杭州電子科技大学
HANGZHOU DIANZI UNIVERSITY

Lecture 1-2.

Information Hiding Technologies

Hui Wang

School of Cyberspace
Hangzhou Dianzi University

2018-2019 Academic Year – 2nd Semester
Febrary 2019

Session Contents

- **Lectures** on Steganography (will be learnt in week 1-3)
- **Lectures** on Digital Watermarking and its Applications (will be learnt in week 4-7)
- **Lectures** on Steganalysis and attacks on Digital watermarking (will be learnt in week 8-9)
- **Programming Practices** (will be learnt in week 10-15)
- **Exercises** (in week 16)

Session Objectives

By the end of the course, the student will have:

- A good knowledge with **Basic principles** of **data hiding**, and the difference between **Steganography** and **watermarking**
- **Applications** of different watermarking techniques used **with different media objects** (Stegeo-objects), such as video, audio and Circuitry
- Different **attacks** on digital watermarking and **benchmarks** used

Session Objectives

By the end of the course, the student will have:

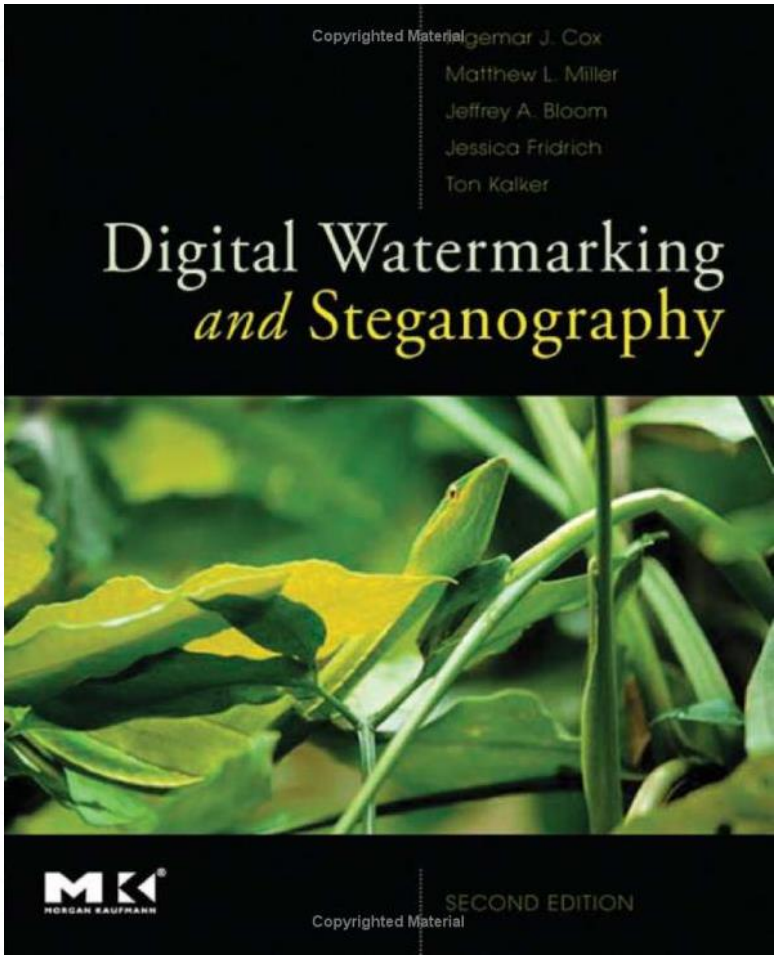
- Learn the basic mathematical concept behind watermarking theory (The prisoners Problem) and its main applications
- The mathematical limits of Watermarking and different analysis techniques for such limits
- Different commercial and e-commerce protocols of Digital watermarking

Reference Book

Digital Watermarking and Steganography,

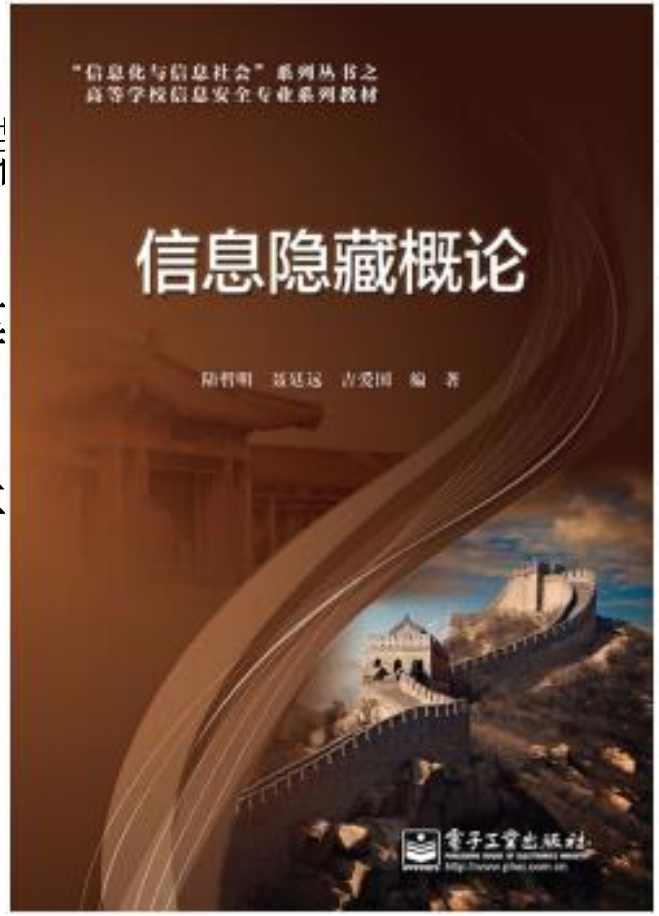
Second Edition

Ingemar Cox , Matthew Miller , Jeffrey Bloom , and Jessica Fridrich , Morgan Kaufmann Publishers , 2007



Reference Books

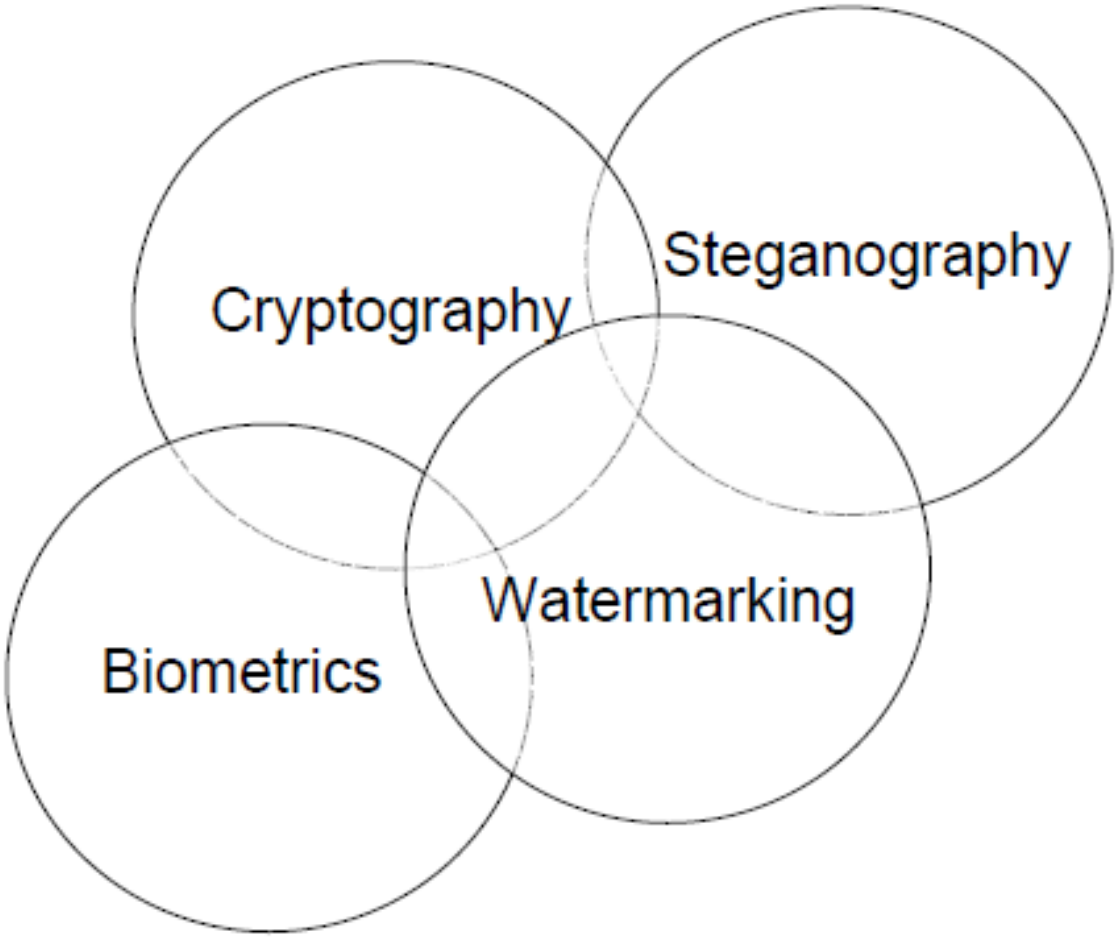
I. 信息隐藏概论，陆哲明等编著，电子工业出版社，2014
II. 数字水印，王颖，黄志蓓等译，Matthew Miller，Jeffrey Bloom著，社，2003
III. 信息隐藏技术与应用，王丽娜等，版社， 2012
IV. 信息隐藏与数字水印，钮心忻著，版社，2004



「 Part One 」

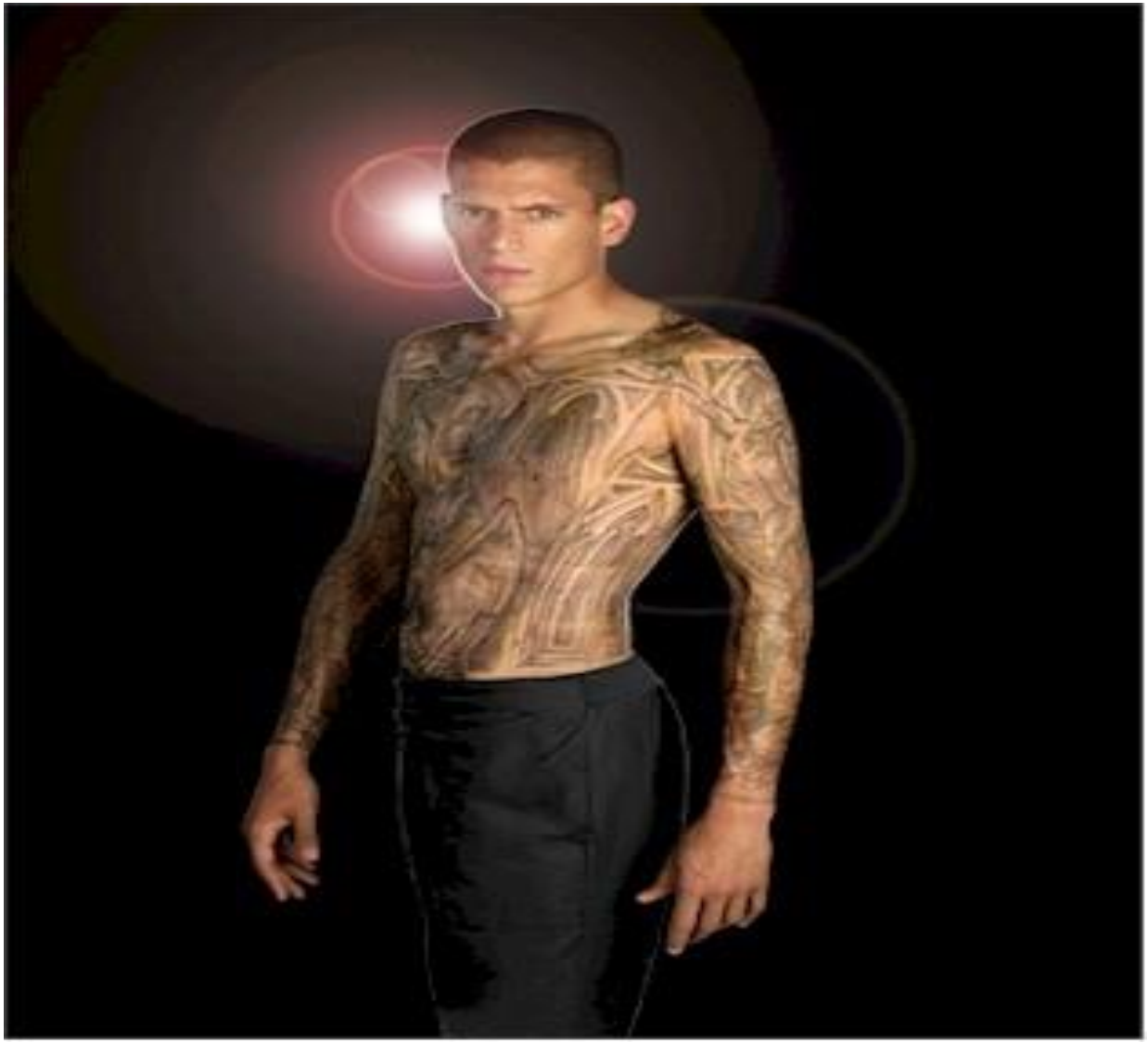
Introduction

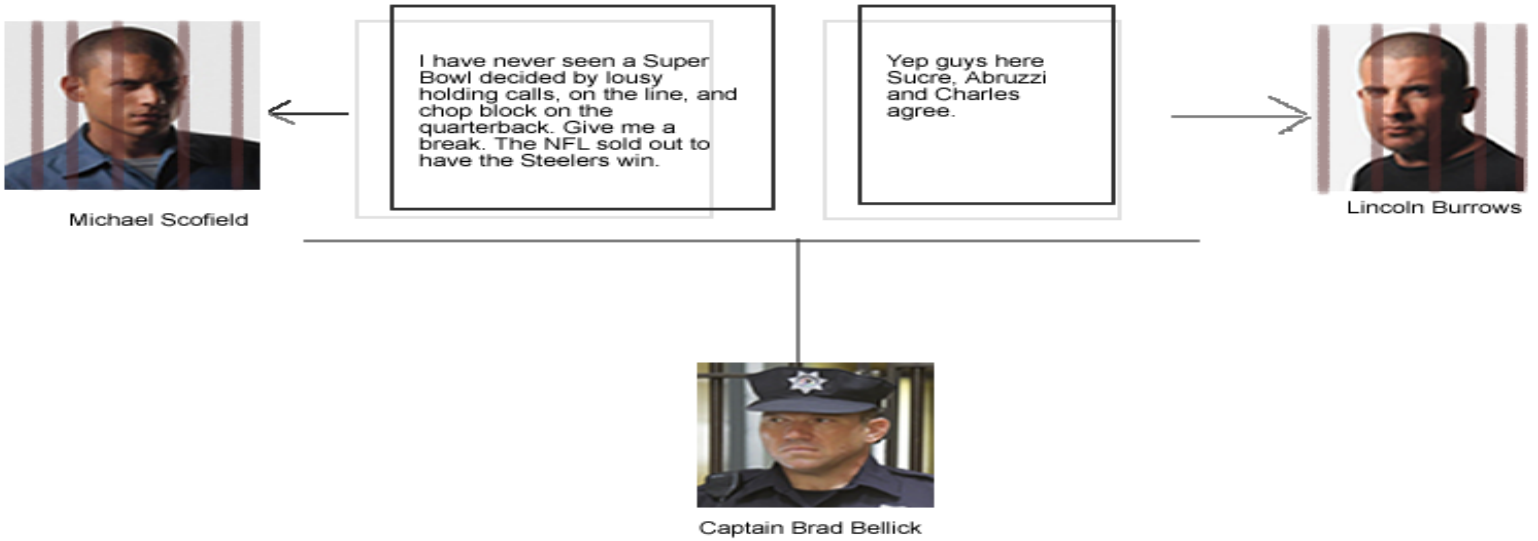
Multemedia Security



Steganography Topics

- What is Steganography?
  - Cryptography vs Steganography vs Watermarking
- Why Steganography?
- Steganography Classes and Methods
  - Spatial and Transform
  - Trade-offs
- Attacks, Steganalysis and Detection



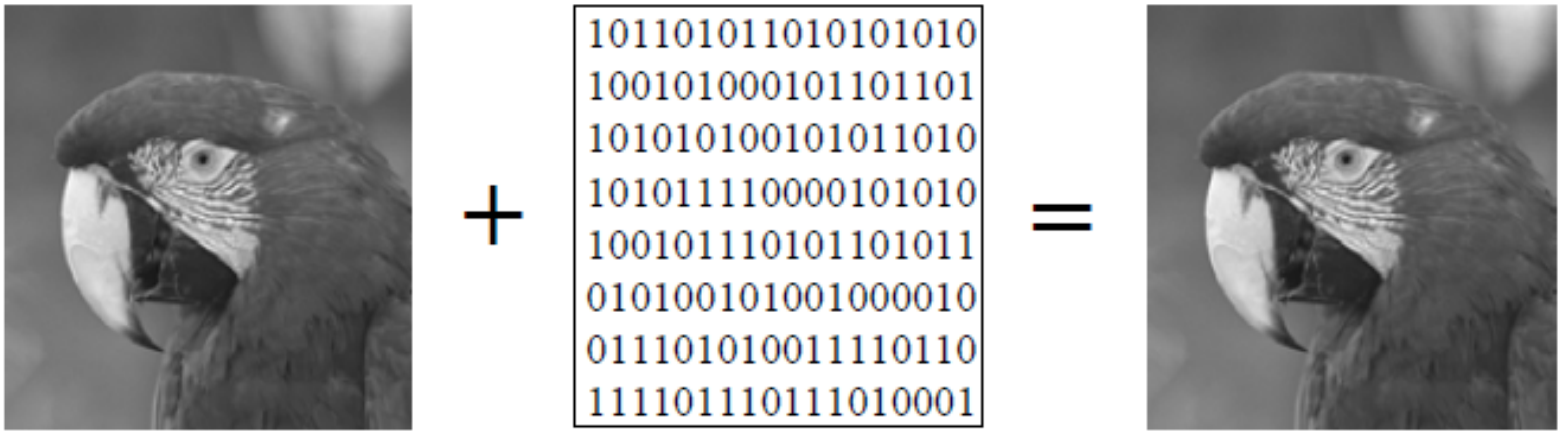


Prisoners Problem

- Michael Scofield and Lincoln Burrows are in jail
- They want to develop an escape plan
- The only way to communicate is through Captain Bellick
- They must communicate in a manner that does not raise suspicion

What is Digital Steganography

- Greek: meaning “Covered (or Hidden) Writing”
- Concealing a message within another message
- Typically host message or “container” is not private
- Cryptography: Conceal message content
- Steganography: Conceal communication
- Watermarking: Subset of Steganography



What is Digital Steganography

- Cryptography and Steganography - both provide **secret communication**:
  - **Cryptography** hides contents of the message from an attacker, but not the existence of the message
  - **Steganography** even hides the very existence of the message in the communicating data

- Consequently, concept of breaking the system is **different** for cryptosystems and stegosystems and watermarking systems

What is Digital Steganography

- Cryptographic system is broken when attacker can read the secret message
- Breaking of steganographic and watermarking system has two stages:
  - Attacker detect that steganography/watermarking has been used
  - Attacker able to read, modify or remove the hidden Message
- Steganography system is considered as insecure already if the detection of steganography is possible

What is Digital Steganography

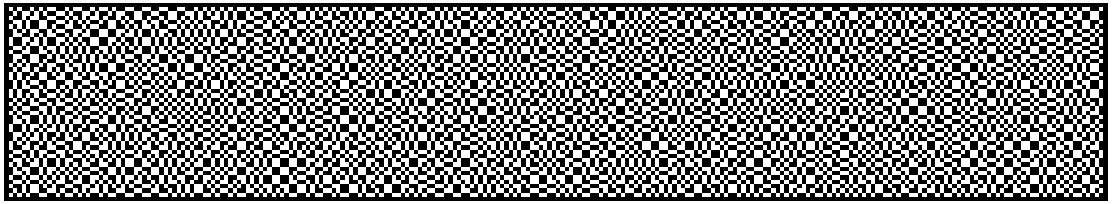
Encryption

Steganography

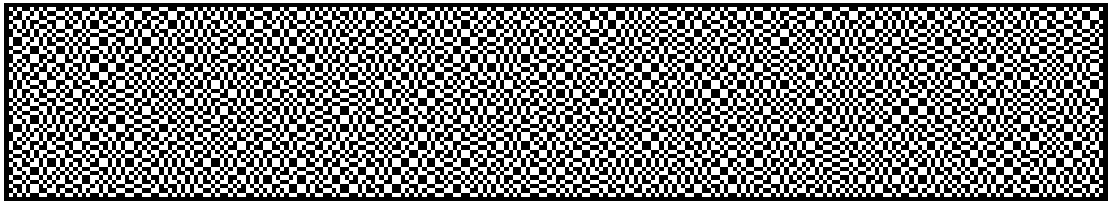
(Contains embedded encrypted message)

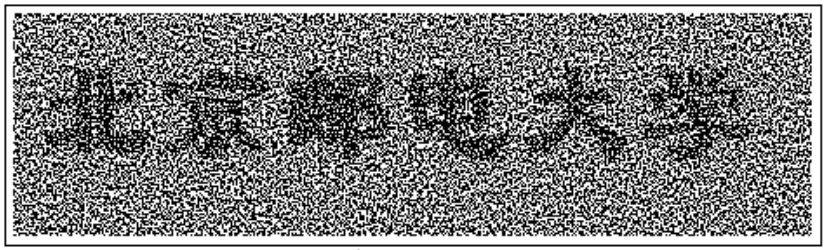
Visual Cryptography

share 1

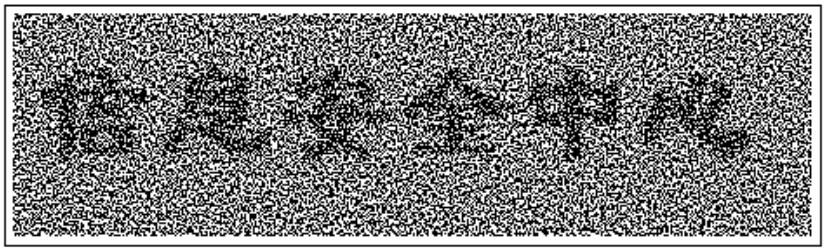


share 2

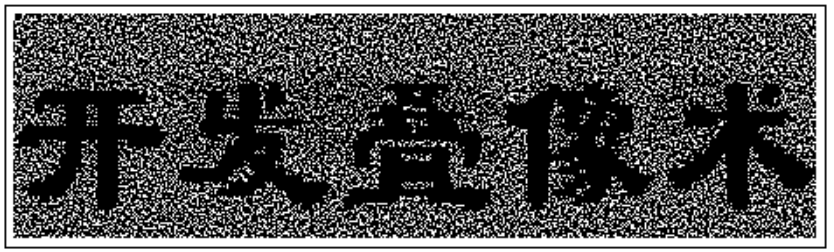




p1 “北京邮电大学”



p2 “信息安全中心”

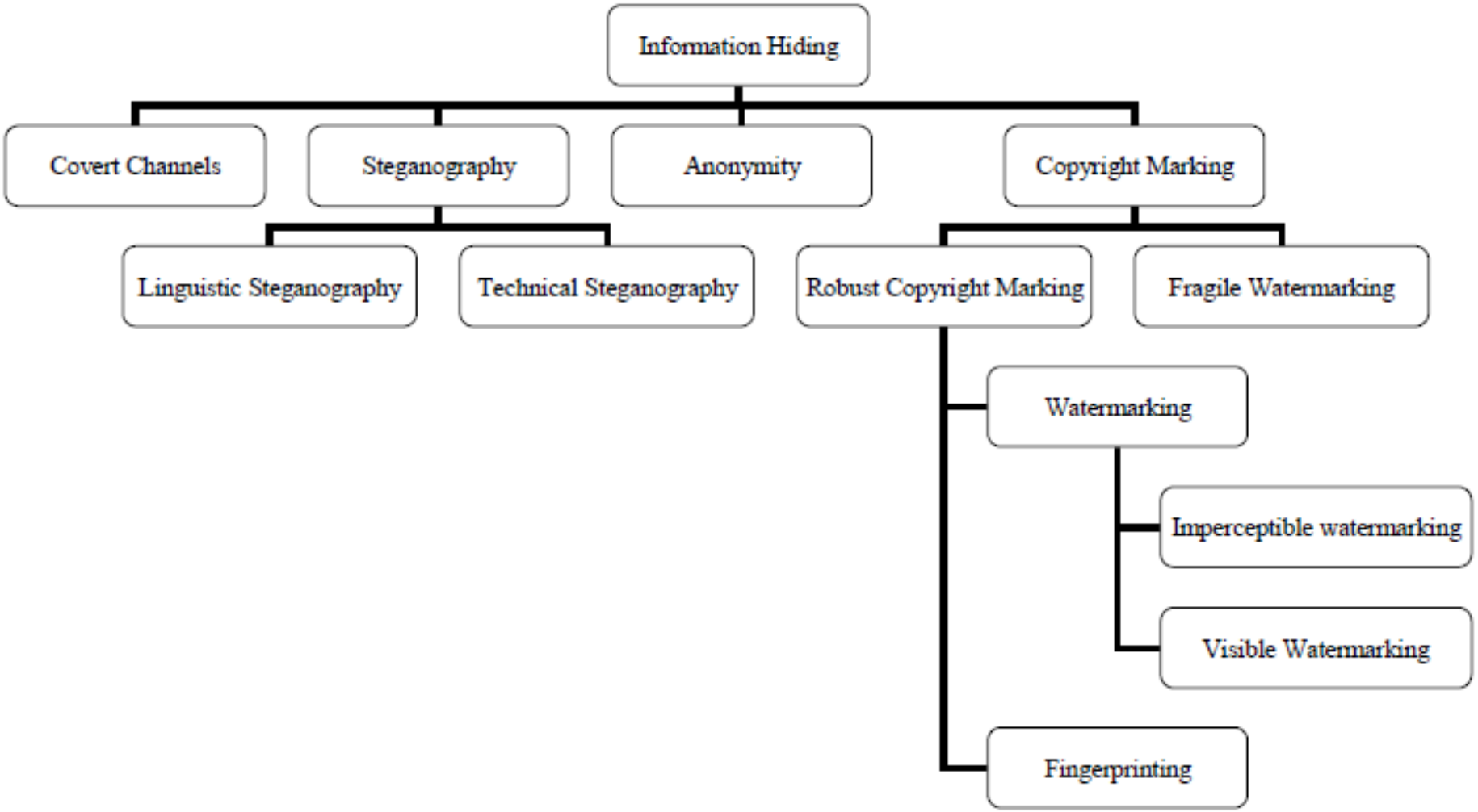


p3=p1+p2=“开发叠像术”

图2 改进后的叠像术

What is Digital Steganography

- **Classification of Information Hiding Techniques**



What is Digital Steganography

- Differences between steganography and watermarking are both subtle and essential, as follows:

  – **Steganography** is **to hide** a message ***m*** in some audio or video (cover) data ***d***, to obtain new data ***d'***, practically indistinguishable from ***d***, by people, in such a way that an eavesdropper ***cannot detect*** the presence of ***m*** in ***d'***

  – **Watermarking** is **to hide** a message ***m*** in some audio or video (cover) data ***d***, to obtain new data ***d'***, practically indistinguishable from ***d***, by people, in such a way that an eavesdropper ***cannot remove or replace*** ***m*** in ***d'***

What is Digital Steganography

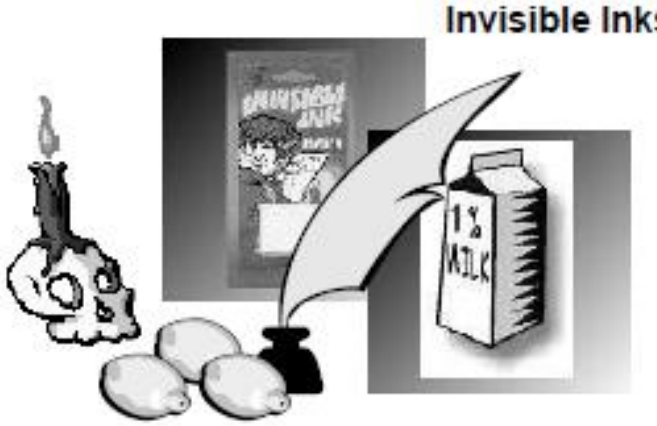
- Often said that goal of steganography is to hide a message in **one-to-one communications** and goal of watermarking is to hide message in **one-to-many communications**
- Cryptography is about **protecting** the content of messages, steganography is about **concealing** its very existence
- Steganography methods usually do not need to provide strong security against removing or modification of the hidden message
- Watermarking methods need to be very robust to attempts to remove or modify a hidden message

Examples of Steganography

Ancient Greece,
5th-Century B.C.
Tattooing secret message
on
slave's head

Trithemius,
Steganographia,
1606

Gaspari Schotti,
Schola
Steganographica,
1665



Null ciphers — camouflaging secret messages in innocent sounding message

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.

Pershing sails from NY June 1

Examples of Steganography

- **Mid-Autumn Festival**

  –Hidden Message (Message to organise a revolt against the Mongols)

  –Container (Moon cakes)

- **Nature**

  - Hidden Message (Leaf Insect, Chameleon)

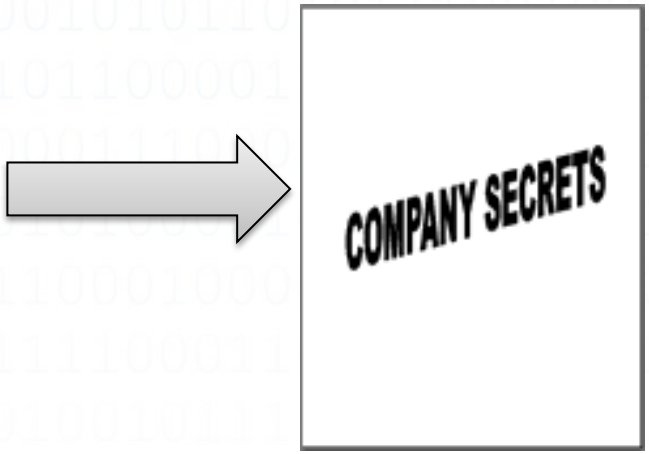
  - Container (Leaves, Surrounding)

Examples of Steganography

Now - Innocent Web Page?

Internet - modern day of “Dead Drop” – Slang describing location where Cold War-era spies left maps, pictures and other information

Estimated 28 Billion Images and 2 Billion Web sites on Internet



Examples of Steganography

- Patient and steady with all he must bear,
- Ready to meet every challenge with care,
- Easy in manner, yet solid as steel,
- Strong in his faith, refreshingly real.
- Isn't afraid to propose what is bold,
- Doesn't conform to the usual mould,
- Eyes that have foresight, for hindsight won't do,
- Never backs down when he sees what is true,
- Tells it all straight, and means it all too.
- Going forward and knowing he's right,
- Even when doubted for why he would fight,
- Over and over he makes his case clear,
- Reaching to touch the ones who won't hear.
- Growing in strength he won't be unnerved,
- Ever assuring he'll stand by his word.
- Wanting the world to join his firm stand,
- Bracing for war, but praying for peace,
- Using his power so evil will cease,
- So much a leader and worthy of trust,
- Here stands a man who will do what he must.

THE LEADER

Examples of Steganography

Examples of Steganography

Null Ciphers (unencrypted messages) - real message is "camouflaged" in an innocent message

This hidden article needs keeping safe
From other renegade
Yeomen of unscrupulous reputation
Awaiting to theorize every new technological idea
of nonsense!

Examples of Steganography

This hidden article needs keeping safe
From other renegade
Yeomen of unscrupulous reputation
Awaiting to theorize every new technological idea of nonsense!

Container = Message or Image
Hidden (watermark) = “Thanks For Your Attention!”
Key: permutation of characters (fixed or random)

Examples of Steganography

Dear George,
Greetings to all at Oxford. Many thanks for **your** letter and for the summer examination **package**. All entry forms and fees forms should be **ready** for final dispatch to the syndicate by **Friday** 20th or at the latest I am told by the **21st**, Admin has improved here though there is **room** for improvement still; just give us all two or **three** more years and we will really show you! **Please** don't let these wretched 16+ proposals **destroy** your basic O and A pattern. Certainly **this** sort of change, if implemented **immediately**, would bring chaos.

Sincerely yours,

Why Steganography now?

- Government agencies are concerned about the use of Steganography
- Common uses include the disguising of corporate espionage
- Rumoured that terrorist cells may use it to secretly communicate information:
  - Common technique used by Al-Qaeda. By posting the image on a website for download by another terrorist cell. Using the same Steganography program, the terrorist cell could then reveal the message with plans for a new attack
- Child pornography by paedophiles

Why Steganography now?

Bin Laden: Steganography Master?
by Declan McCullagh

2:00 a.m. Feb. 7, 2001 PST

WASHINGTON -- If there's one thing the FBI hates more than Osama bin Laden, it's when Osama bin Laden starts using the Internet.

So it should be no surprise that the feds are getting unusually jittery about what they claim is evidence that bin Laden and his terrorist allies are using message-scrambling techniques to evade law enforcement.

USA Today reported on Tuesday that bin Laden and others "are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other websites, U.S. and foreign officials say."

The technique, known as steganography, is the practice of embedding secret messages in other messages -- in a way that prevents an observer from learning that anything unusual is taking place. Encryption, by contrast, relies on ciphers or codes to scramble a message.

Why Steganography now?

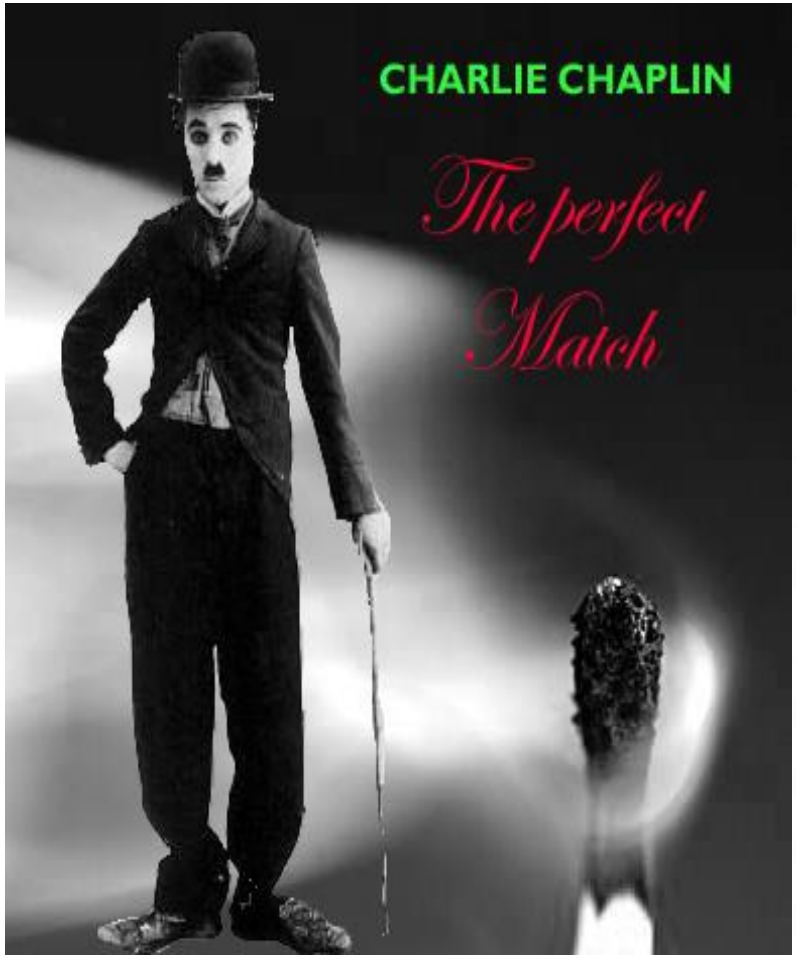
- Steganography is primarily of use in **maintaining anonymity** and it can be applied to virtually any **digitized audio, graphics, or text file**
- Uses include:
  - Creating covert channels for private communications
  - Data infiltration/exfiltration
  - Digital signatures for file authentication (digital watermarking or copyrighting)
  - Web surfer tracking/direct marketing

Why Watermark?

Why Watermark?

Copyright Protecton:

To prove
the ownership
of digital media



Copyright Protection:


皇帝奉天之宝玺


敕正万邦之宝玺


敕正万民之宝玺

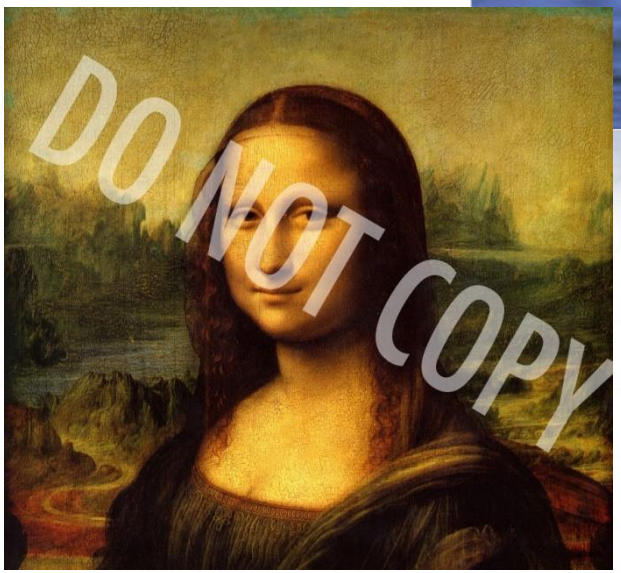
Why Watermark?

Watermark

Image with watermark

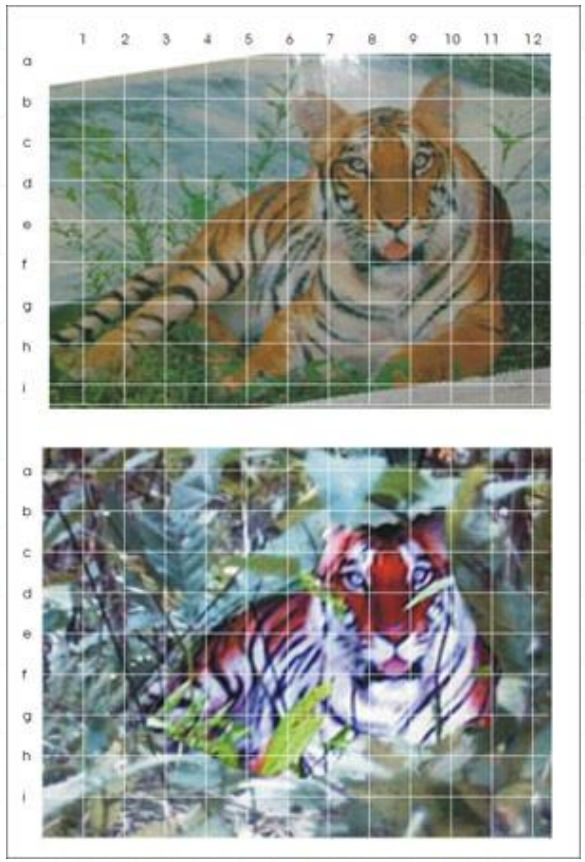
Embed

Remove

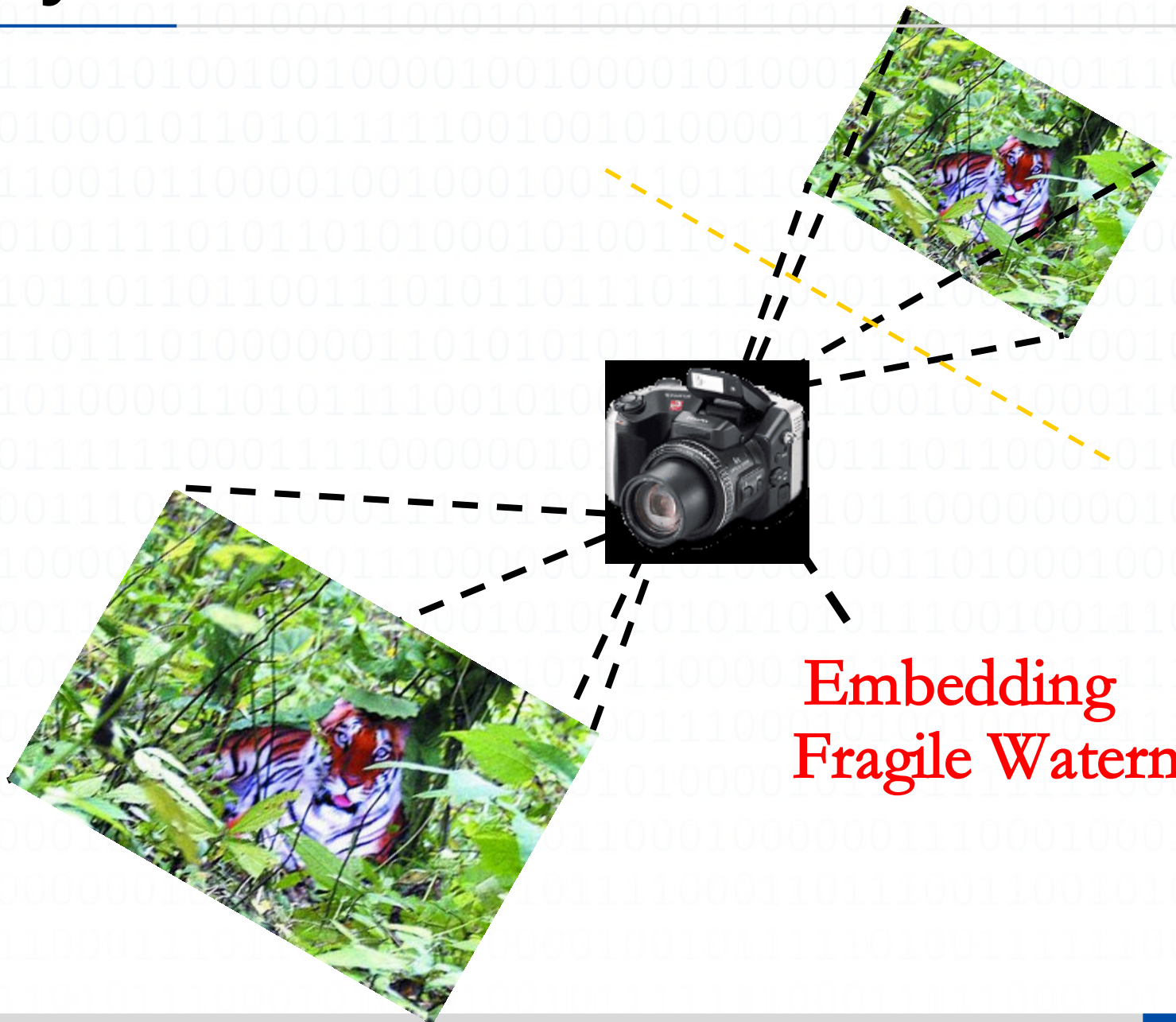


Why Watermark?

The authenticity of the news report:



Why Watermark?



Embedding
Fragile Watermark

Why Watermark?

An example of digital image modification[1]

Why Watermark?

- The problem:

  How to detect ***fakes*** like this?

Digital image evidence: ***fake*** or ***not***?
Applications:
traffic enforcement, crime scene investigation, news report, medical imaging …


CNGBA.COM
UNA PELÍCULA DE STEVEN SPIELBERG
tom hanks
salvar al soldado ryan
edward burns matt damon tom sizemore
la misión es un hombre.
PARAMOUNT PICTURES Y DREAMWORKS PICTURES
UNA PRODUCCIÓN AMBLIN ENTERTAINMENT EN ASOCIACIÓN CON MUTUAL FILM COMPANY
EDWARD BURNS MATT DAMON TOM SIZEMORE
PSP资源分享联盟
www.psp1more.com


拯救礦工鄭大世
在有安全隐患的煤矿，
每一次下井对矿工来说都无异于参加一次残酷的战役，
生命无法得以保障！
国家安全生产监督管理局

「 Part Two 」

IH Technologies

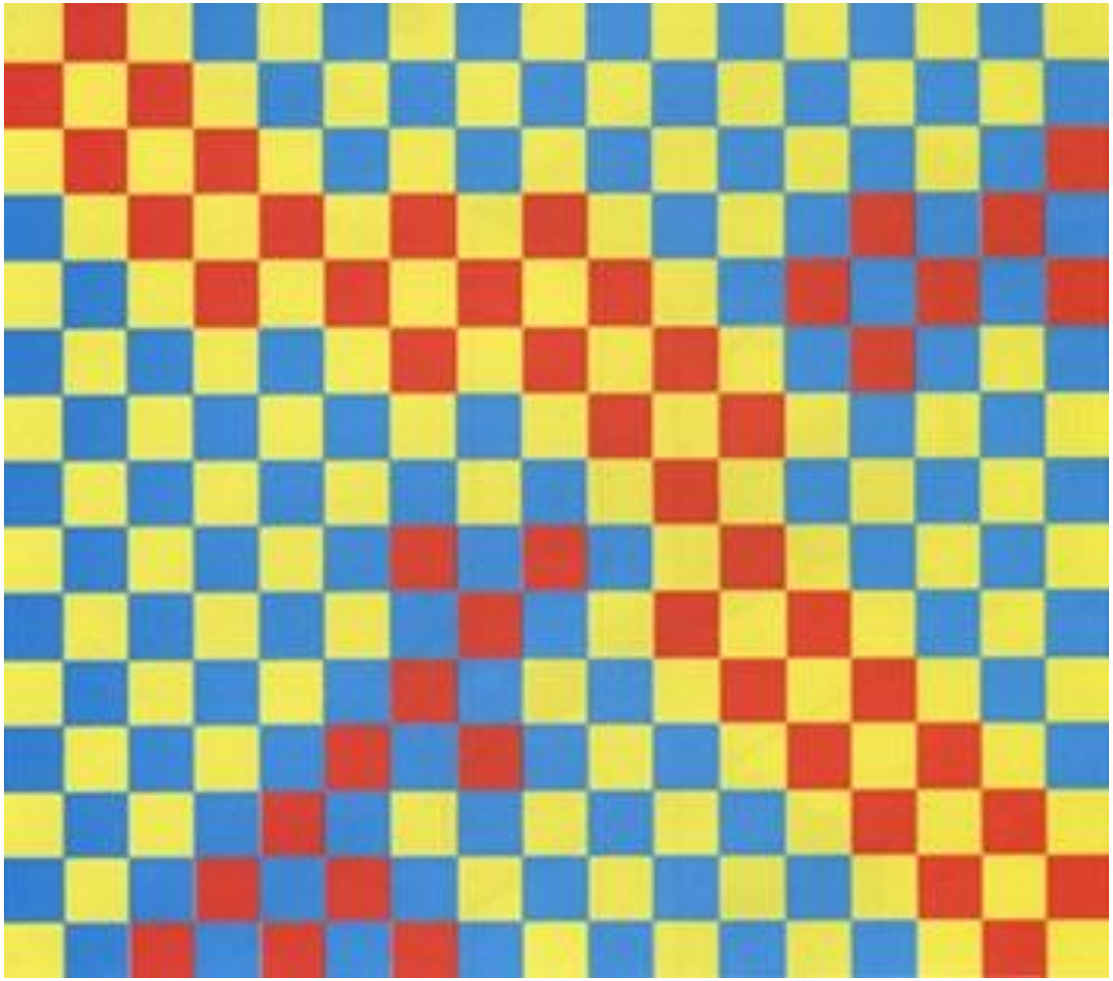
Why is it available?

- Using Human Visual Redundancy
- Using Redundancy of a Computer Processing System
- Based on Subliminal Channel Theory

It is feasible in technology!

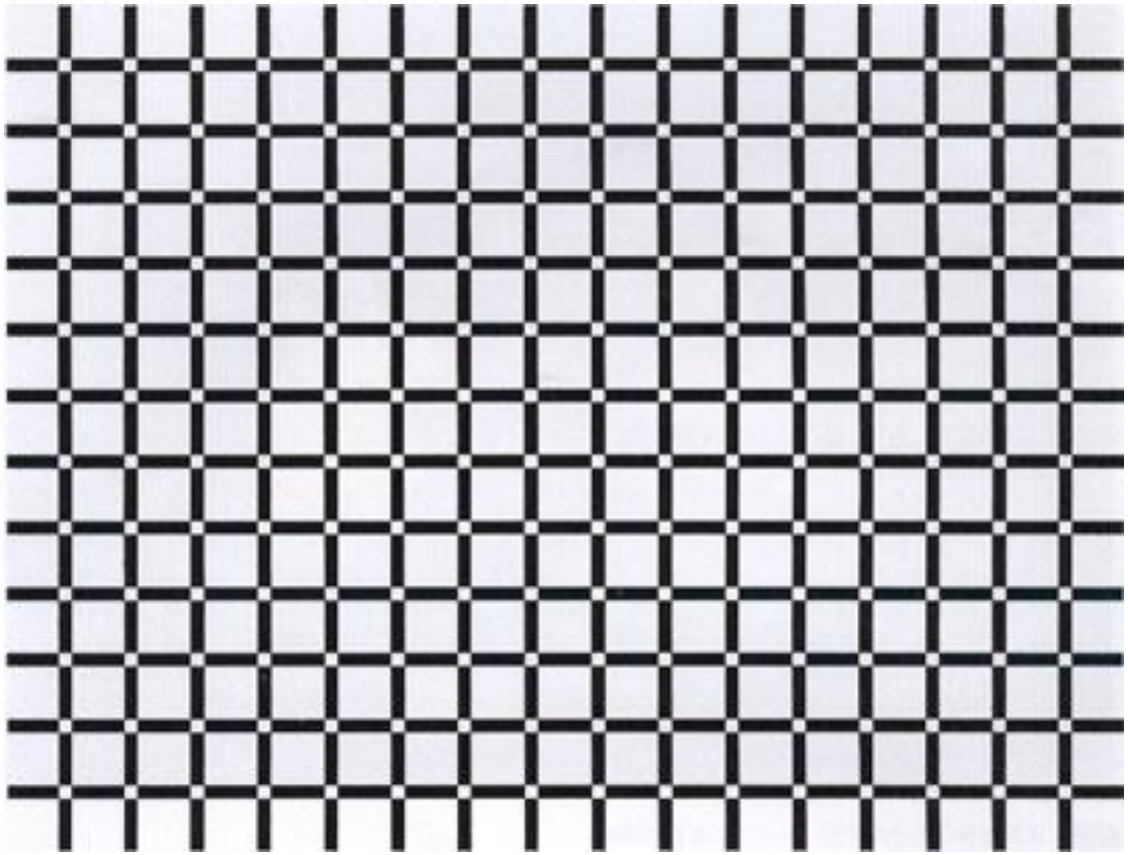
Human Visual Redundancy

比泽尔德幻觉：图中所有的红色看起来都一样吗？



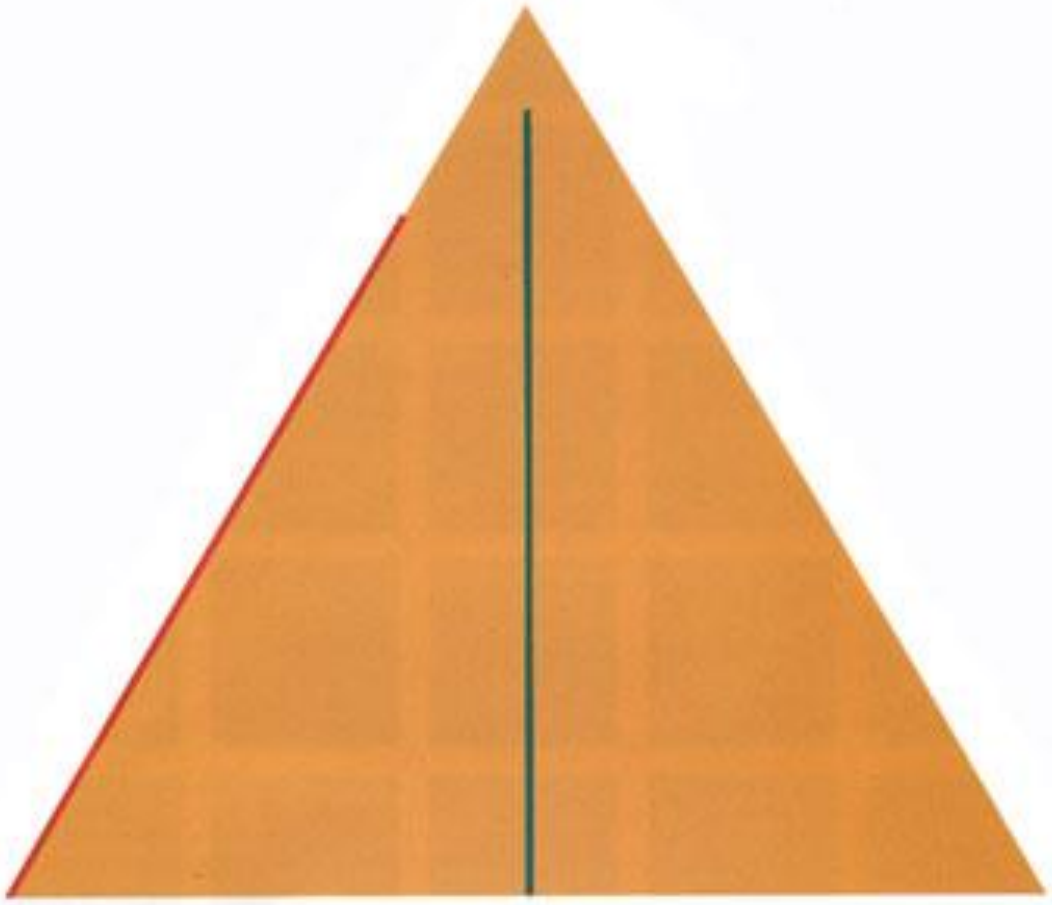
Human Visual Redundancy

共时对照幻觉：交叉部分的白点是不是显得比白色方格更白更亮？



Human Visual Redundancy

三角长度幻觉：哪个颜色的线看起来更长？



Human Visual Redundancy

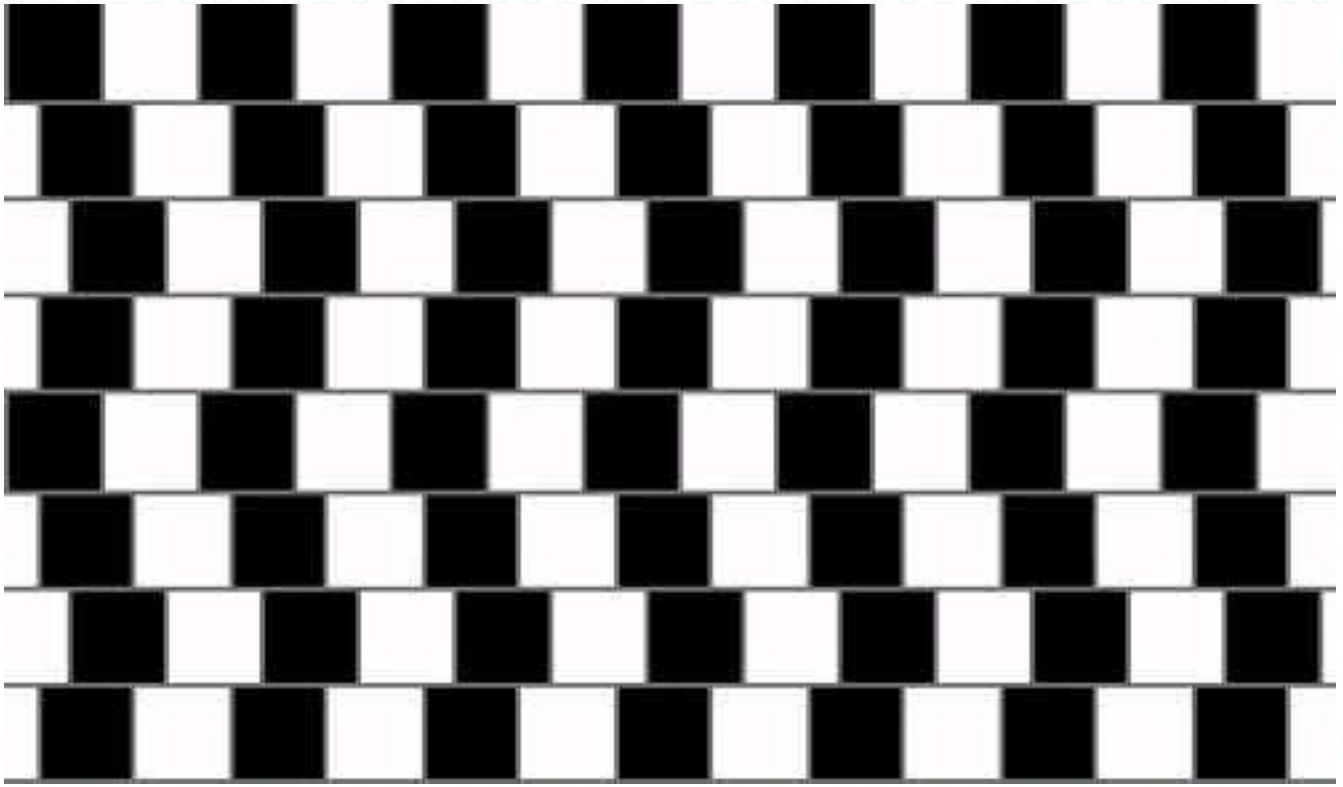
韦德螺旋：这真是一个螺旋吗？

Human Visual Redundancy

这只动物驴子还是海豹？

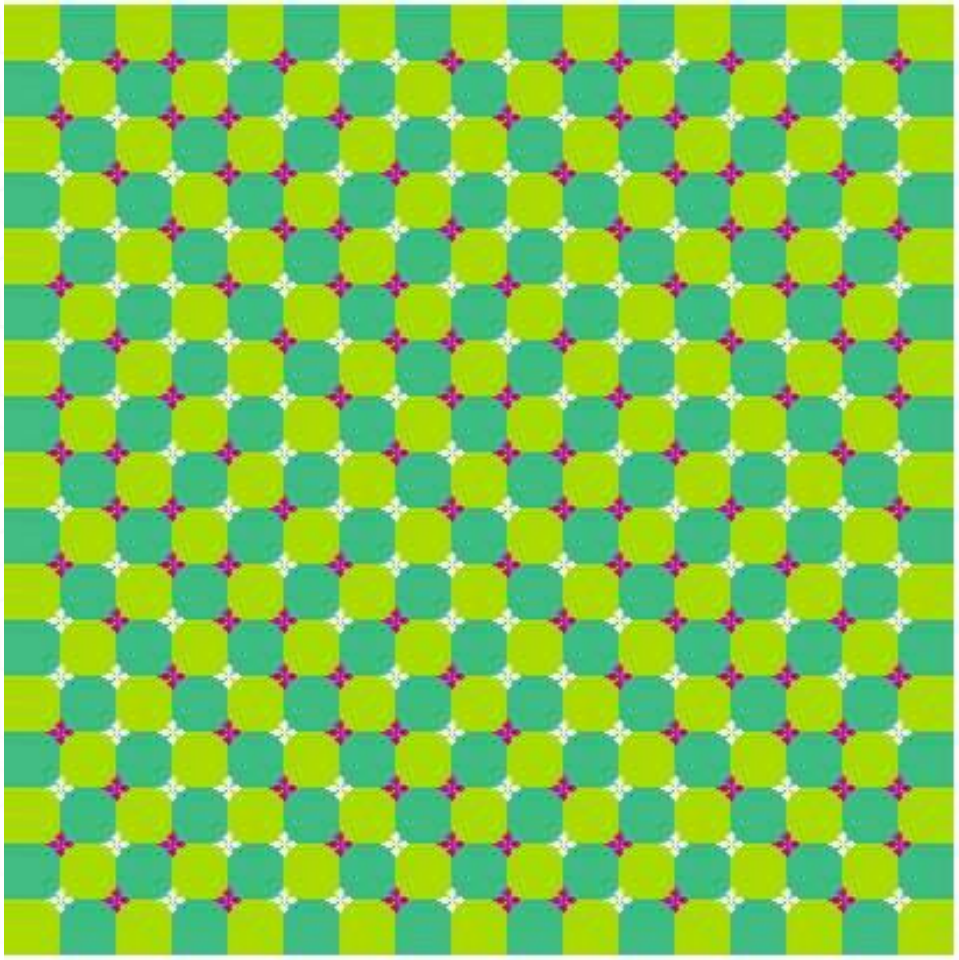
Human Visual Redundancy

不可思议平行线



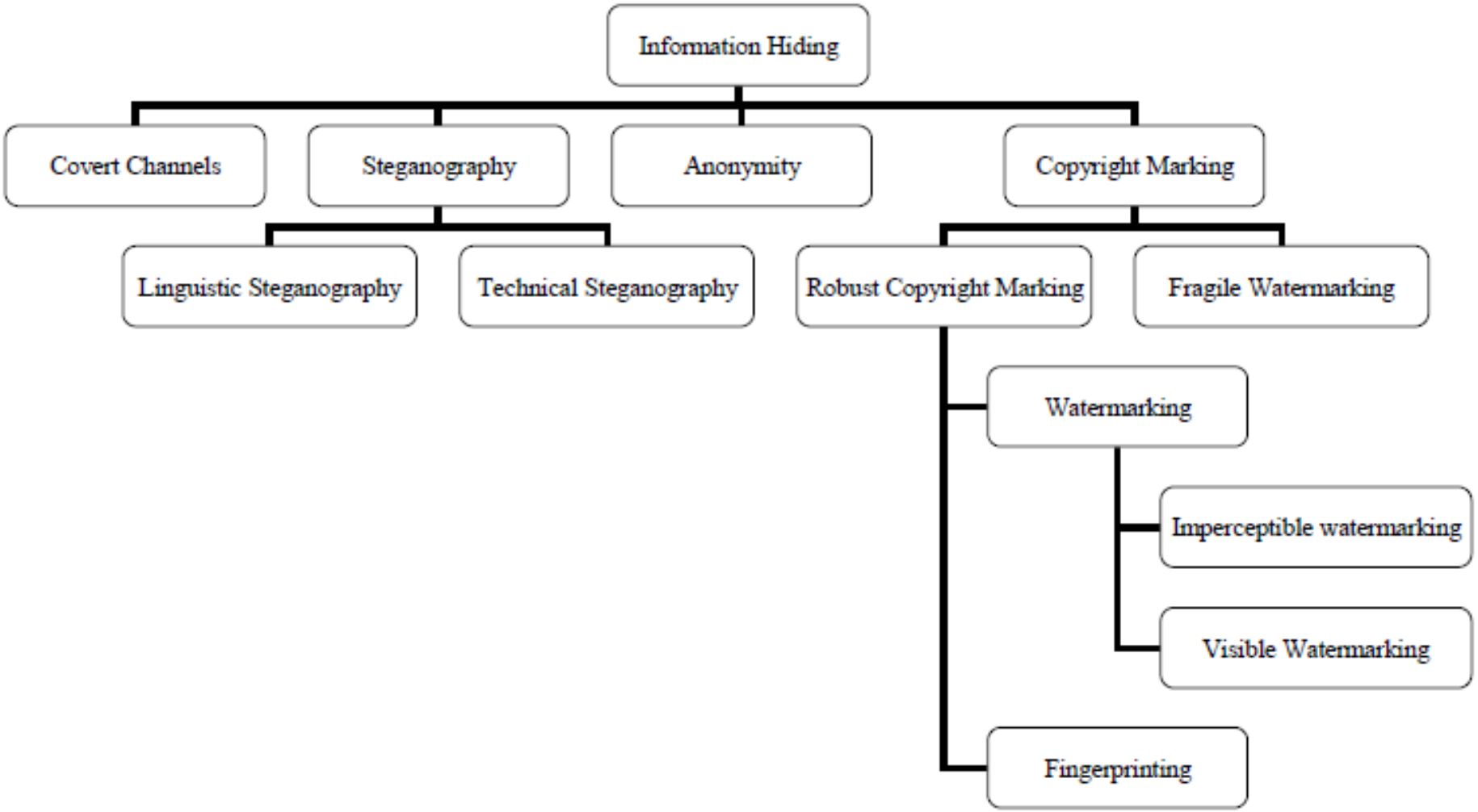
Human Visual Redundancy

- 波涛荡漾：前后伸伸头，左右挪挪头



Classification

❖ Classification of Information Hiding Techniques



Information Hiding

- Information Hiding…..started with:

Steganography (art of hidden writing):

The art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. The existence of information is secret.

Stego – Hidden , Graphy – Writing → ‘art of hidden writing’

Digital Watermarking

Digital Watermarking:

Application of Information hiding (Hiding Watermarks in digital Media, such as images)

Digital Watermarking can be ?

- Perceptible (e.g. author information in .doc)
- Imperceptible (e.g. author information in images)

Visibility is application dependent

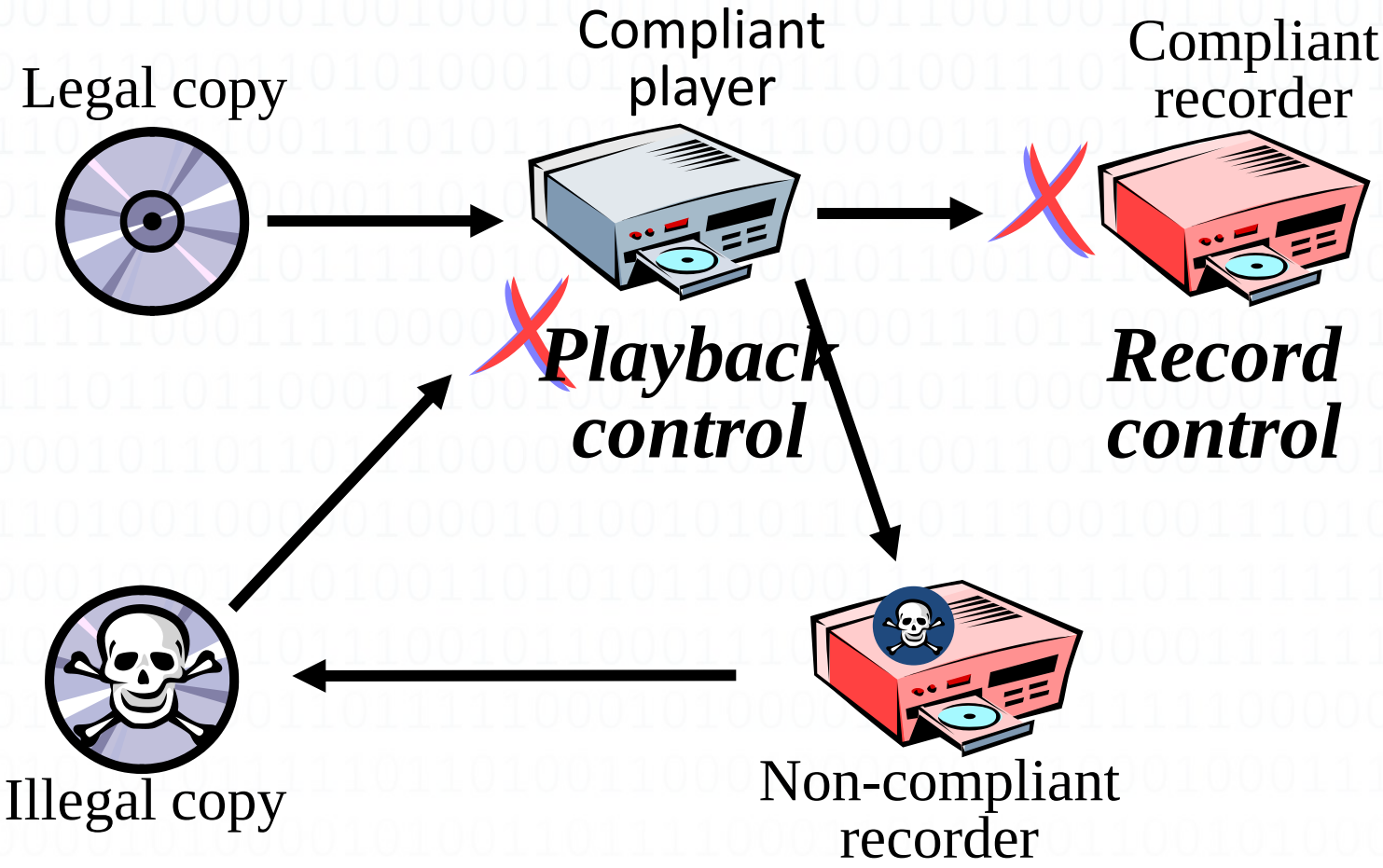
Invisible watermarks are preferred

Applications of Digital Watermarking

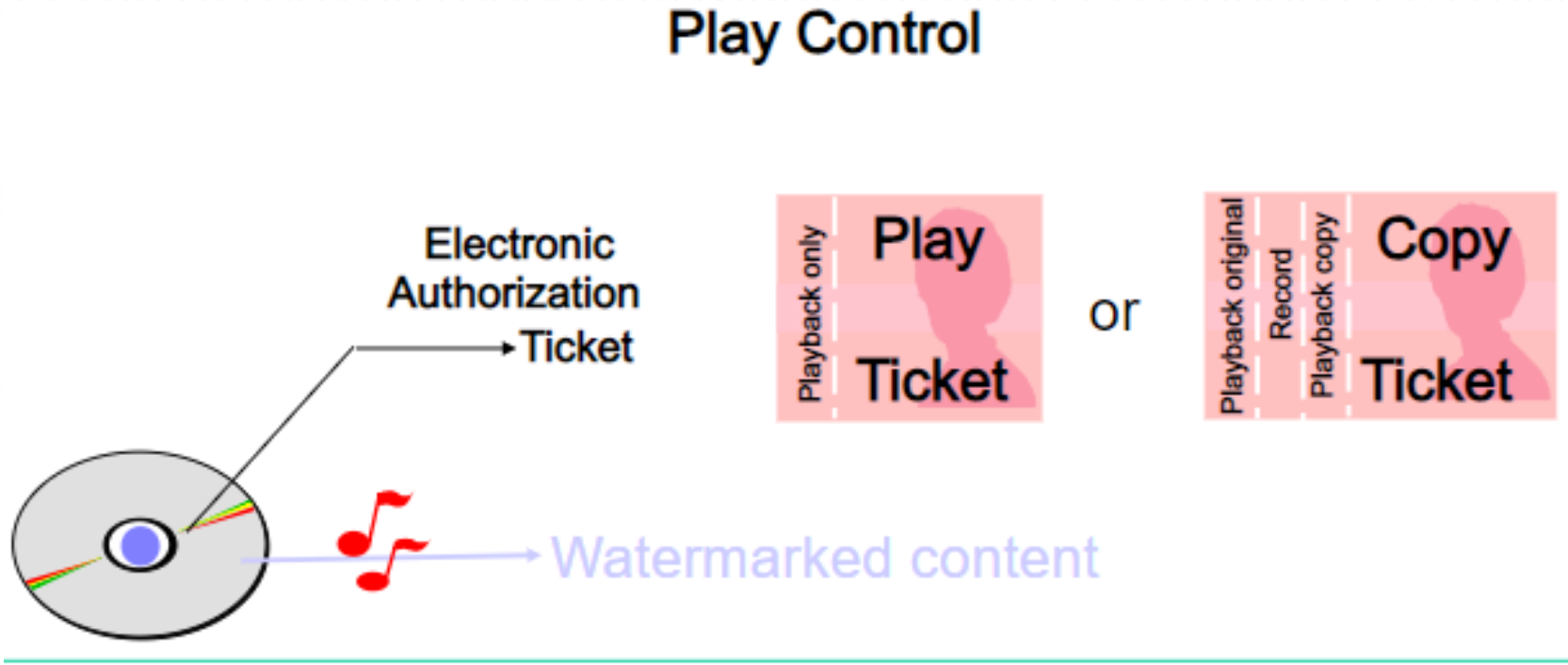
- Copyright Control
  - playback, copy-generation control (DVD, SDMI)
- Proof of Ownership
- Proof of Authenticity
- Transaction Tracking
- Broadcast Monitoring
  - check on royalty payments
  - commercial verification
- Distribution Tracing
  - fingerprinting

Applications of Digital Watermarking

- Copy Control



Applications of Digital Watermarking



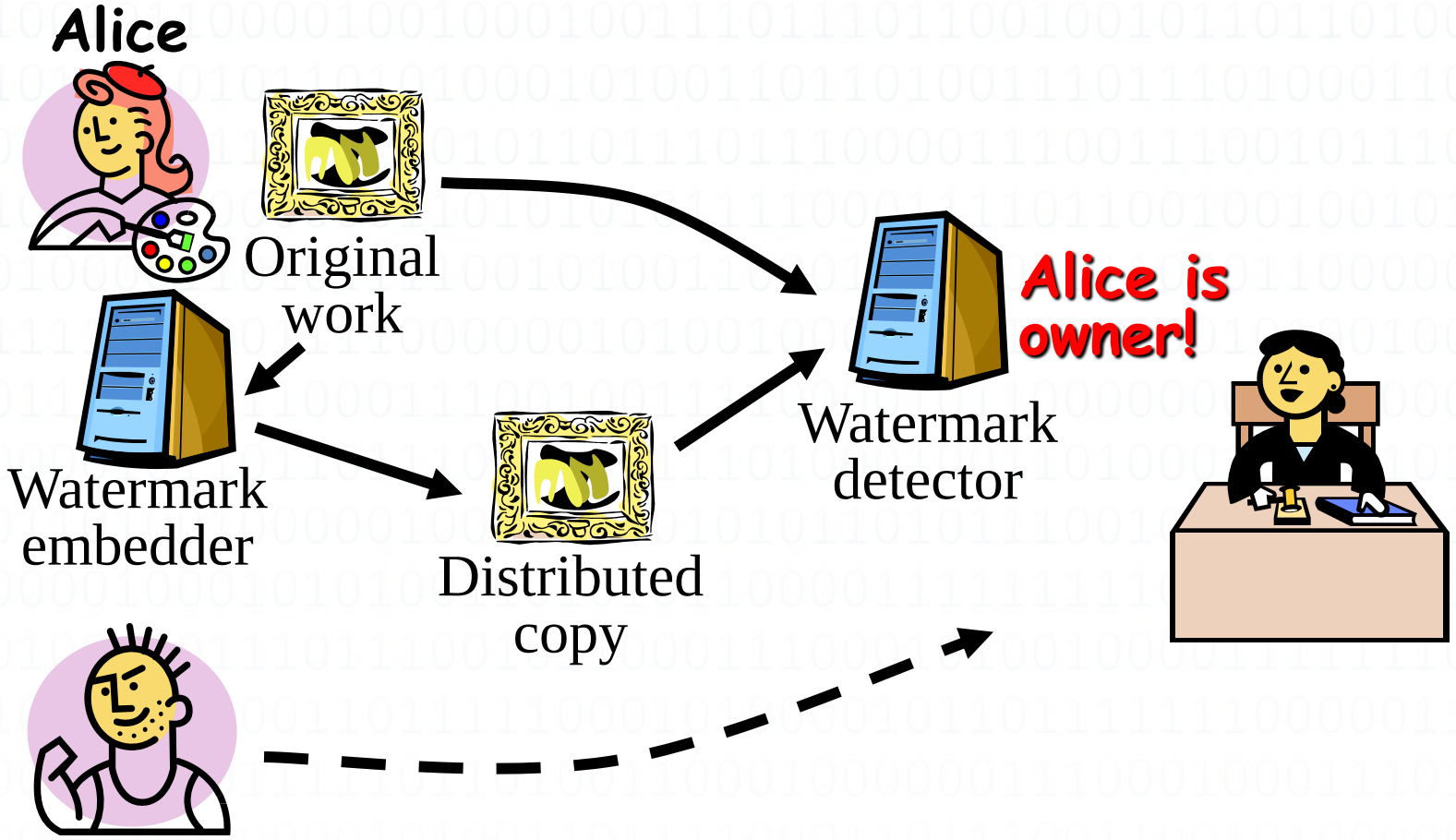
Record / playback ONLY if

+ Copy Ticket : Watermark matches with valid ticket

or : Free-Copy: No Watermark

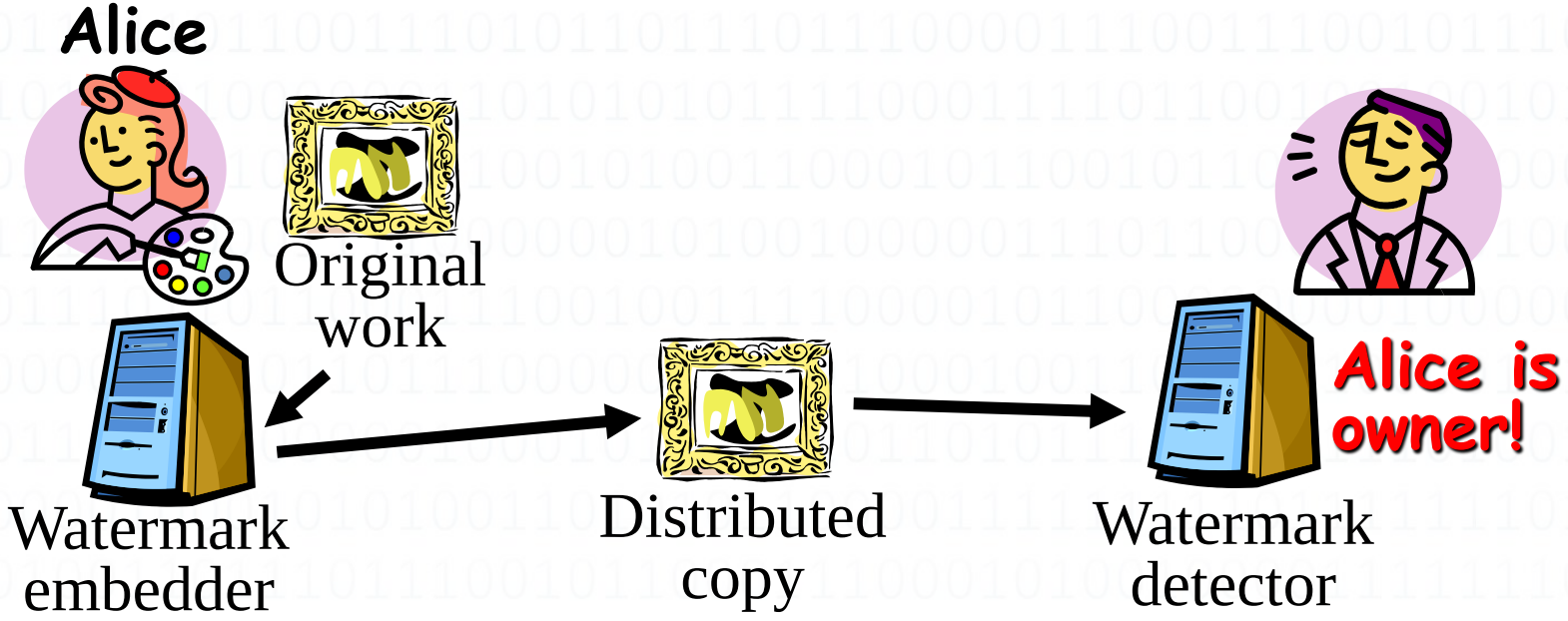
Applications of Digital Watermarking

- Proof of ownership



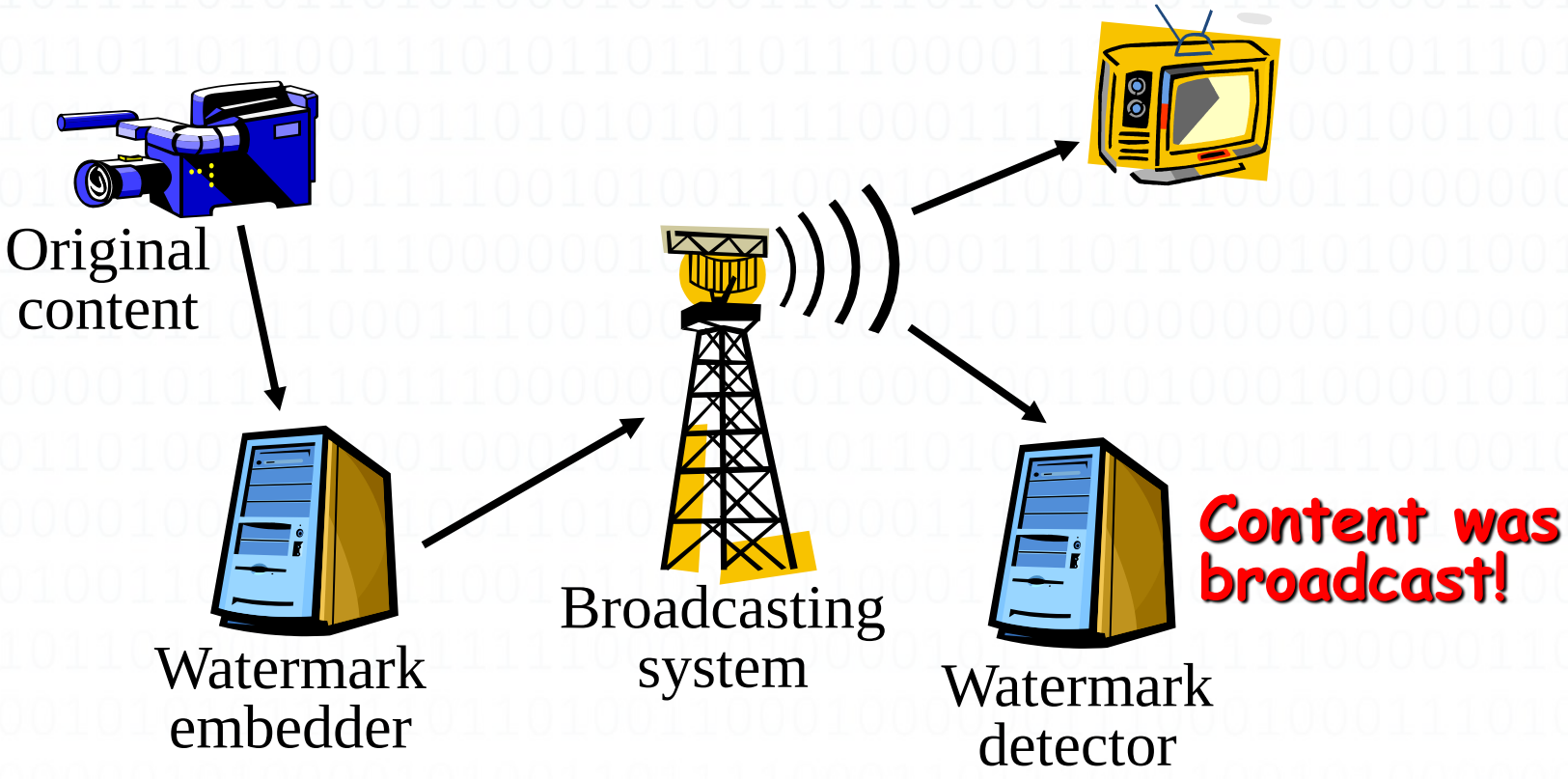
Applications of Digital Watermarking

- Owner identification



Applications of Digital Watermarking

- Broadcast Monitoring



Applications of Digital Watermarking

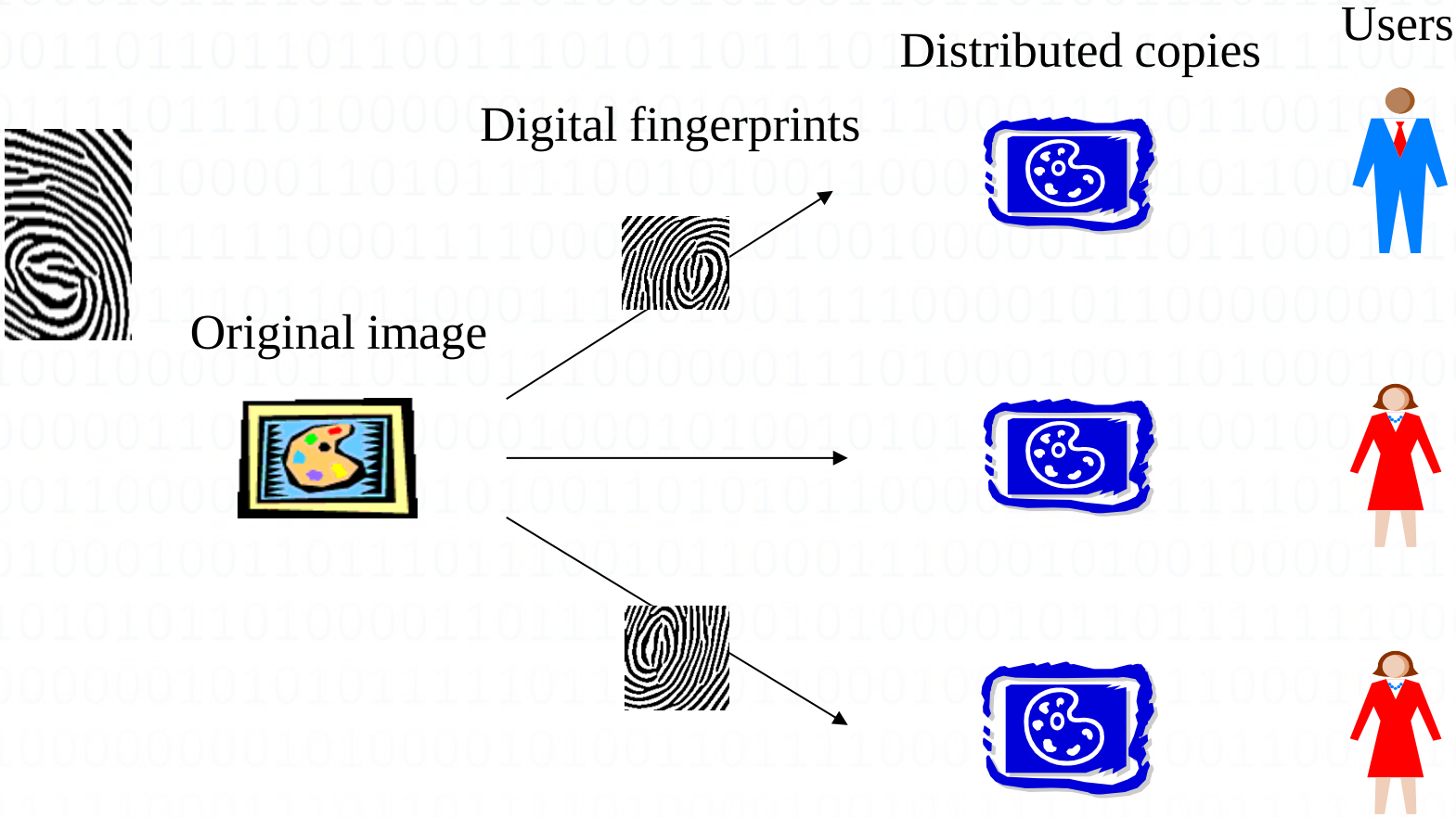
(a) (b) (c)

Figure : Using digital watermarks for integrity verification. The protected image is on the left. A modified image is obtained by swapping the numbers 9 and 4. Watermarking technology allows to detect and highlights the modified areas, as shown on the right.

Applications of Digital Watermarking

Applications of Digital Watermarking

Digital Fingerprints



Applications of Digital Watermarking

叛逆者追踪

1981 British Cabinet Betrayal of Confidentiality Event

Applications of Digital Watermarking

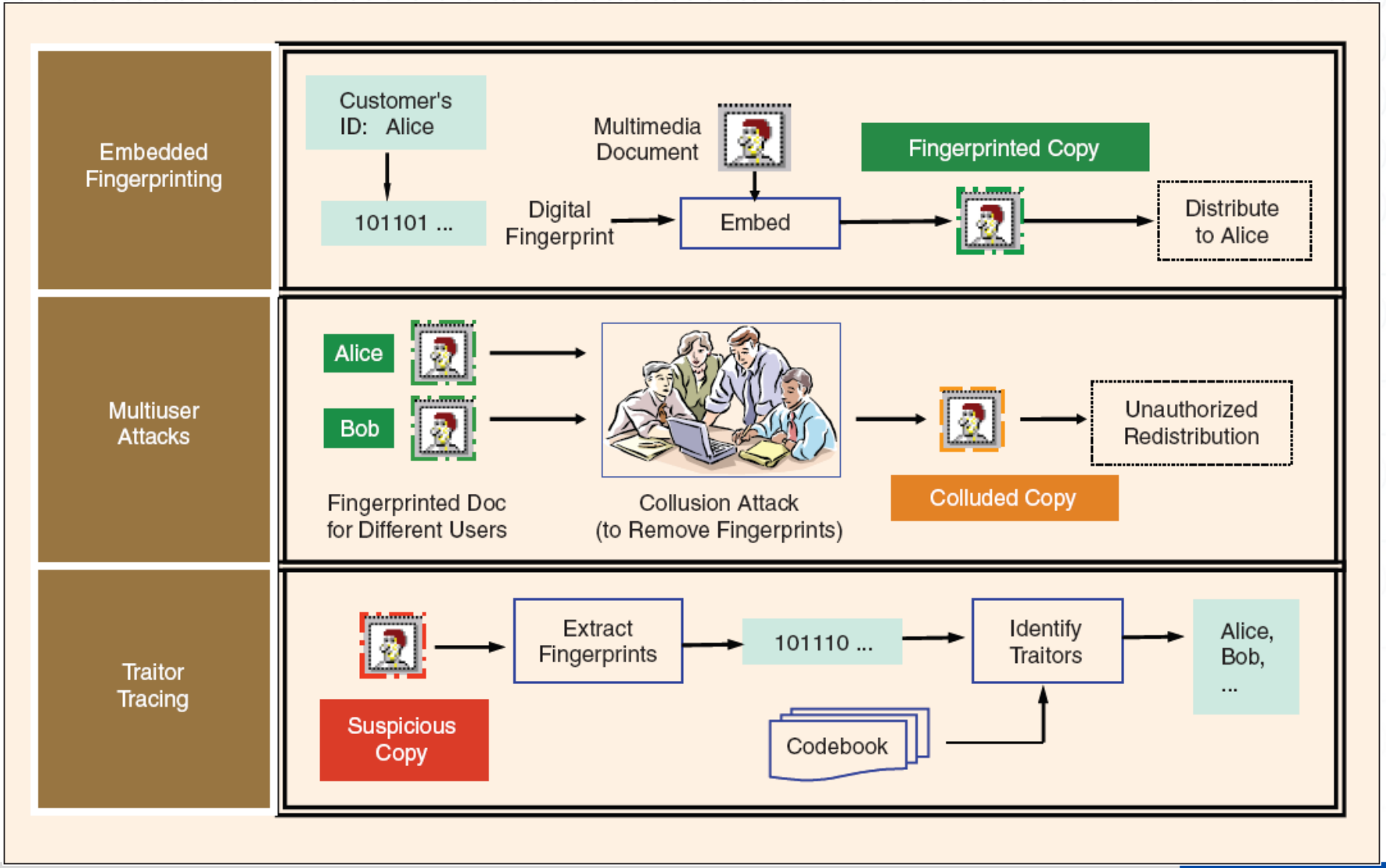
Now	is	the	time	for	all	men/women	to ...
Now	is	the	time	for	all	men/women	to ...

Now is the time for all men/women to ...

Now is the time for all men/women to ...

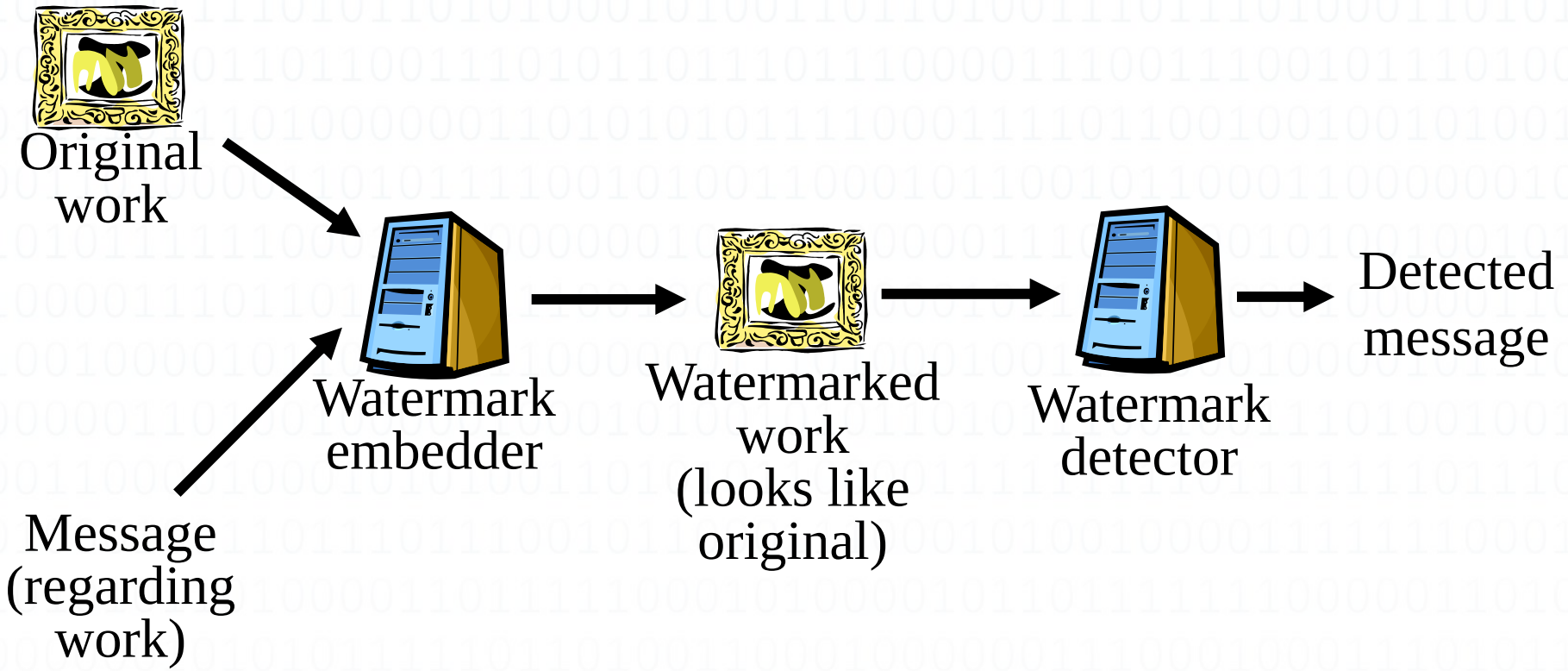
Applications of Digital Watermarking

叛逆者追踪



Digital Watermarking System

- Basic design of a system



「 Part Three 」

IH Terminology

Terminology

- Embedding effectiveness 嵌入的有效性
- Fidelity 保真性
- Data payload 数据容量
- Blind vs. informed detection 盲检测或含辅助信息检测
- False positive rate 虚警率或错误肯定率
- Robustness 鲁棒性
- Security 安全性

Terminology

- 水印载体 Carrier
- 嵌入域 Embedding domain
- 鲁棒性 Robustness
- 可见性（可察觉性） Visibility
- 检测方式 Detection
- 可逆性 Reversibility

Terminology

- 图像水印 Image watermarking
- 视频水印 Video watermarking
- 音频水印 Audio watermarking
- 文档水印 Text watermarking
- 软件水印 Software watermarking

Terminology

- 空域水印

Watermark embedded by modifying pixel values.

- 变换域水印

Watermark embedded in transform domain.

DCT, DFT or wavelet.

Coefficients of global or block transform modified.

Terminology

- 鲁棒水印 Robust

  Against adversary based attack.

- 脆弱水印 Fragile

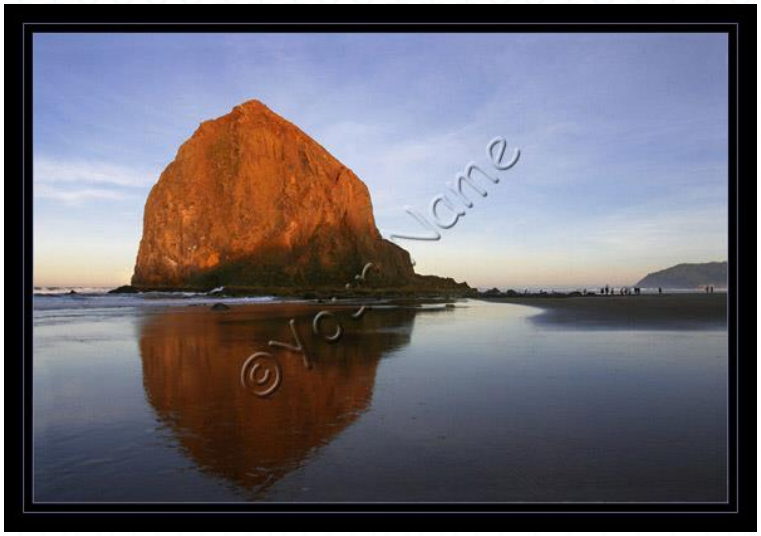
  For tamper proofing, e.g. losing watermark implies tampering.

- 半脆弱水印 Semi-Fragile

  Robust against user level operations, e.g. image compression.

Terminology

- 可见水印: Visible Watermarking



Terminology

- 不可见水印: Invisible Watermarking

Figure 1 : This example shows that digital watermarking allows to hide information in a totally invisible manner : the original image is on the left, the signed image is on the right.

Terminology

- 非盲检测 Non-blind detection

  Use the original signal.

- 盲检测 Blind detection

  Don’t use original signal or side information.

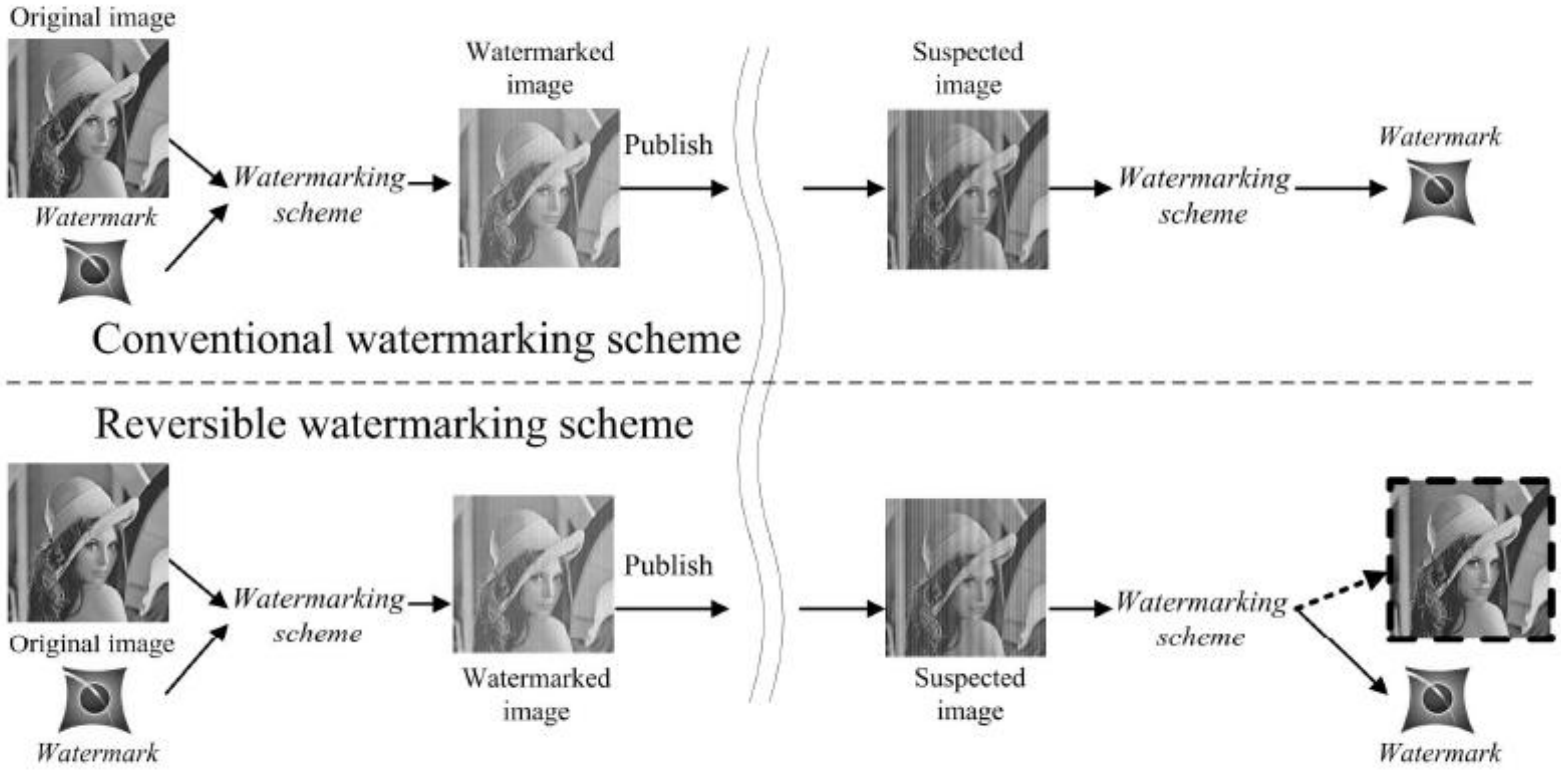
- 半盲检测 Semi-blind/Informed detection

  Don’t use the original signal,

  Use side information and/or original watermark.

Terminology

- 不可逆水印 Non-reversible
- 可逆水印 Reversible/Invertible/Lossless



Terminology

- 秘密通信 Secrete communication
- 广播监控 Broadcast monitoring
- 所有权识别 Owner identification
- 内容验证 Content authentication
- 叛逆者追踪 Traitor tracing
- 元数据嵌入 Metadata embedding
- 拷贝控制 Copy control

Attacks

- Signal enhancement (sharpening, contrast enhancement, etc.)
- Additive and multiplicative noise (gaussian, uniform, etc.)
- Filtering (High pass, low pass, linear, nonlinear, etc.)
- Lossy compression (JPEG, MPEG-x, H.26x, etc.)
- Geometric transforms (translation, rotation, etc.)
- Data reduction (cropping, clipping, etc.)
- Transcoding (MPEG2, H.263, etc.)
- D/A and A/D conversion (print-scan, etc.)
- Collusion attack
- Mosaic attack
- Ambiguity attack
- ……

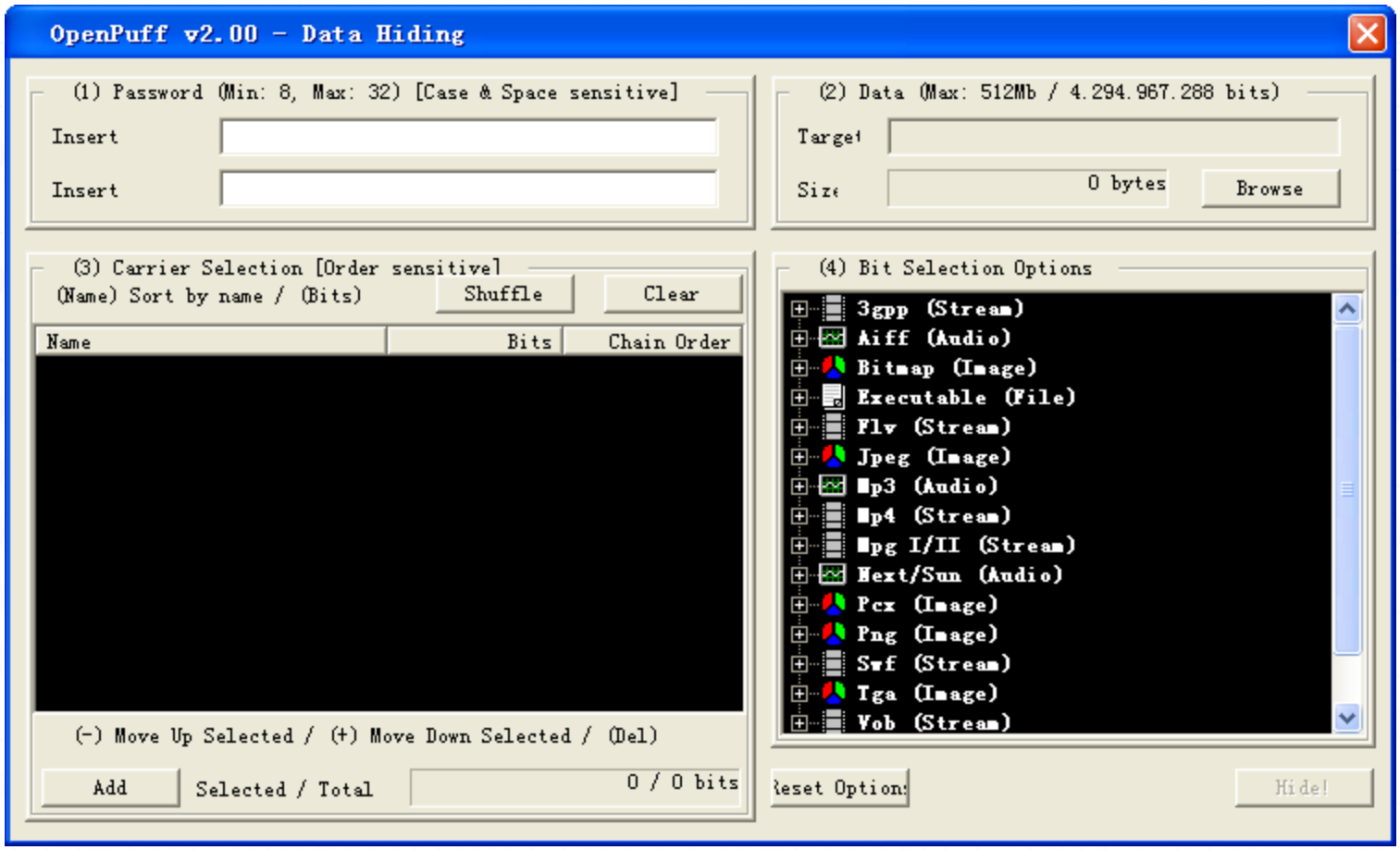
Mosaic Attack:

「 Part Five 」

Network Resources

Application Resources

PUFF V2.00 STEGANOGRAPHY & WATERMARKING



Application Resources

S-Tools: BMP_file_format, Gif, Wav, unused floppy disk space

MP3Stego: Mp3

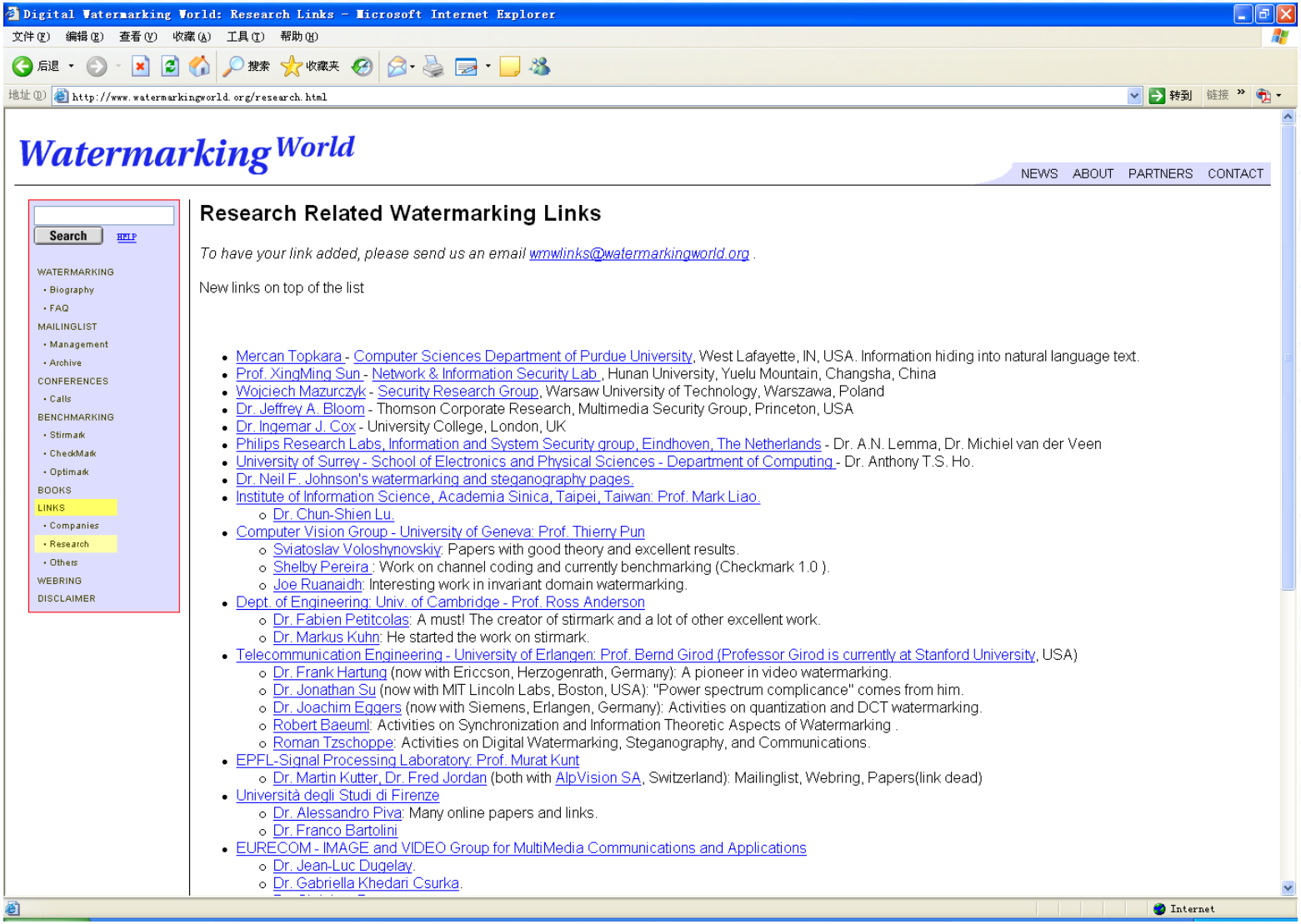
Invisible Secrets: BMP_file_format, Portable_Network_Graphics, Jpg, Wav, Html

StegFS: Steganographic_file_system

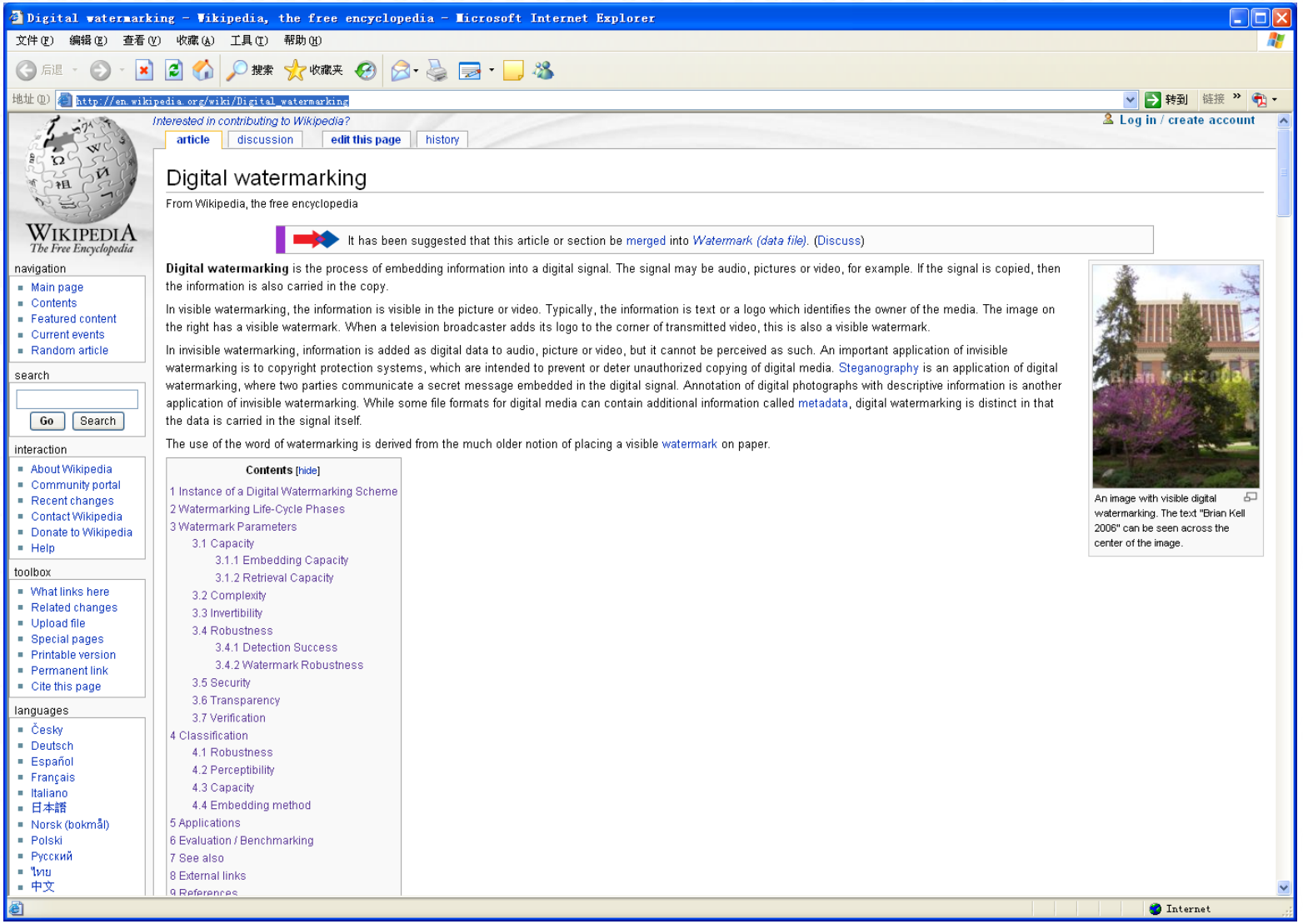
Steganography tools

PhilProxy PNG Steganography

Internet Resource



Internet Resource



Internet Resource

- ftp://skynet.ecn.purdue.edu/pub/dist/delp/watermark-proceedings/paper.pdf
- http://www.cosy.sbg.ac.at/~pmeerw/Watermarking/
- http://www.cosy.sbg.ac.at/~pmeerw/Watermarking/MasterThesis/
- http://www.eso.org/projects/esomidas/doc/user/98NOV/volb/node308.html
- http://www.jjtc.com/Steganography/
- http://www.mathworks.com/matlabcentral/files/3508/digital%20watermarking.pdf
- Mihcak, Mehmet Kivanc. “Information Hiding Codes and Their Applications to Images and Audio”, PhD Thesis. 2002.

- http://en.wikipedia.org/wiki/Steganography
- http://en.wikipedia.org/wiki/Digital_watermark
- http://www.cypak.com/pictures/med/Cypak%20microchip.jpg

Thank you!