Digital Watermarking and Steganography

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

Chapter 1. Introduction

Lecturer: Jin HUANG

Message and Work

Relationship between the message and the work:

水印 每个人都能看出来

- Watermark: imperceptible message about the work.

  信息和work强相关

  - image on cash.
  - signature in video.

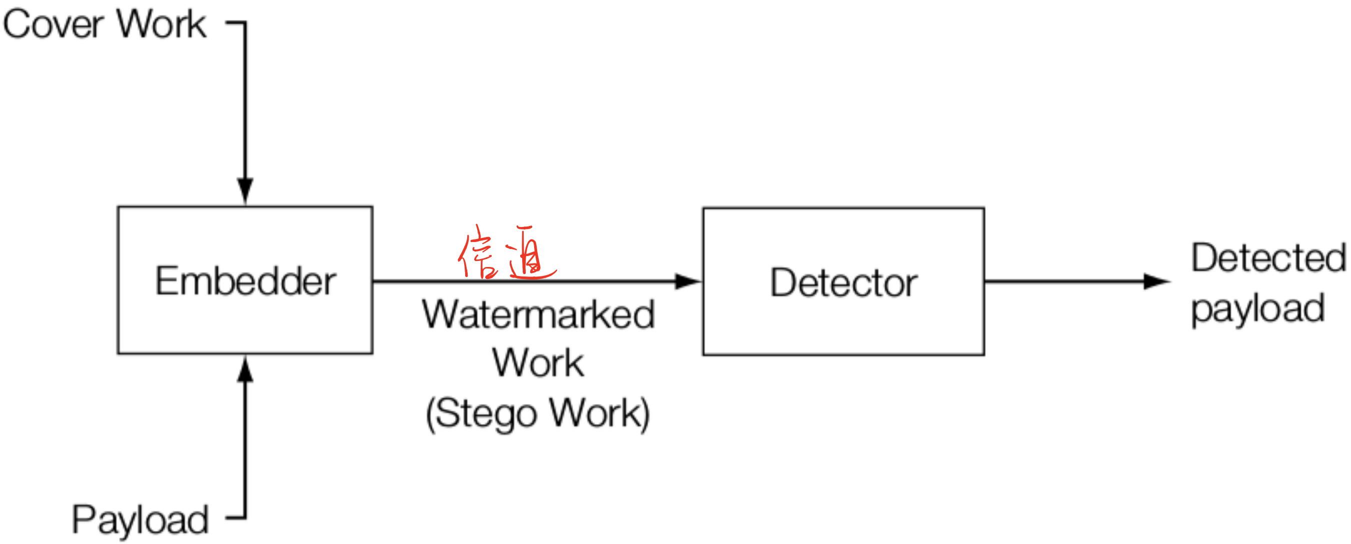
隐写 不可检测出来

- Steganology: undetectable and secret message in the work.

  信息和work不一定相关

  - text written by milk.
  - text on the head of a slaver.

System overview



Payload: watermark or secret message.

Why Digital Watermarking?

Contents (数字化)

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

Applications

- copyright 板权认证
- no copy 防拷贝
- check modification 防修改
- monitor usage 监控使用

Why Steganology?

Terrorist, criminal activity, spy.

Least Significant Bit embedding in

修改最后一位 (很难看出 undetectable)

- 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. ⇒ 机器
- WM: Watermarking: imperceptible. ⇒ 人

Four categories of information hiding

	Cover Work **Dependent**	Cover Work **Independent**
Existence **Hidden**	eg. 光盘刻录包含身份信息，藏头诗. Covert 英国内阁. Watermarking	Steganology
Existence **Known**	Overt Watermarking eg. 浙江大学印刷水印	Overt Embedded Communications eg. 收音机调时 Time Code

公开说明图片有水印
(艺术馆图片)

eg. 美苏导弹. 芯片传信息 (不同时间段左右偏移).

Covert Watermarking

monitor usage

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

内阁

- 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?

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.

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.

- If the words related to the 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.

在发送时间左右偏移传递更多信息.

- 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. 艺术馆高清图象打码.

- 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?

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?

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.

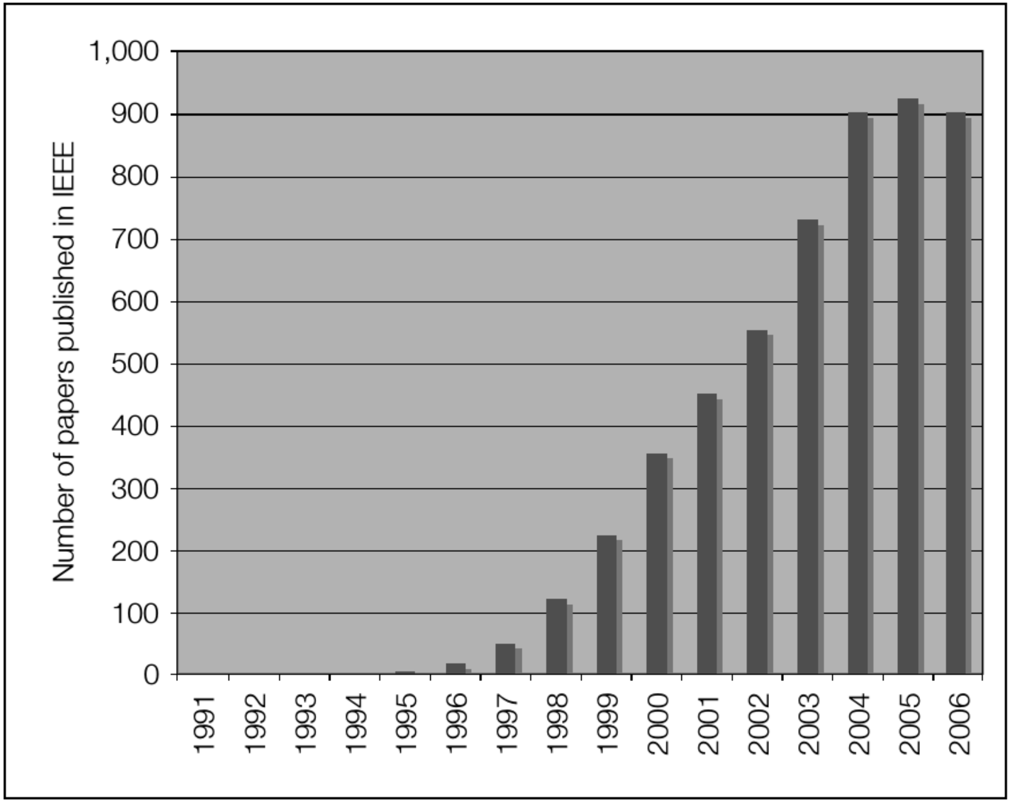


FIGURE 1.3

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

Importance

- Watermarking
  - Copy prevention and copy-right protection.
  - Why not cryptography?

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. 解密后可拿到原版.
  - ...
- 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

Overview

应用需求 $\overset{\text{融合}}{\Longleftrightarrow}$ 技术特性

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.

集成到应用

Features/performance of watermarking

条码

jpG 中扩展(拍摄时间，地点，光圈...)

- Features: Compare to other descriptors (e.g. bar code, meta info etc.).

  水印和条码，meta info 对比：必需和work不可轻易分离

  - Imperceptible. 分开 (无法轻易看到))
  - Inseparable. 不可分离
  - Transform along with the work.
- Performance: Importance depends on the application.
  - Robustness: how well watermarks survives. 图象压缩，裁剪后水印不消失
  - Fidelity: how imperceptible the watermarks are. 原图和加水印后的图无差别
  - ...

Features/performance of steganography

- Features: Compare to encryption.
  - Hiding the presence/communicating
- Performance: The balance depends on the application.

  不可检测性

  - Statistical undetectability: how difficult it is to detect the existence.

  传输信息多/次

  - Steganographic capacity: the maximum payload without causing statistically detectable artifacts.
  - ...

2.1 Applications of Watermarking

Watermarking: Broadcast Monitoring

监视

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, ... 降低码率

Watermarking: Owner Identification

Who made this?

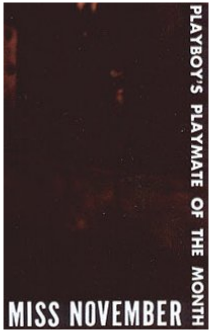
明确的

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

Watermarking: Owner Identification

Who made this?

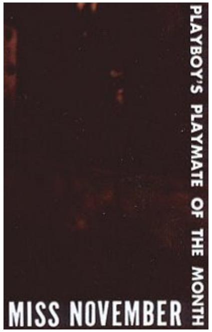
- Explicit copyright notices
  - Ugly and cover the work
  - Easy to remove
- Watermarking
  - Imperceptible
  - Inseparable



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.

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. 别人不能轻易移除
  - But one can add more watermarks. 不能轻易检测
  - Countering ambiguity attacks (Chapter 10). eg.公私钥

反击

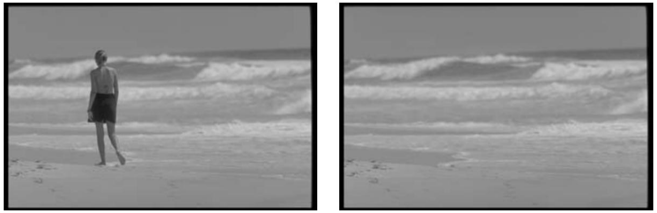
Watermarking: Transaction Tracking

盗版

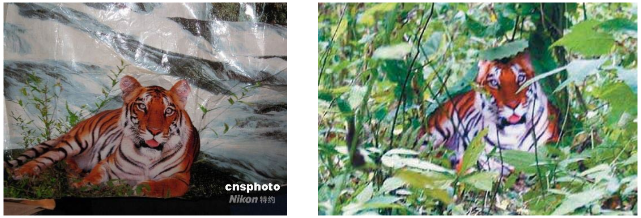
Who/How the work is leaked/pirated?

- 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



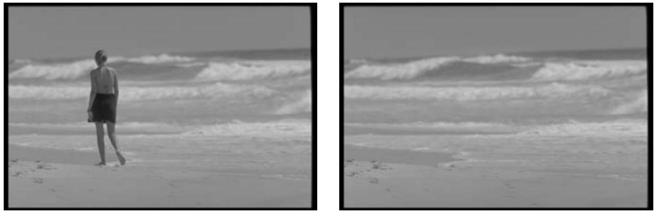
Which one is true?



Tiger ZHOU?

Tamper detection.

Watermarking: Content Authentication 1



Which one is true?

Tiger ZHOU?

Tamper detection.

脆弱

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.

篡改

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.

数字 模拟

Watermarking: Copy Control 2

Record control

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

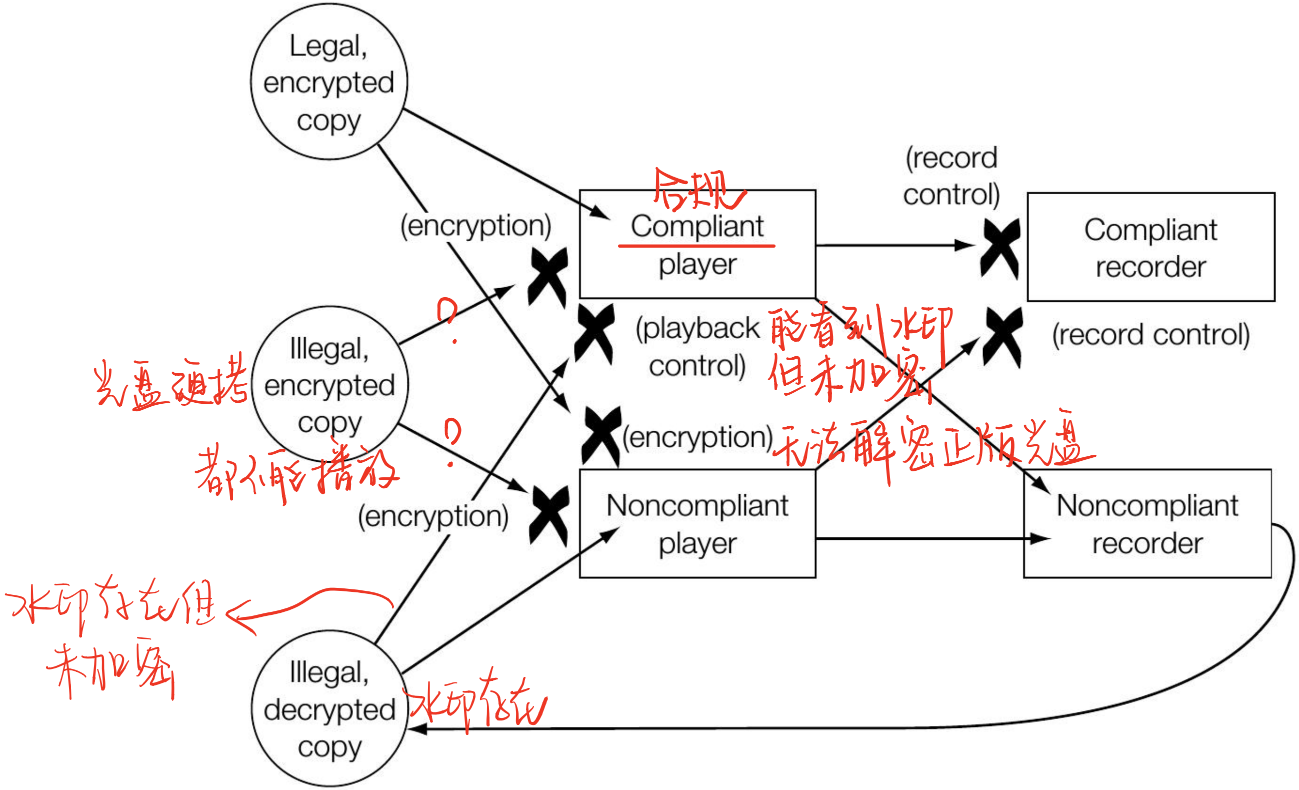
Patent-license approach for DVD players and recorders producers:

加密的光盘

- To play CSS-encrypted disks → must include watermark detectors. 解密的同时得要检测水印

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. 硬拷光盘无密钥
  - Bit-for-bit copy from non-compliant recorder. Lead-in area is only read by compliant player.

Challenges

From “Miller et al. Watermarking in the Real World:An Application to DVD, 1998”

- Enforcement: expense of owning two and law.
- System Tampering: watermark removing
  - better watermark algorithm 有办法去除水印
  - patent watermark removing algorithm
- Geometric distortion: robust watermarking
- Compression: watermark survive MPEG quantization
- False positive: no one can record the historical event!

水印
↓
破解水印
↓
申请专利

Presentation: DVD Authoring and Production

无法拷贝

- Why the PS/4 disk cannot be easily cloned by DVD burning?
  - What is the cover, and what is the message?
  - Introduce burst cutting area (BCA). 写入序列号，不能被刻录，是加密的.
- Counterfoil and printer

  票据

  - The rough idea of "Tartan Threads" (or paper "Information Hiding to Foil the Casual Counterfeiter")

    认出水印拒绝打印

①打印机认出票据拒绝打印

②事后追踪，打印机打印就上序列号.

- Influence of internet to such techniques.