Exposing Traitors: Traitor Tracing, Watermarks and DRM

Abram Hindle

CSC482A/582B

University Of Victoria

abez@cs.uvic.ca

December 22, 2003

This Presentation

- What am I going to cover?
  - Introduction to Digital Rights Management
  - Introduction to Watermarking
  - Introduction to Traitor Tracing
  - Examples of Traitor Tracing
  - Current Research on Traitor Tracing
  - Summary

Introduction

- What is DRM?
  - Digital Rights Management
  - Protections related to retaining copyright information on media
  - Prevention of duplication of media.
  - Restrictions and Licensing of the use of digital media.
  - Possibly benefit both consumer and producer
  - Currently Favors producer heavily

Problems

- What are the issues facing DRM?
  - Resolving Copyright Holders
  - Licensing
  - Integrating P2P and Micropayments
  - Enabling users to share media while maintaining the licensing.
  - Distributed License Keys vs Centralized
  - Online realtime vs Offline deffered

Problems

- What are the issues facing DRM?
  - Fair Use
  - Restricts Consumers
  - False Positives
  - Losing Control over Damaged Data
  - Analog Hole

Watermarks

- What is a watermark?
  - A watermark is a mark that is
    - (i) embedded into an artifact (text, image, video, audio) or piece of intellectual property (hardware, software, algorithm, data organization),
    - (ii) designed to identify the author, the source, the used tools and techniques and/or recipient of the artifact or the intellectual property, and
    - (iii) difficult to detect and remove.
  - [KLMS+98]

Watermarks

- What is a watermark?
  - Classically it is used to mark offical documents. Certify the authority behind a document.
  - Used on cheques.
  - Signing a digital document (image, audio, text). ..
  - Used to infer ownership.
  - Used as protection of copyright by deterrance and the ability to prove author
  - Watermarks can be used to determine if media has been altered signifigantly beyond filters and compression.

Watermarks

- Where are watermarks used?
  - Motion Pictures
  - Images on the web
  - P2P audio
  - Movie Screeners
  - VLSI Chips and Design
  - Optimization constraints [KLMS+98]

Watermarks

- What are general issues with watermarking
  - Correctly identifying author
  - Watermark detection vs Watermark extraction
  - Quality loss
  - Protection against transformation
  - Are watermarks already in the media or do we add it?
  - Are watermarks detectable?
  - Who needs to look for the watermark.
  - Deadlock [Kwo03]

Watermarks

- How are watermarks done in images?
  - Aesthetically unimportant parts of the images are altered. Shades in colors, areas of blank space or noise are used to embed watermarks to avoid visual quality loss.
  - Addition of watermarks effectively reduces quality of images.
  - In some cases, the lower frequencies in a DCT of an image block are manipulated s.t. the watermark will survive compression
  - Sometimes lower order bits are manipulated to create a water mark. [Ber97]
  - Subtle or light overlay of a traditional watermark. [Ber97]

Watermarks

- This is an Algorithm presented in “Secure Distribution of Watermarked Images for a Digital Library of Ancient Paper”:
- – Watermark key is generated and used in a Reed Solomon Error Control code.
  - Each symbol is encoded into a random signal vector.
  - These vectors are added to the DCT coeffecient of the image from 8x8 blocks of the image. This is best done during JPEG compression. [RRP97]
  - Thus this technique withstands JPEG compression very well as the low frequencies are manipulated (which are the frequencies saved by JPEG compression).

Watermarks

- What are the difficulties in watermarking images?
  - Protecting against, distortion, rescaling, color shift, perspective, compression, alteration. [TH00]
  - What if someone adds another watermark to the file?
  - For images used for analysis, such as satellite imagery, watermarks can provide too much distortion thus skewing mathematical analysis [HY03].

Watermarks

- How are watermarks done in audio?
  - Embedded in parts of audio that will still be compressed but not necessarily heard.
  - Addition of watermarks effectively reduces quality of audio.
  - Sometimes frequency domain modifications, sometimes amplitude.

Watermarks

- The paper “Digital Watermarks for Audio Signals” describes how add watermarks to audio [BTH96]
  - Test the current compression scheme for the masking it uses. We’ll generate the watermark within its mask.
  - Per block, adapt the water mark to match the source audio
  - Watermark is encoded as audio and added to signal
  - Watermark might have to be amplified to be reencoded safely.

Watermarks

- What are the difficulties in watermarking audio?
  - Lossy compression throws away non-aesthically necessary parts of audio (thus probably the watermark)
  - Difficult to survive transformations.
  - Speed of compression, if we watermark every unique download.

Traitors

- What is a traitor?
  - A traitor is an authenticated user who colludes with a 3rd party in order to subvert the security of a system.

Traitors

- What are some example of traitors
  - A subscriber to a website who gives away their user login.
  - A satelitte tv subscriber who shares their keys.
  - A user who buys music then distributes it over p2p .
  - A movie critic who copies a movie screener.
  - A pay per view subscriber who shares their keys.

Traitor Tracing

- What is Traitor Tracing
  - Using signatures and watermarks we attempt to deduce the orignal traitor or traitors who were responsible in collusion.
  - Collusion of users to destroy fingerprints/watermarks by comparing differences.

Traitor Tracing

- Example
  - We watermark an mp3 with a different watermark per each transaction with a user. So each user gets a unique mp3 of the same song. When we find an instance of our mp3 on a P2P network we can check it for watermarks. If any of the watermarks we retrieve match the watermarks we assigned users, we will be able to determine who the original traitor of the program was.

Traitor Tracing

- Can we retrieve a list of all the traitors?
  - In cases of broadcast and key collusion yes.
  - Research has been done on how to determine the colluding traitors for satellite TV keys. Satellite TV signal keys are usually shared by small groups of subscribers (4 or more). [Poo99]
  - In cases where users collude to destroy watermarks we can attempt to derive the watermarks of all the colluding users [BS95]

Traitor Tracing

- How does Traitor Tracing relate to cryptography?
  - in the case of tracing the keys that were used in collusion.
  - Key tracing
  - Broadcast keys
  - Hiding of watermarks
  - Signing media
  - Encoding watermarks in such away that colluding users are identified (error correction codes help)

Traitor Tracing

- Directions of Research taken and being taken in Traitor Tracing
  - Fingerprinting Digital Data
  - Protecting against Collusion
  - More optimal traitor tracing algorithms
  - Linear and Bilinear traitor tracing
  - Traitor tracing for broadcast messages

Summary

- DRM will always suffer from the fact that the end user eventually has to be trusted to use the DRM protected media.
- DRM seems less for copyright protection and more for changing users expectations of digital media
- “The main purpose of DRM is not to prevent copyright infringement but to change consumer expectations about what they are entitled to do with digital content.” [Sam03]
- Watermarks can be used to determine copyright owners as well as purchaser.
- Watermarks can be fragile or robust.
- Watermarks don’t restrict the user but provide a detterance against collusion.
- Traitor Tracing admits that most DRM schemes will be circumvented but those responsible can still be discovered.

References

[Ber97] Hal Berghel. Watermarking cyberspace. *Commun. ACM*, 40(11):19–24, 1997.

[BS95] Dan Boneh and James Shaw. Collusion-secure fingerprinting for digital data. *Lecture Notes in Computer Science*, 963:452–??, 1995.

[BTH96] Laurence Boney, Ahmed H. Tewfik, and Khaled N. Hamdy. Digital watermarks for audio signals. In *International Conference on Multimedia Computing and Systems*, pages 473–480, 1996.

[HY03] Gregory L. Heileman and Yunlong Yang. The effects of invisible watermarking on satellite image classification. In *Proceedings of the 2003 ACM workshop on Digital rights management*, pages 120–132. ACM Press, 2003.

[KLMS+98] Andrew B. Kahng, John Lach, William H. Mangione-Smith, Stefanus

Mantik, Igor L. Markov, Miodrag Potkonjak, Paul Tucker, Huijuan Wang, and Gregory Wolfe. Watermarking techniques for intellectual property protection. In *Design Automation Conference*, pages 776–781, 1998.

[Kwo03] Sai Ho Kwok. Watermark-based copyright protection system security. *Commun. ACM*, 46(10):98–101, 2003.

[Poo99] J.S. Poovendran, R.; Baras. Optimal scalable security architectures in the presence of colluding mobile traitors. In *Wireless Communications and Systems, 1999 Emerging Technologies Symposium, Vol.*, pages 18.1–18.5. IEEE, 1999.

[RRP97] Christian Rauber, Joe Ruanaidh, and Thierry Pun. Secure distribution of watermarked images for a digital library of ancient papers. In *Proceedings of the second ACM international conference on Digital libraries*, pages 123–130. ACM Press, 1997.

[Sam03] Pamela Samuelson. Drm and, or, vs. the law. *Commun. ACM*,

46(4):41–45, 2003.

[TH00] Andrew Z. Tirkel and Tom E. Hall. Watermarking at point of origin. In *Proceedings of the 2000 ACM workshops on Multimedia*, pages 135–138. ACM Press, 2000.