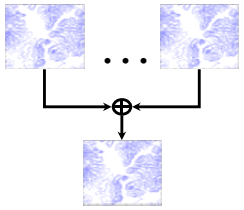
Embedded Fingerprinting for Multimedia

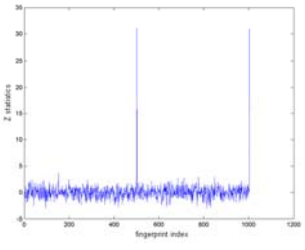


Collusion-Resistant Fingerprinting of Maps

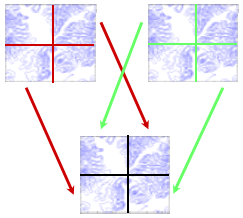


5-User Averaging Attack





2-User Interleaving Attack



- Also survive combination attacks of collusion + print + scan

Example of Anti-Collusion Fingerprint Code:

Embed 16-bit Code for Detecting ≤3 Colluders Out of 20

User-1 **(-1,-1, -1, -1, 1, 1, 1, 1, …, 1)**

(-1, 1, 1, 1, 1, 1, …, -1, 1, 1, 1) *User-4*

Embed fingerprint via HVS-based spread spectrum embedding in block-DCT domain

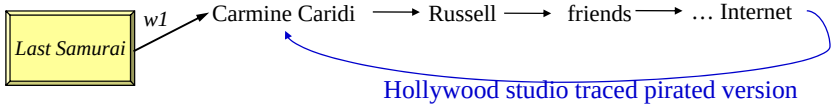
Collude by Averaging

Uniquely Identify User 1 & 4

Extracted fingerprint code **(-1, 0, 0, 0, 1, …, 0, 0, 0, 1, 1, 1)**

Case Study: Tracing Movie Screening Copies

- Potential civilian use for digital rights management (DRM)
  - *Copyright industry – $500+ Billion business ~ 5% U.S. GDP*
- Alleged Movie Pirate Arrested (23 January 2004)
  - A real case of a successful deployment of 'traitor-tracing' mechanism in the digital realm
  - Use invisible fingerprints to protect screener copies of pre-release movies



http://www.msnbc.msn.com/id/4037016/

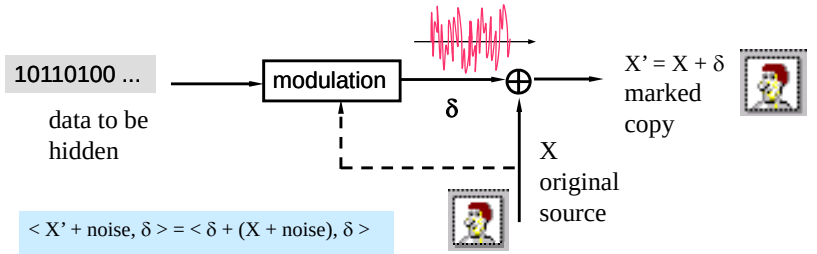
Summary

- Multimedia watermarking for rights management
- Reading Assignment
  - F. Hartung and M. Kutter: “Multimedia Watermarking Techniques”, Proc. of the IEEE, pp.1079-1107, July 1999.
  - M. Wu and B. Liu, “Multimedia Data Hiding”, Chapter 10 on SDMI audio watermark challenge, preprint, 2002 (electronic handout).
  - M. Wu, W. Trappe, Z. Wang, and K.J.R. Liu: "Collusion Resistant Fingerprinting for Multimedia", IEEE Signal Processing Magazine, Special Issue on Digital Rights Management, pp.15-27, March 2004. http://www.ece.umd.edu/~minwu/public_paper/Jnl/0403FPcollusion_IEEEfinal_SPM.pdf
- This week’s Lab session:
  - Continue on audio project

For Further Explorations:
General Formulation of Two Types of Watermarking

To Explore Further: Type-I Additive Embedding

- Add secondary signal in host media
- Representative: spread spectrum embedding
  - Add a noise-like signal and detection via correlation
  - Good tradeoff between imperceptibility and robustness
  - Limited capacity: host signal often appears as major interferer

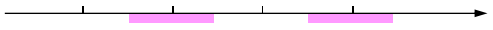


$< X' + \text{noise}, \delta > = < \delta + (X + \text{noise}), \delta >$

$< X' + \text{noise} - X, \delta > = < \delta + \text{noise}, \delta >$

Type-II Relationship Enforcement Embedding

- Deterministically enforcing relationship
  - Secondary information carried solely in watermarked signal



feature value	2kQ	(2k+1)Q	(2k+2)Q	(2k+3)Q
odd-even mapping	0	1	0	1

- Representative: odd-even embedding

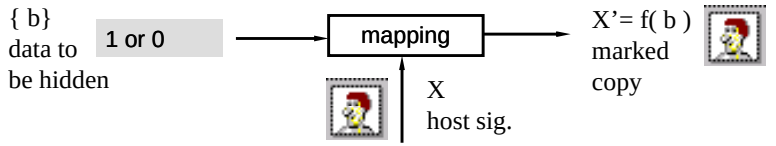
```
even "0"
odd  "1"
```

  - No need to know host signal (no host interference)
  - High capacity but limited robustness
  - Robustness achieved by quantization or tolerance zone

E.g. enforcing black pixel# per block to odd/even to hide data in binary image

Type-II Relationship Enforcement (cont'd)

- General approach:
  - Partition host signal space into sub-regions
    - *each region is labeled with 0 or 1*
    - *marked sig. is from a region close to orig. & labeled w/ the bit to hide*
  - Secondary info. carried solely in **X'**
    - *difference (X'-X) doesn't necessarily reflect the embedded data*



- Advanced embedding:
  - Combining the two types with techniques suggested by info. theory