Digital Watermarking and Steganography

by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker

Chapter 1. Introduction

Lecturer: Jin HUANG

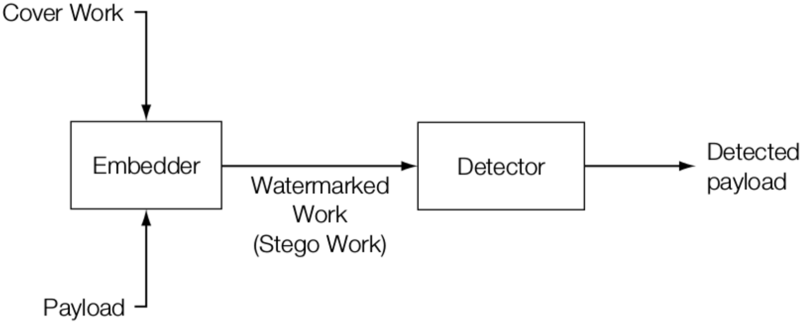
2015

Message and Work

Relationship between the message and the work:

- Watermark: imperceptible message about the work.
  - image on cash.
  - signature in video.
- Steganology: undetectable and secret message in the work.
  - text written by milk.
  - text on the head of a slaver.

System overview



Payload: watermark or secret message.

Why Digital Watermarking?

Contents

- image, video
- 3D model
- executable code
- integrated circuits

Applications

- copyright
- no copy
- check modification
- monitor usage

Why Steganology?

Terrorist, criminal activity, spy or rival in love.

Least Significant Bit embedding in

- BMP, GIF
- JPEG
- Audio
- Multimedia

Information Hiding

A general term. Hiding means

- making the information imperceptible.
- OR keeping the existence of the information secret.
- STG (Steganology): secret.
- WM: Watermarking: imperceptible.

Four categories of information hiding

	Cover Work **Dependent**	Cover Work **Independent**
Existence **Hidden**	Covert Watermarking	Steganology
Existence **Known**	Overt Watermarking	Overt Embedded Communications

Covert Watermarking

Tracking the source leak in photographic reprints (1981, confidential British cabinet):

- Cover work: Copy of document to the minister.
- Information: Each copy had a different word spacing that was used to encode the identity of the recipient.

Other example? Leading words in a poem.

Steganology

Additional information from the sensors about SALT-II treaty between the United States and the Soviet Union:

- Cover work: tell the other country whether or not its silo was occupied, but nothing else.
- Information: communicate additional information, such as the location of its silo, hidden inside the legitimate message.

Overt Watermarking

The web site of the Hermitage Museum in St. Petersburg, Russia.

- Cover work: Digital copies of its famous collection.
- Information: watermarked to identify the Hermitage as its owner, and a message on each web page indicates this fact, along with the warning that the images may not be reproduced.

Why overt? Helps deter piracy.

Other example? Cash!

Overt Embedded Communications

Transmission of auxiliary, hidden information that is unrelated to the signal in which it is embedded.

- Cover work: Radio.
- Information: Time code in the broadcast at a specified frequency.

History

Lots of interesting stories there.

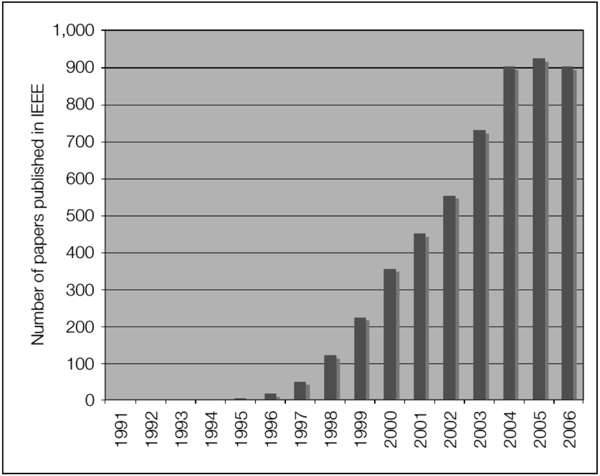


FIGURE 1.3

Annual number of papers published on watermarking and steganography by the IEEE.

Importance

- Watermarking
  - Copy prevention and copy-right protection.
  - Why not cryptography? it can protect content in transit, but once decrypted, the content has no further protection.
  - ...
- Steganology
  - Terrorists
  - Crime
  - Political

Project: Basic Content Manipulation

IO and “display”:

- Image
- Audio
- Video

Digital Watermarking and Steganography

by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker

Chapter 2. Applications and Properties

Lecturer: Jin HUANG

2015

Overview

Good solution is always a nice integrating of

- Technique features/performance.
- Application requirements

We will introduce:

- The features/performance of watermarking and steganography.
- Integrating to various applications.

Features/performance of watermarking

- Features: Compare to other descriptors (e.g. bar code, meta info etc.).
  - Imperceptible.
  - Inseparable.
  - Transform along with the work.
- Performance: Importance depends on the application.
  - Robustness: how well watermarks survives.
  - Fidelity: how imperceptible the watermarks are.
  - ...

Features/performance of steganography

- Features: Compare to encryption.
    - Hiding the presence/communicating
- Performance: The balance depends on the application.
    - Statistical undetectability: how difficult it is to detect the existence.
    - Steganographic capacity: the maximum payload without causing statistically detectable artifacts.
    - ...

2.1 Applications of Watermarking

Watermarking: Broadcast Monitoring

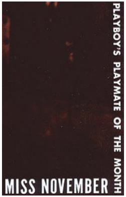
I payed to many media for my advertisement.
Have they been properly broadcast?

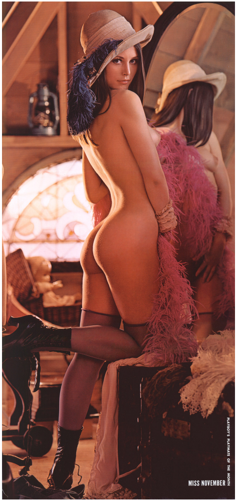
- Human observer: costly and error prone.
- Passive monitoring
  - signal → **signature** → database **search**
  - High cost and low accuracy.
- Active monitoring
  - Encoded in imperceptible channel (the vertical blanking interval (VBI) of a video signal).
  - Channel disappear, format change, ...

Watermarking: Owner Identification

Who made this?

- Explicit copyright notices
    - Ugly and cover the work
    - Easy to remove
- Watermarking
    - Imperceptible
    - Inseparable





Lena from Playboy

Watermarking: Proof of Ownership

How to claim that it is made by me?

- Explicit copyright notices: can be forged.
- Central repository: costly.
- Keeping origin: can be forged.

Watermarking

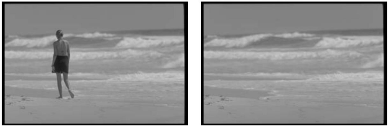
- Not removable: no public detector.
  - But one can add more watermarks.
  - Countering ambiguity attacks (Chapter 10).

Watermarking: Transaction Tracking

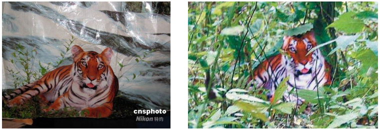
Who/How the work is leaked/pirated?

- Each media player (DiVX) places a unique watermark into every media it played.
- Movie dailies in film industry.
- In 2004, the 70-year-old actor, Carmine Caridi, was caught for leaking movie in Oscar Awards.

Watermarking: Content Authentication 1



Which one is true?



Tiger ZHOU?

Tamper detection.

Using authentication mark, a **fragile** watermark

- Digital signature via asymmetric encryption.
- In digital cameras (e.g. Epson).
- Embed the signature directly into the work.

Watermarking: Content Authentication 2

Embedding is also a “tamper”.

Separating the work into two parts:

- one for which the signature is computed.
- one into which the signature is embedded.

How the work has been tampered with?

- Localized authentication: Which parts have been modified (e.g. license plate on a car).
- Semi-fragile watermark: compression is OK, but invalidated by major changes.

Watermarking: Copy Control 1

Prevent people from making illegal copies of copyrighted content.

Encryption?

- Content must be decrypted before using, and once decrypted, all protection is lost.
- Digital → Analog → Re-digitization.

Watermarking: Copy Control 2

Record control

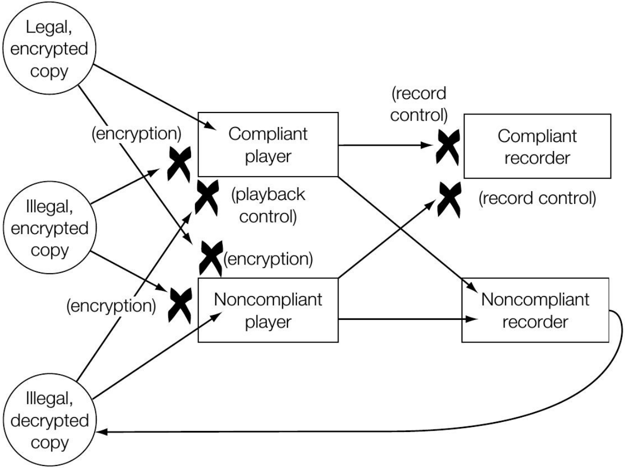
- Prohibit recording whenever a never-copy watermark is detected at its input.
- In every recording device.
  - Reduces the value of the recorder.
  - By law? EVERY country in the world?

Patent-license approach for DVD players and recorders producers:

- To play CSS-encrypted disks → must include watermark detectors.

Watermarking: Copy Control 3

Noncompliant device: Neither watermark detection nor CSS decryption.



Watermarking: Copy Control 4

Playback control Compliant player shuts down if the input

- Not encrypted AND has never-copy watermark.
    - Play via compliant player and record via non-compliant recorder.
- Encrypted but has no lead-in area containing the key to decrypt.
    - Bit-for-bit copy from non-compliant recorder. Lead-in area is only read by compliant player.

Presentation: DVD Authoring and Production

References:

- “DVD Authoring and Production: An Authoritative Guide to DVD-Video, DVD-ROM”, Ralph LaBarge.
- “Encrypted data signal, data storage medium, data signal playback apparatus, and data signal recording apparatus”, US 20020015494 A1.
- “Watermarking in the Real World: An Application to DVD”, Matt L. Miller, Ingemar J. Cox, and Jeffrey A Bloom.
- ...