

Lecture 1-2.

Information Hiding Technologies

Hui Wang

School of Cyberspace
Hangzhou Dianzi University

2018-2019 Academic Year – 2nd Semester
February 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** (Steegeo-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:

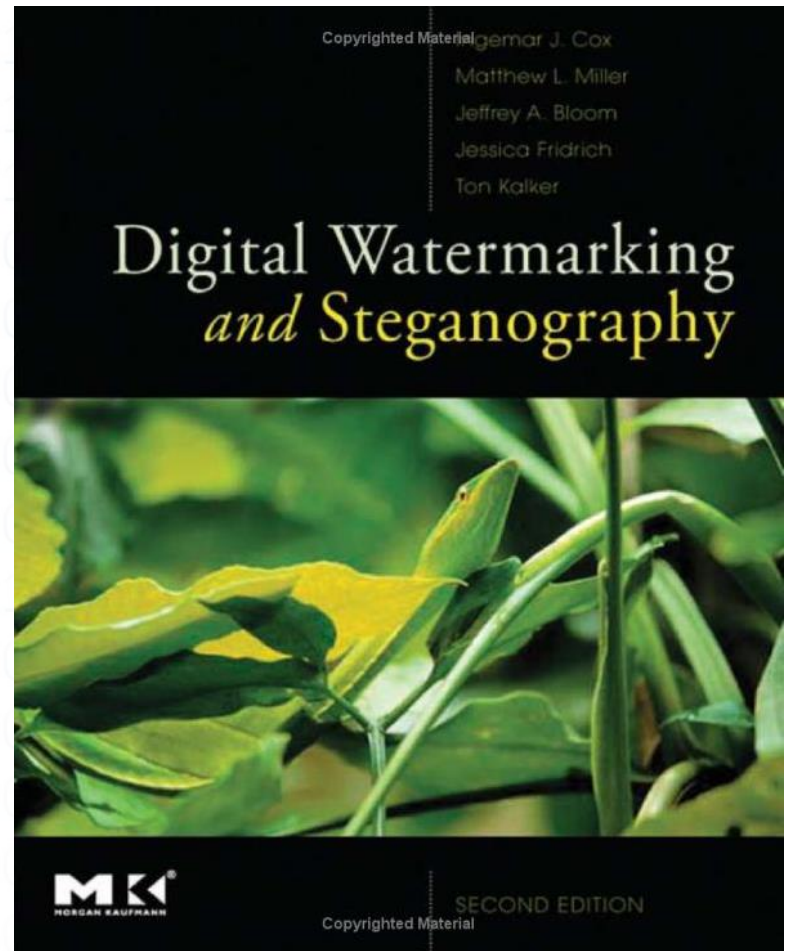
- Learn the basic mathematical concept behind watermarking theory (The prisoners Problem) and its main applications
- The mathematical limits of Watermarking and different analysis techniques for such limits
- Different commercial and e-commerce protocols of Digital watermarking

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等编著，2003
- III. 信息隐藏技术与应用，王丽娜等编著，2012
- IV. 信息隐藏与数字水印，钮心忻著，2004

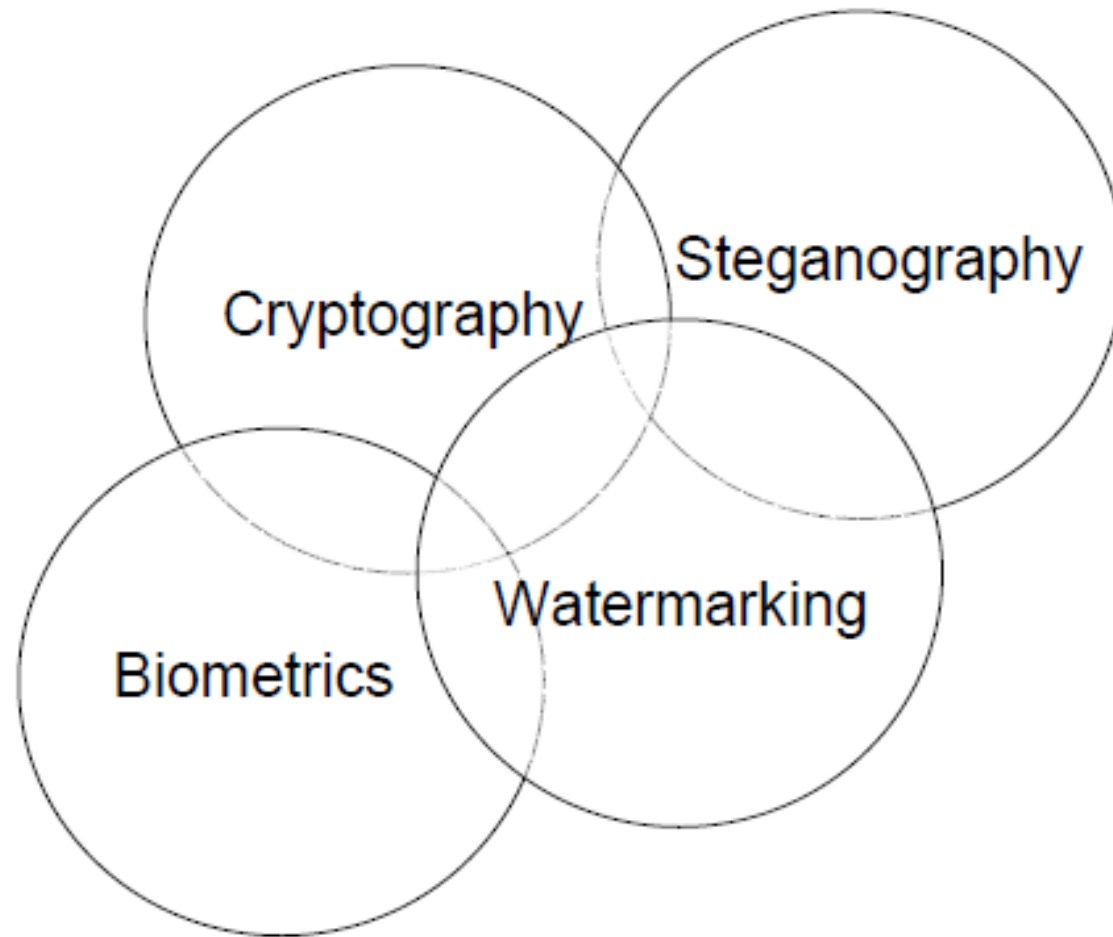


「 Part One 」



Introduction

Multimedia Security



Steganography Topics

❖ What is Steganography?

– Cryptography vs Steganography vs Watermarking

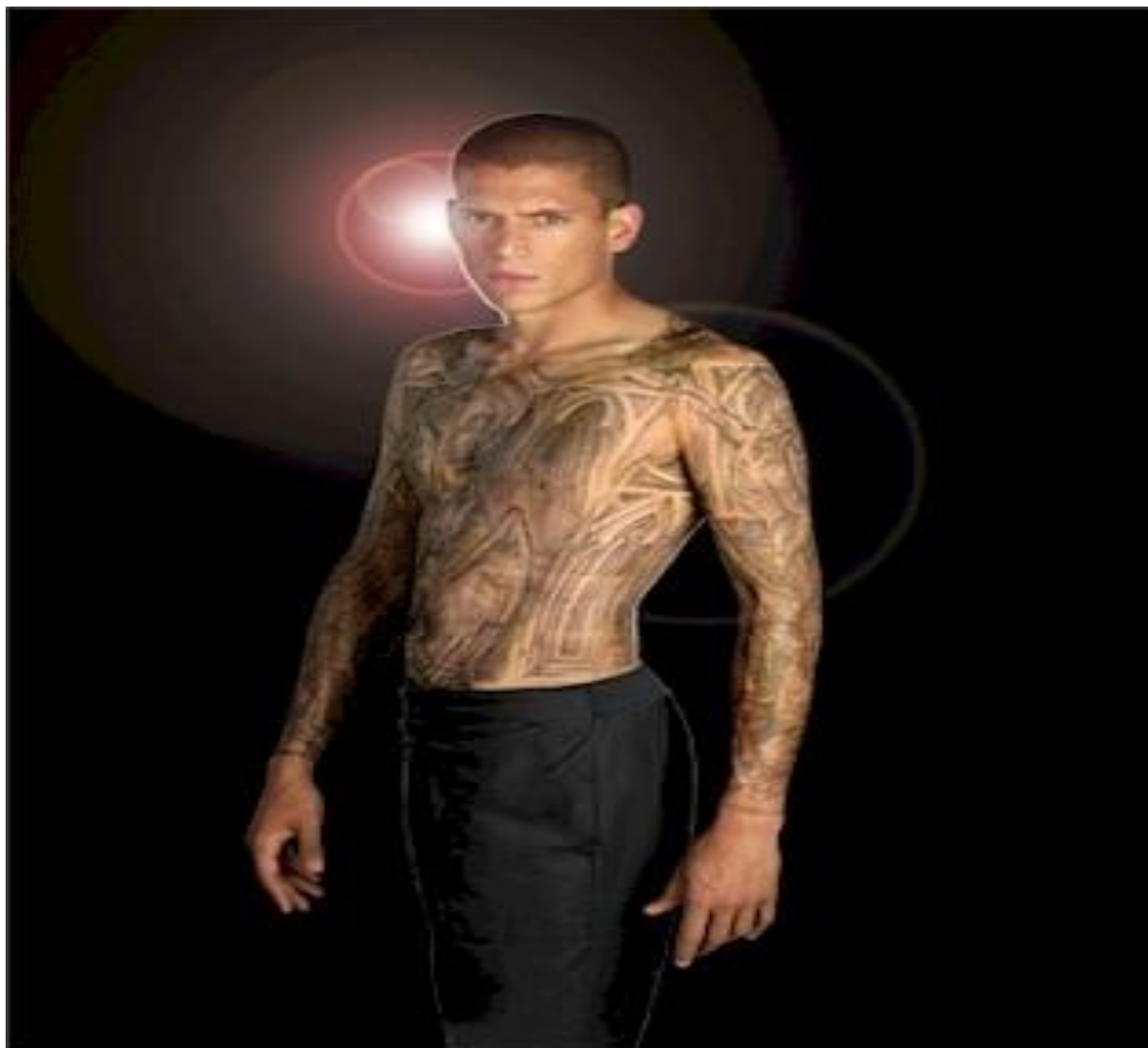
- Why Steganography?

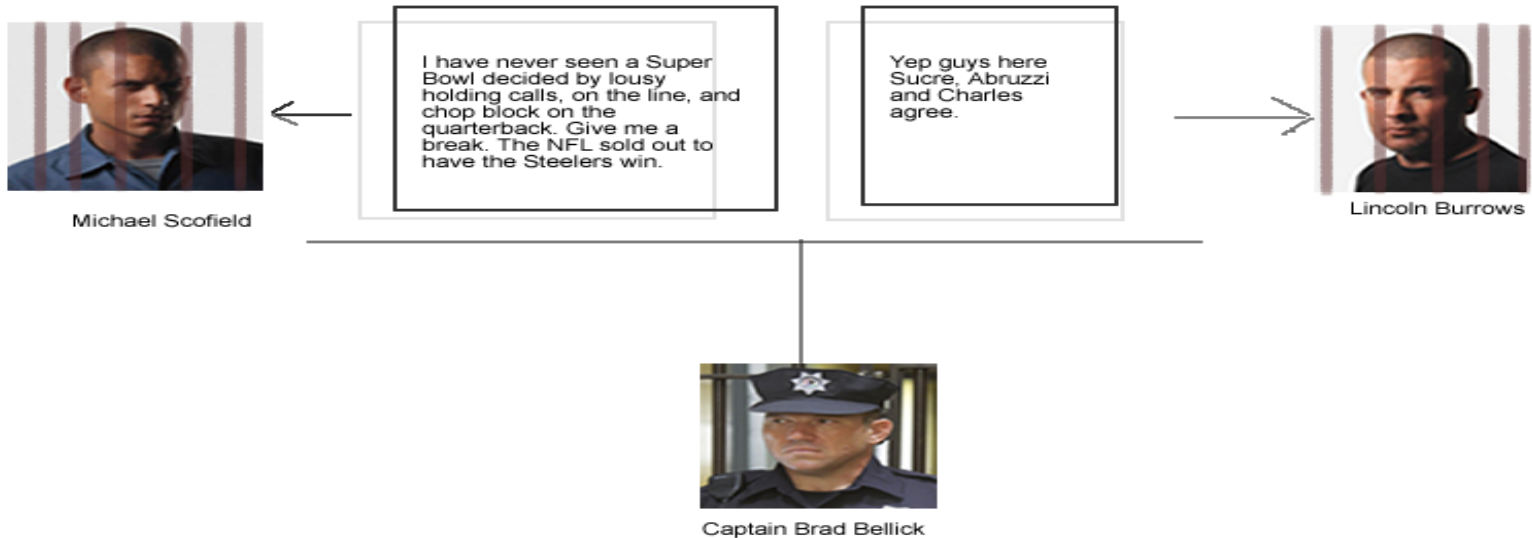
- Steganography Classes and Methods

 - 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



+

101101011010101010
100101000101101101
101010100101011010
101011110000101010
100101110101101011
010100101001000010
011101010011110110
111101110111010001

=



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

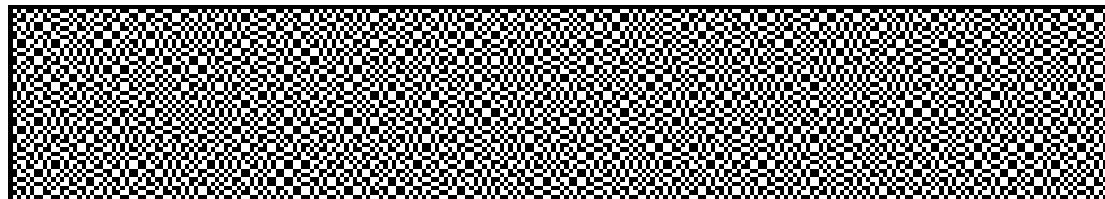


Steganography

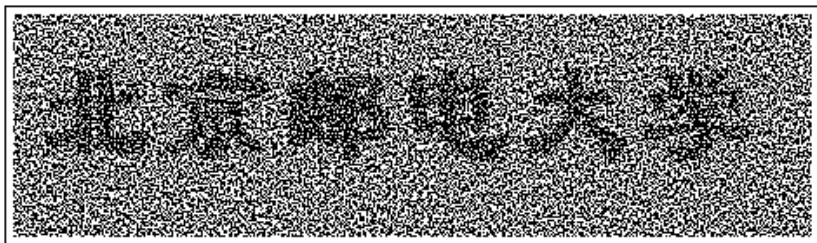
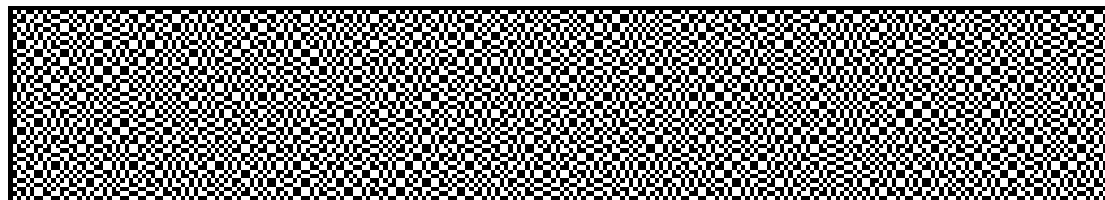
(Contains embedded encrypted message)

Visual Cryptography

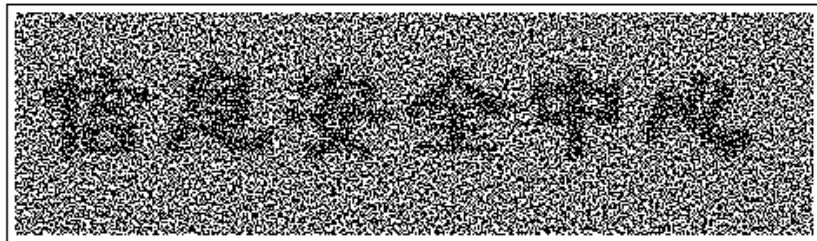
share 1



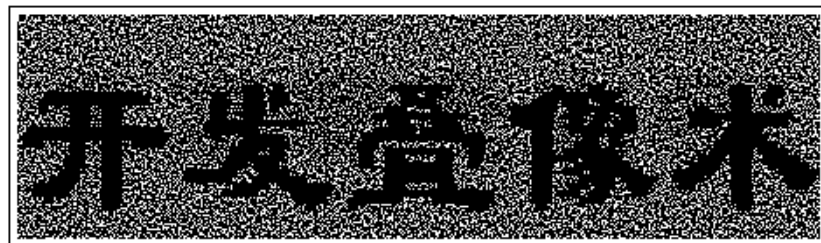
share 2



p1 “北京邮电大学”



p2 “信息安全中心”

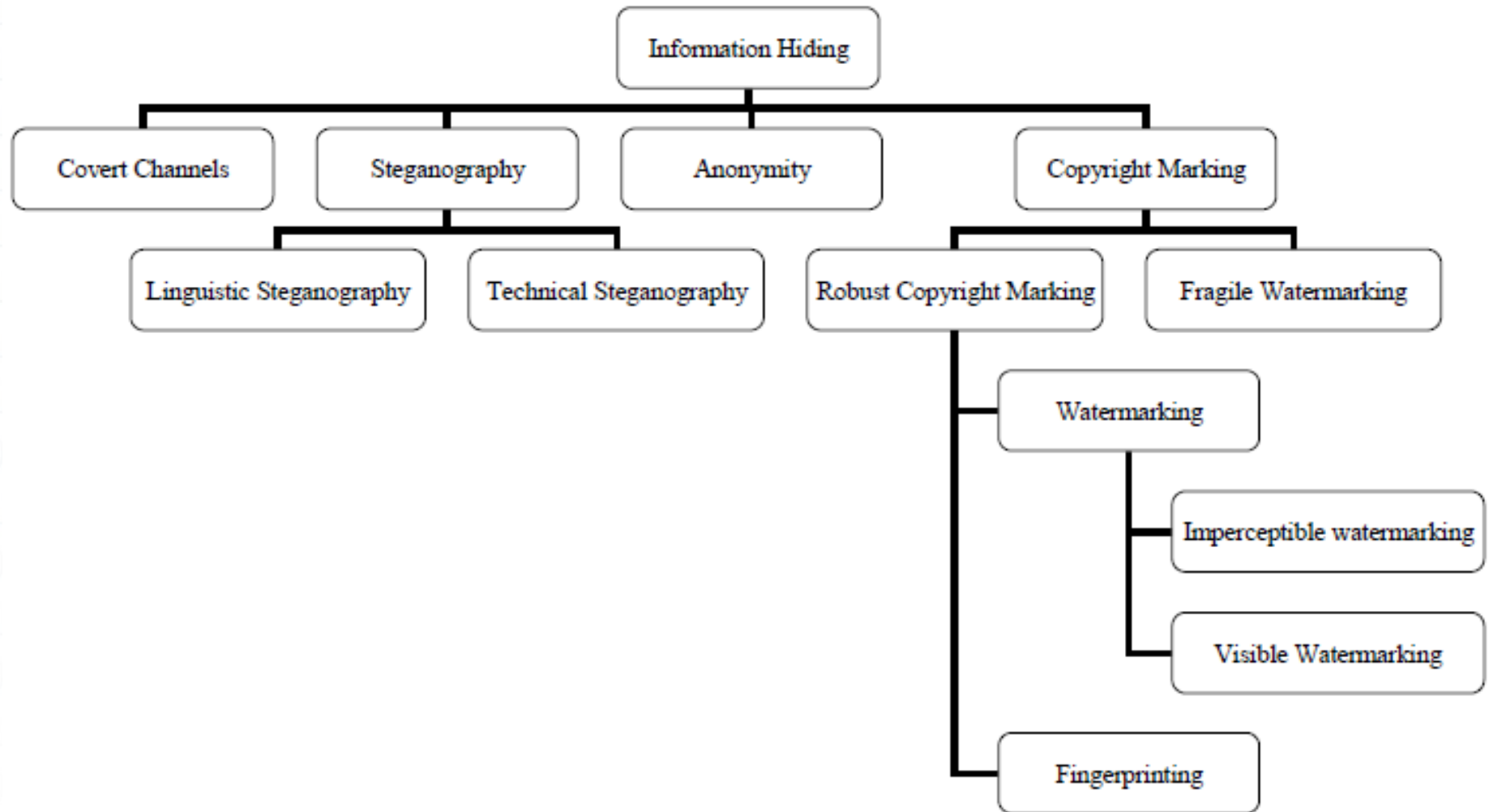


$p3 = p1 + p2 = \text{“开发叠像术”}$

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

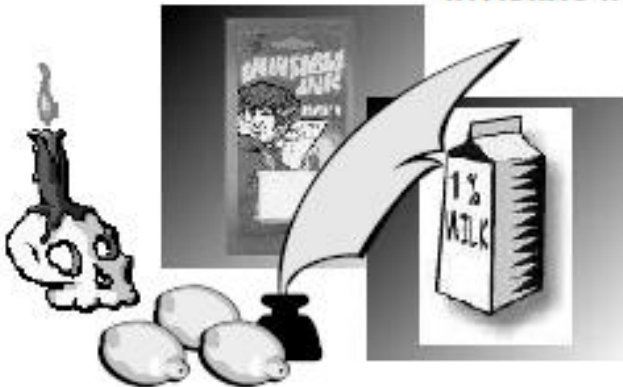


Trithemius,
Steganographia,
1606



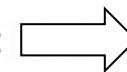
Gaspari Schotti,
*Schola
Steganographica*,
1665

Invisible Inks



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

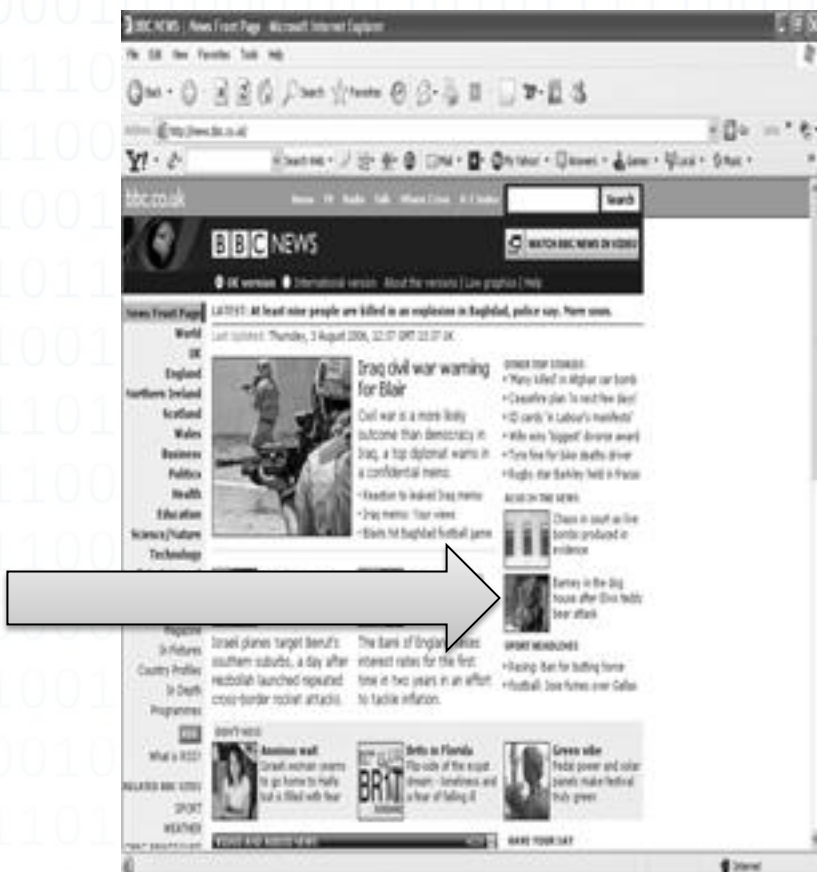
- Hidden Message (Leaf Insect, Chameleon)
- Container (Leaves, Surrounding)

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



COMPANY SECRETS

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

To the Members of the California State Assembly:

I am returning Assembly Bill 1176 without my signature.

For some time now I have lamented the fact that major issues are overlooked and unnecessary bills come to me for consideration. Water reform, prison reform, care are major issues my Administration has brought to the table, but the Governor keeps the can down the alley.

Yet another legislative year has come and gone without the measure overwhelmingly deserve. In light of this, and after careful consideration, it is unnecessary to sign this measure at this time.

Sincerely,

Arnold Schwarzenegger



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 Protection:

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



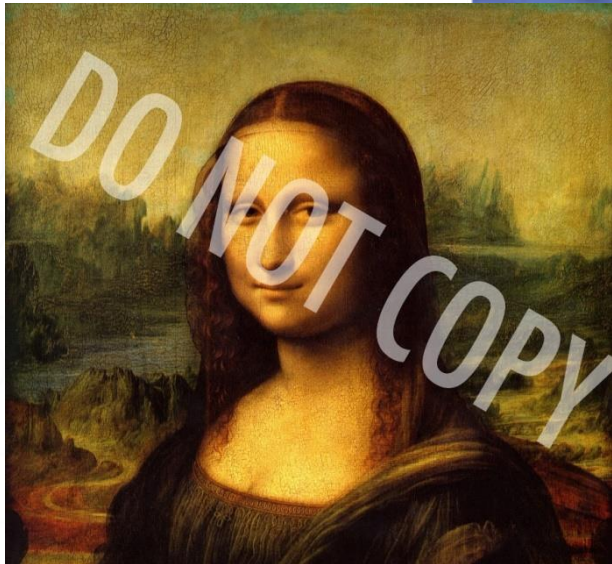
Why Watermark?



Watermark



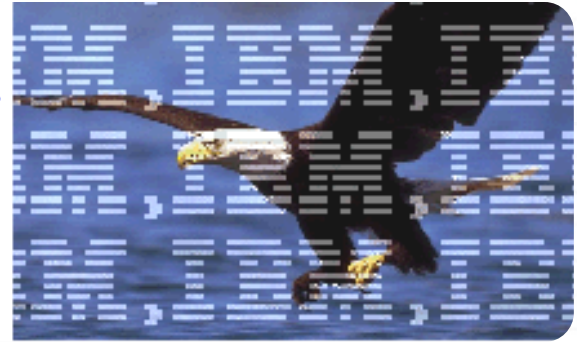
Image with watermark



Embed

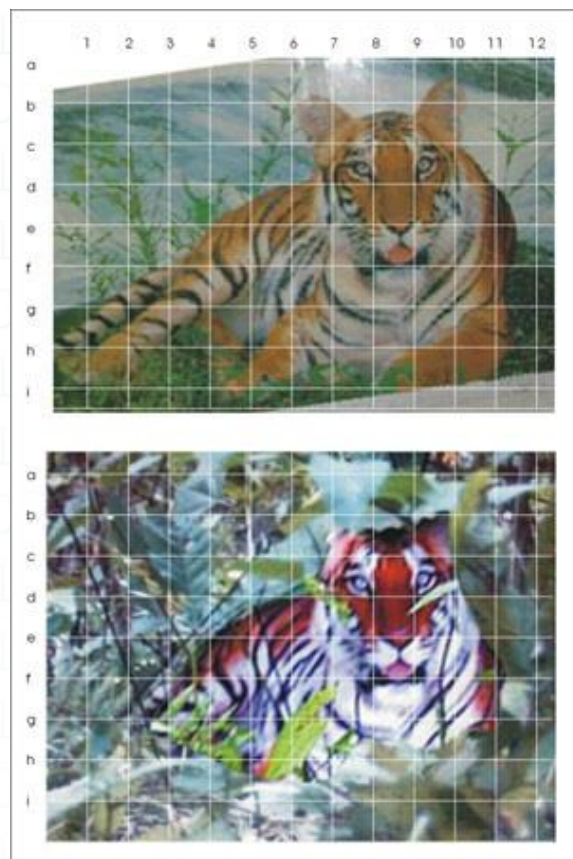


Remove

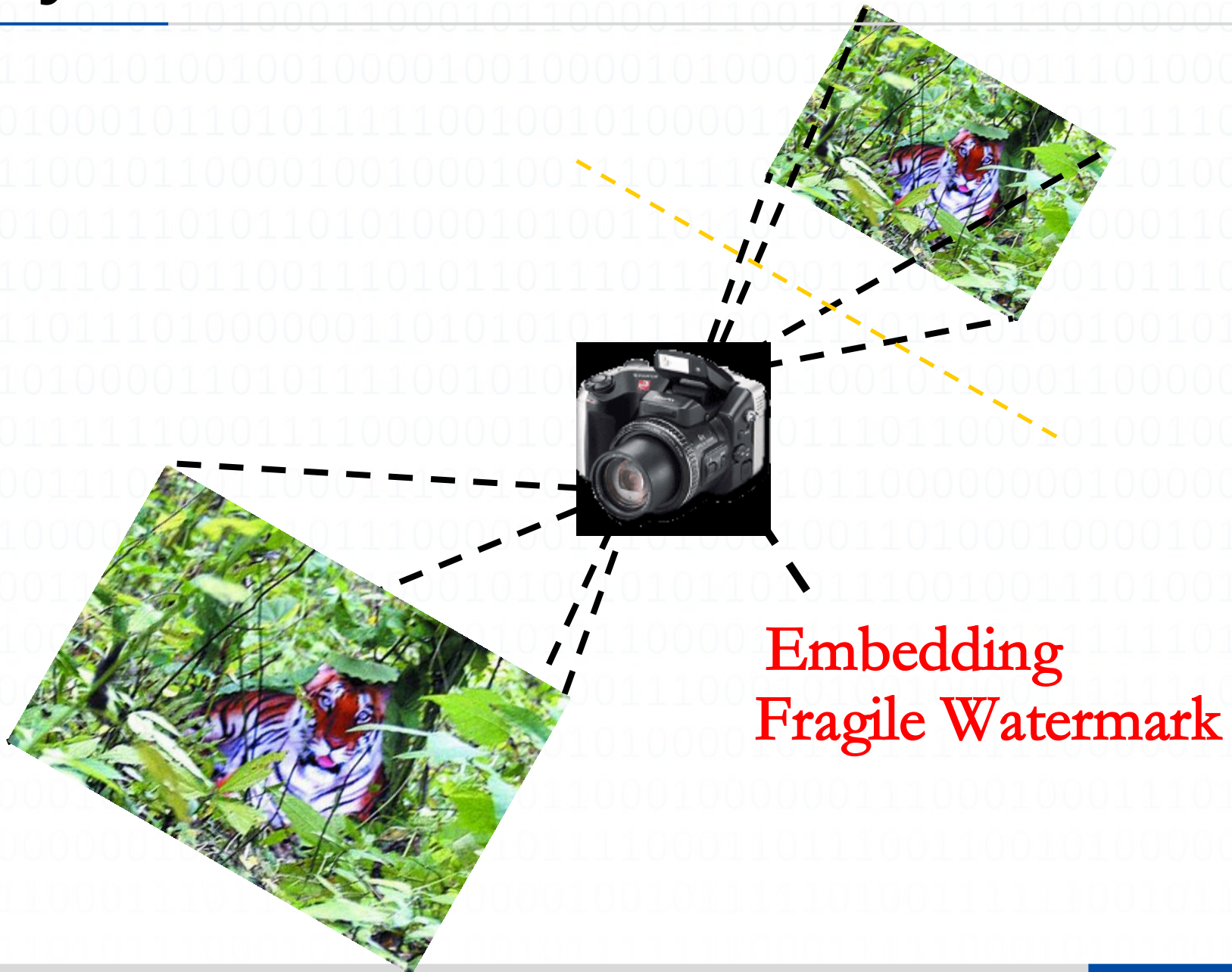


Why Watermark?

The authenticity of the news report:



Why Watermark?



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 ...



「 Part Two 」



IH Technologies

Why is it available?



Using Human Visual Redundancy



Using Redundancy of a Computer Processing System

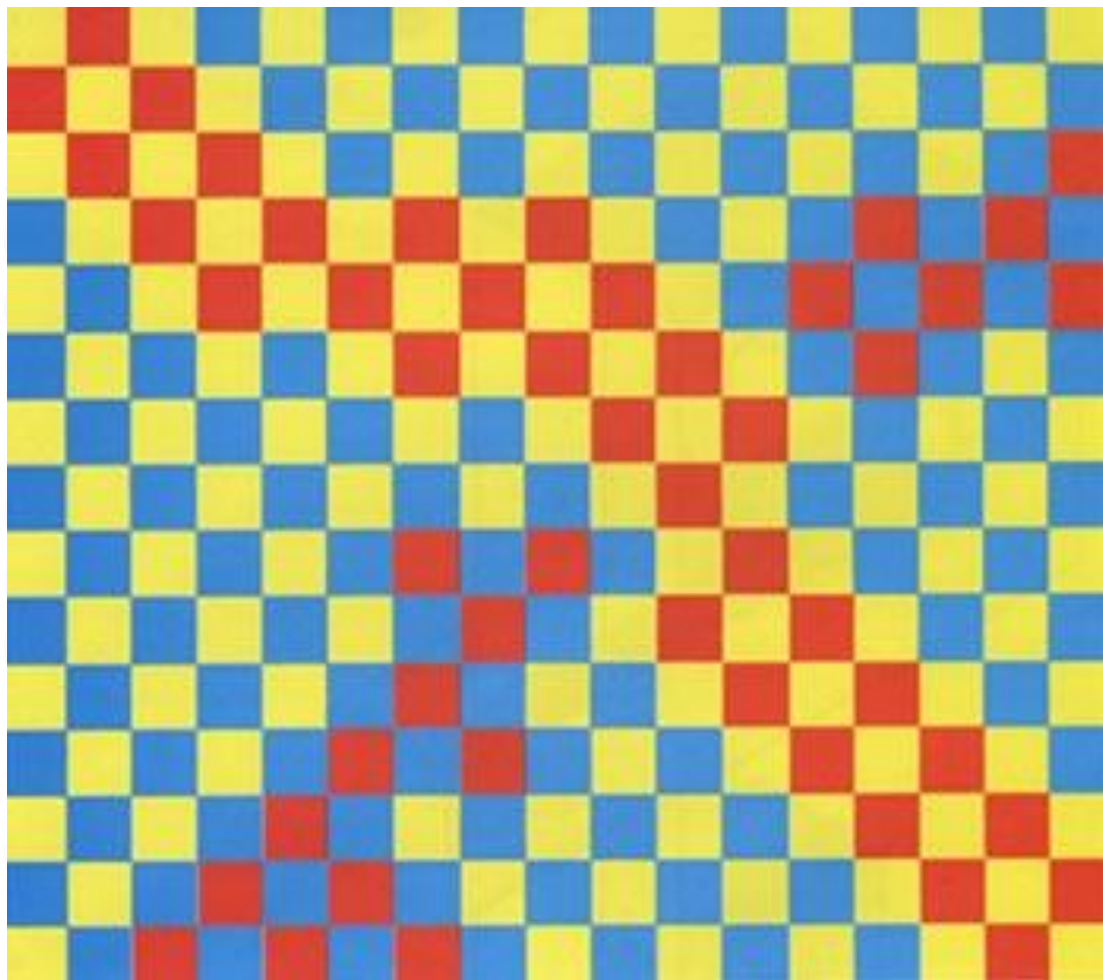


Based on Subliminal Channel Theory

It is feasible in technology!

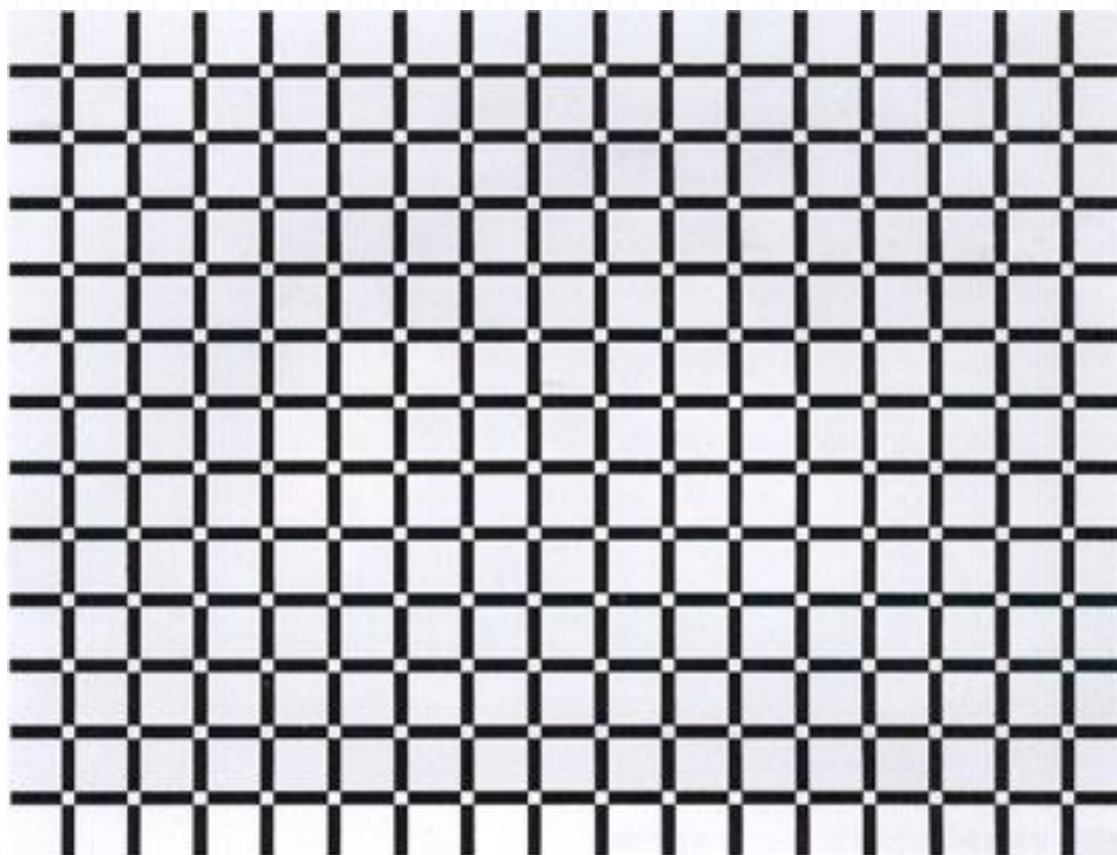
Human Visual Redundancy

比泽尔德幻觉：图中所有的红色看起来都一样吗？



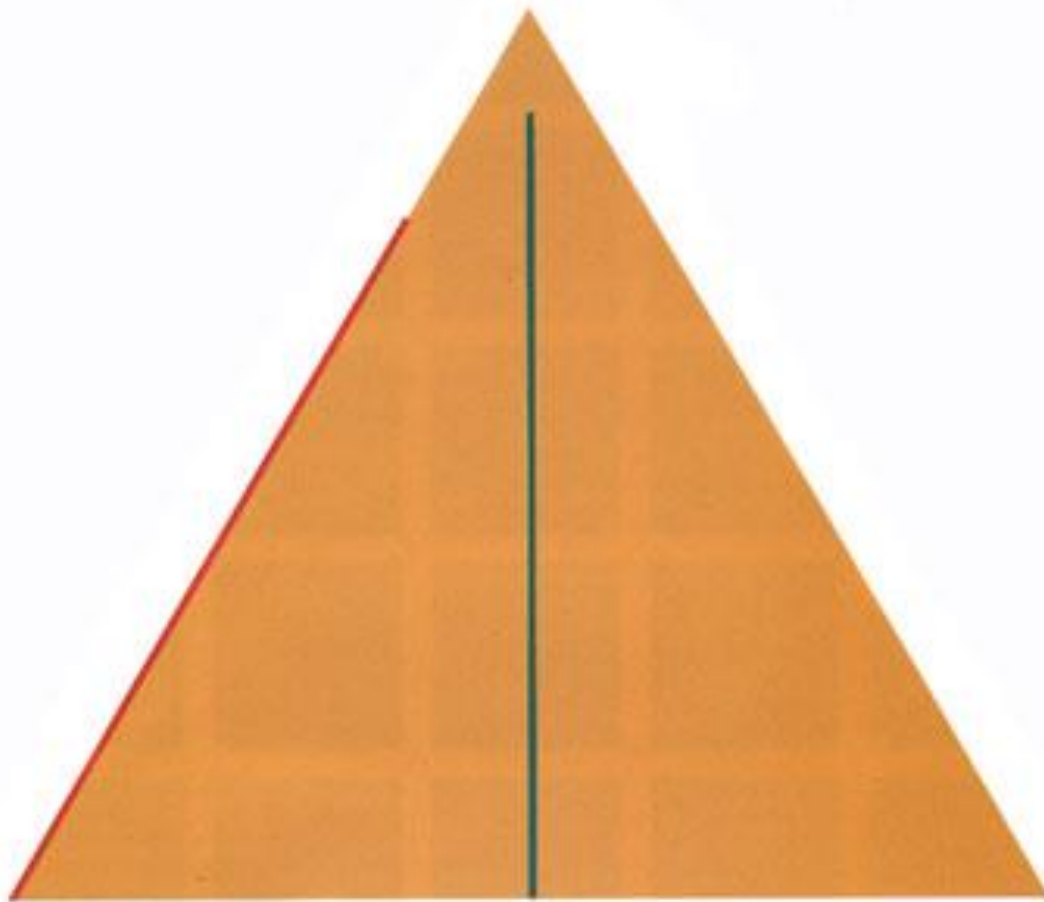
Human Visual Redundancy

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？



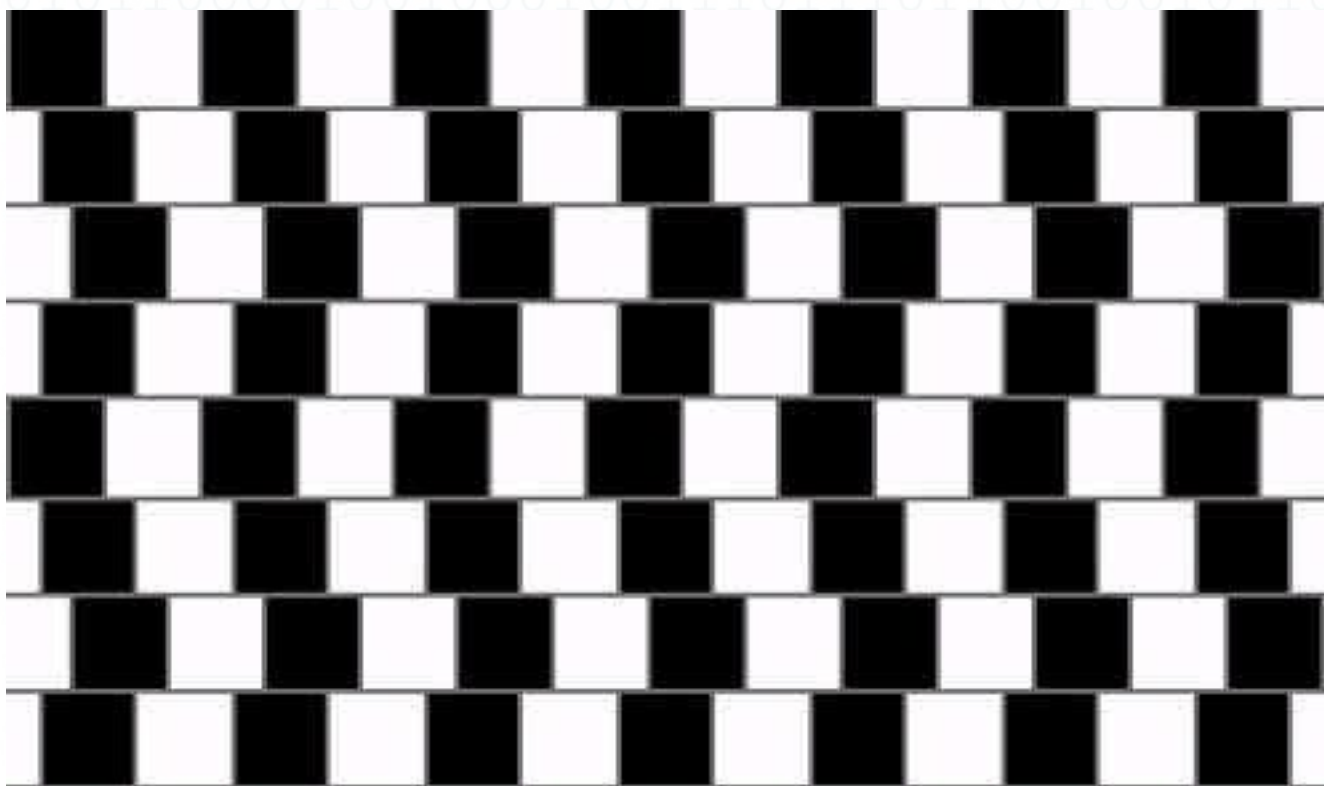
Human Visual Redundancy

这只动物驴子还是海豹？



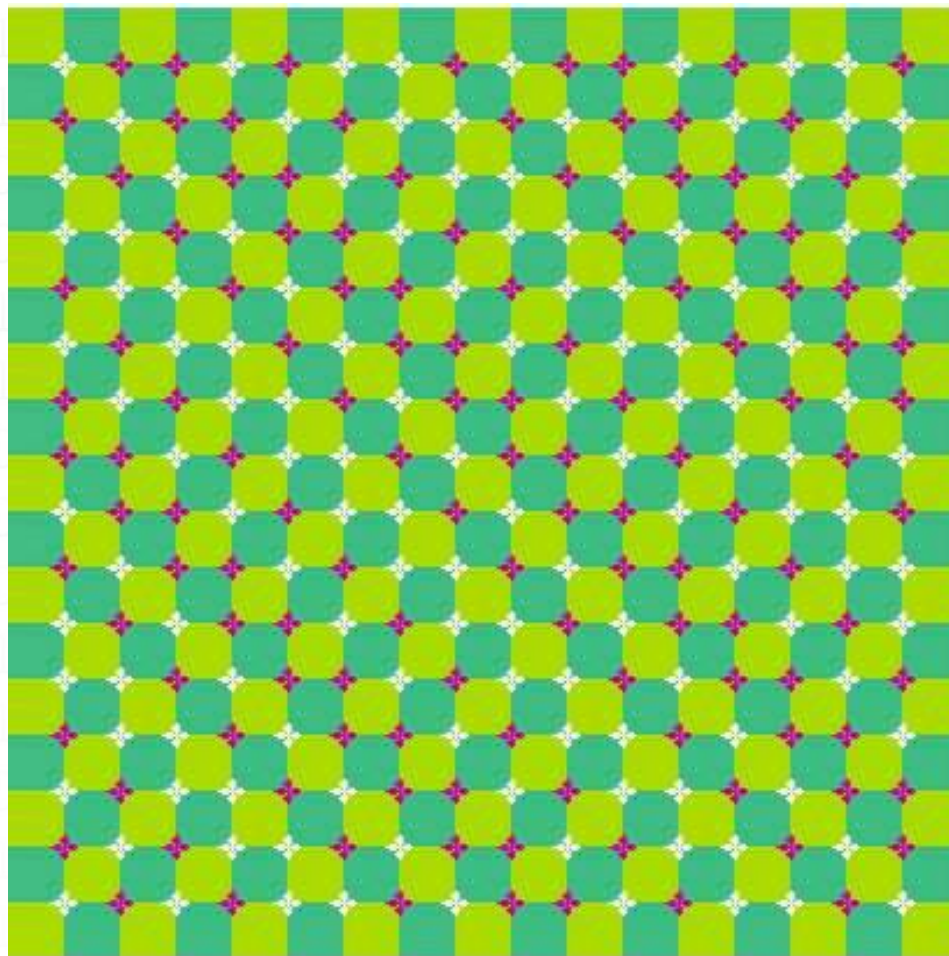
Human Visual Redundancy

不可思议平行线



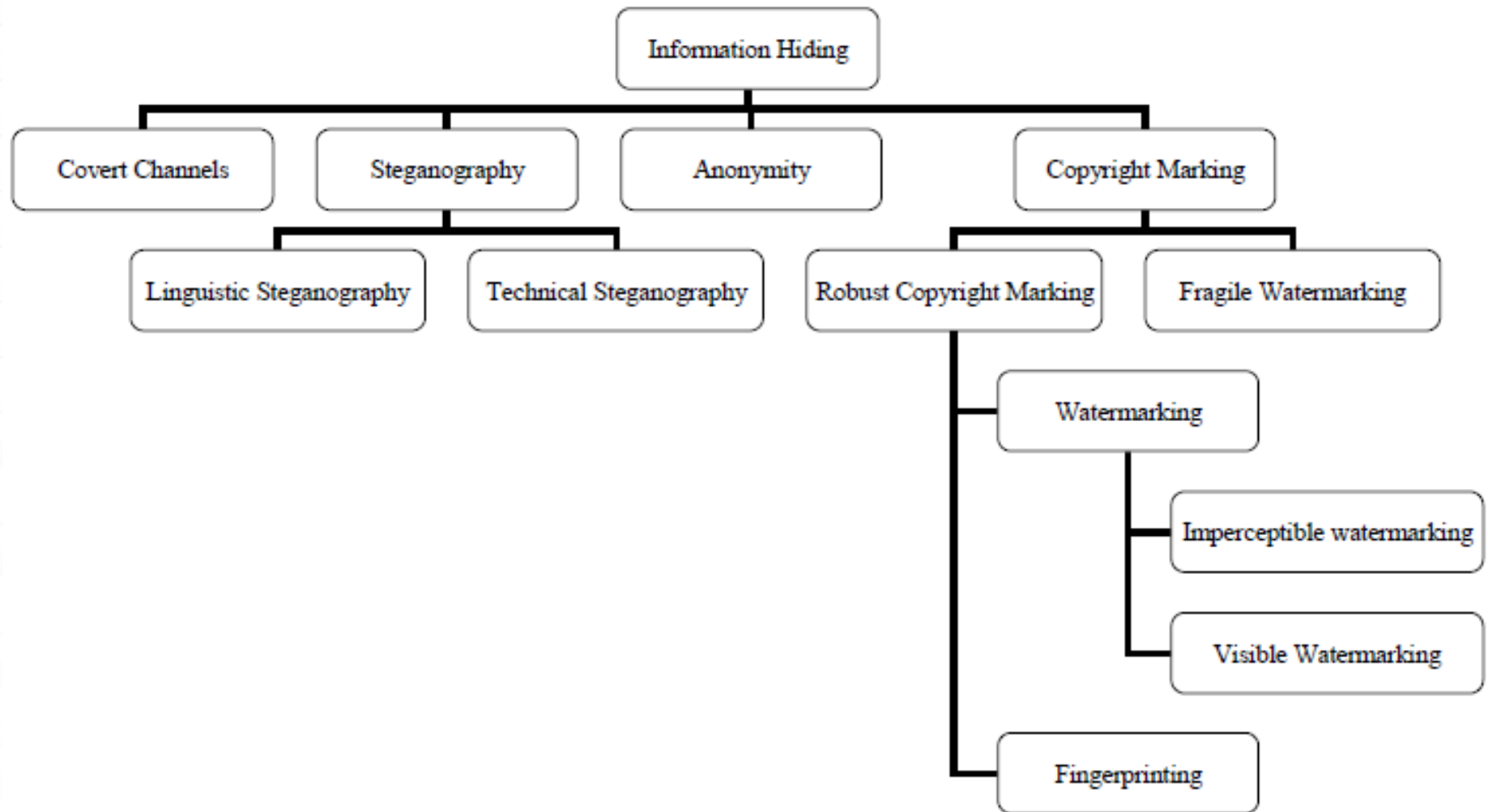
Human Visual Redundancy

- 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

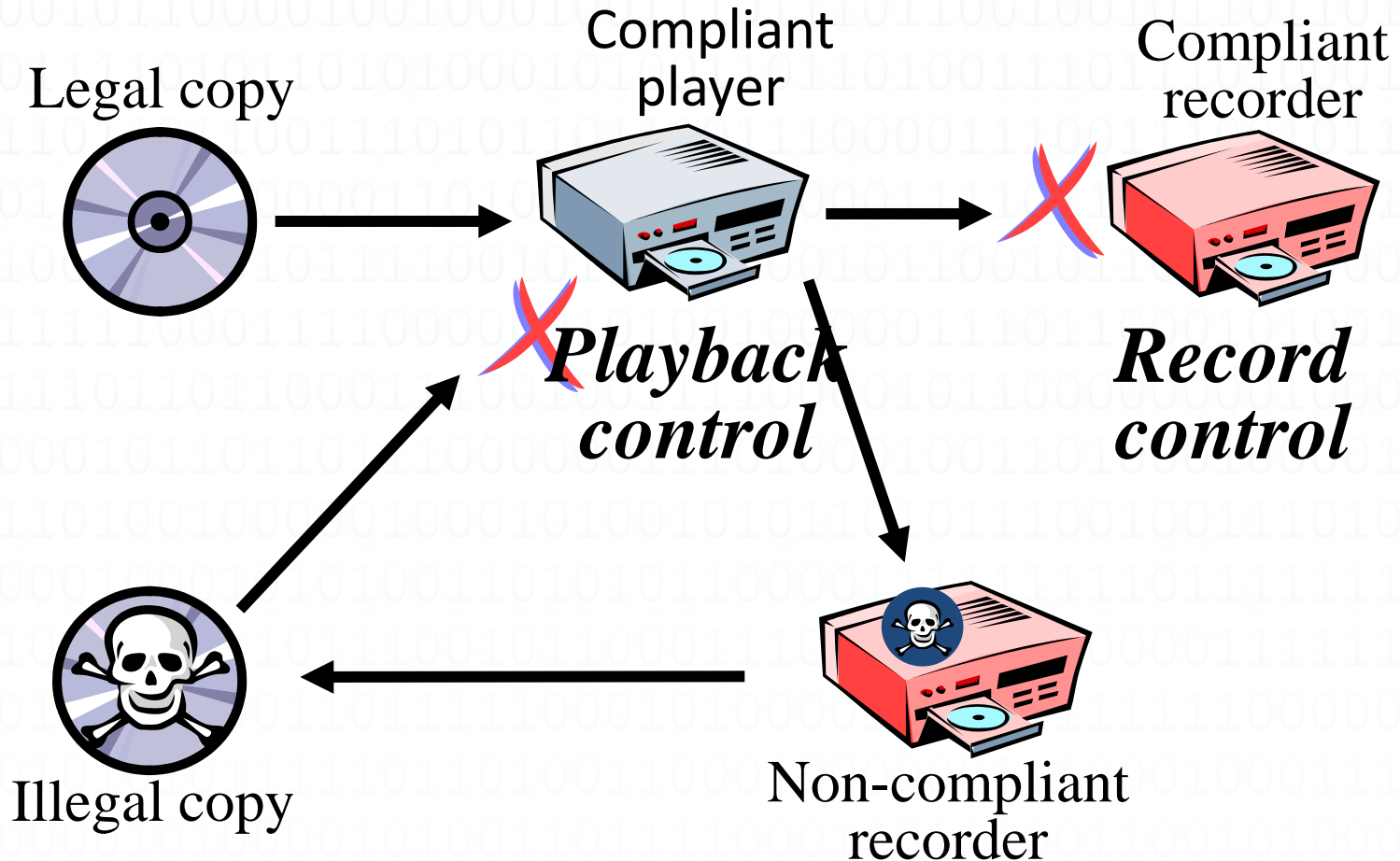
Invisible watermarks are preferred

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

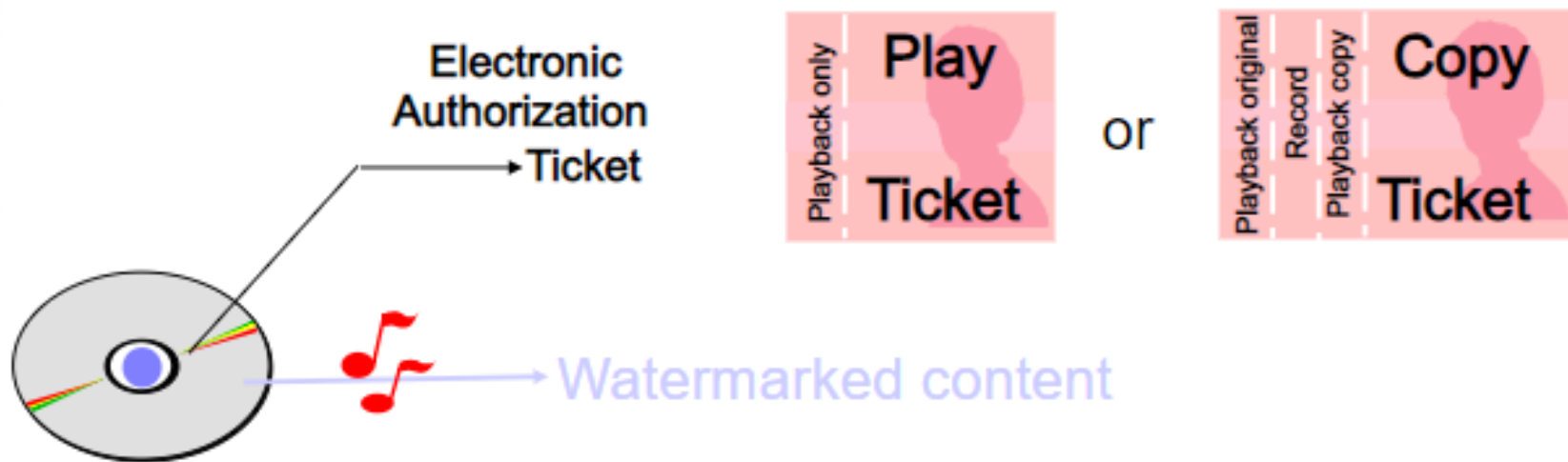
Applications of Digital Watermarking

- Copy Control


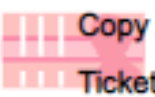



Applications of Digital Watermarking

Play Control

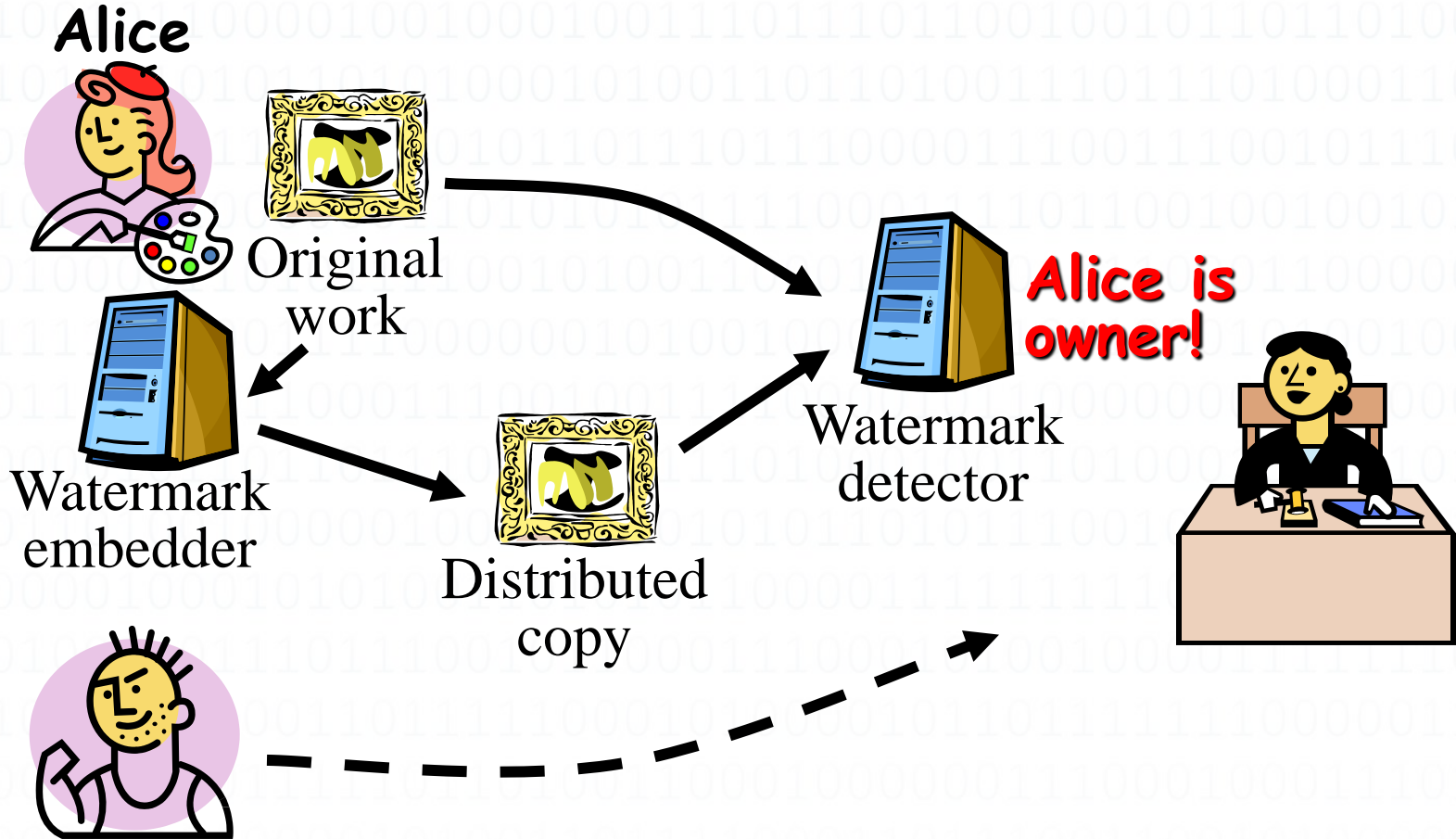


Record / playback ONLY if

 +  : Watermark matches with valid ticket
or  : Free-Copy: No Watermark

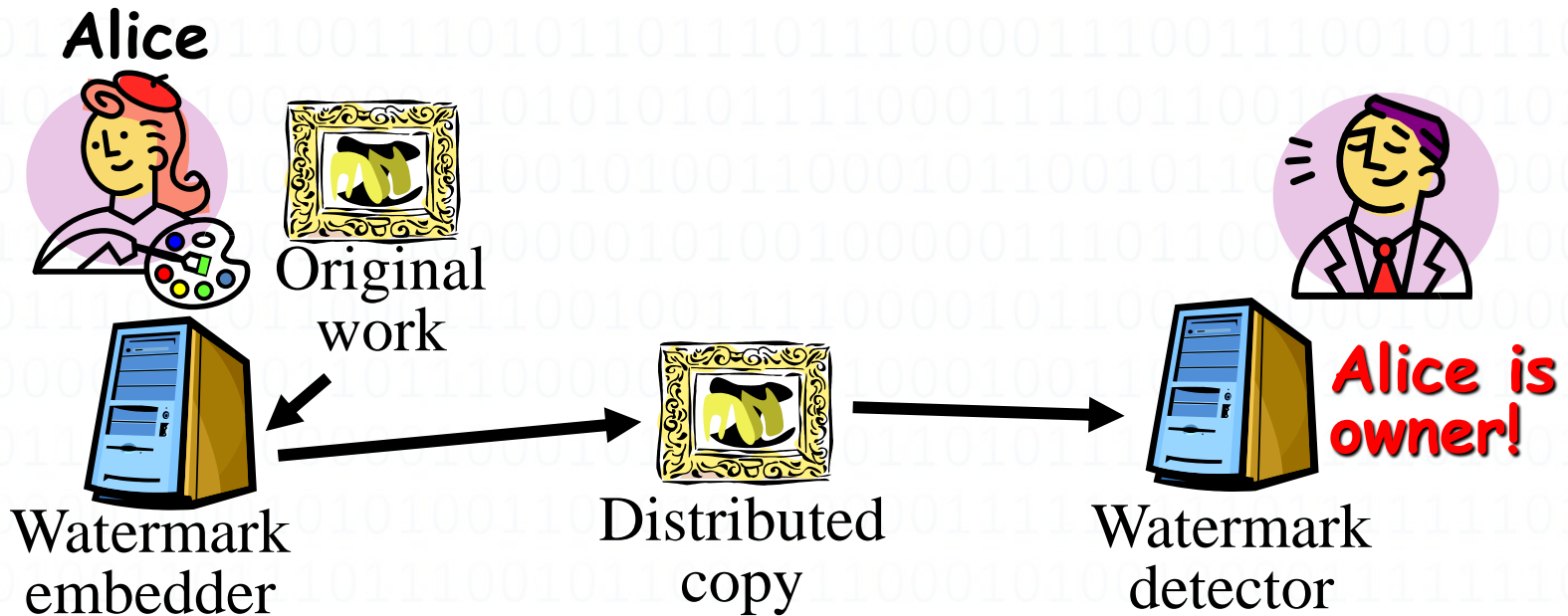
Applications of Digital Watermarking

- Proof of ownership



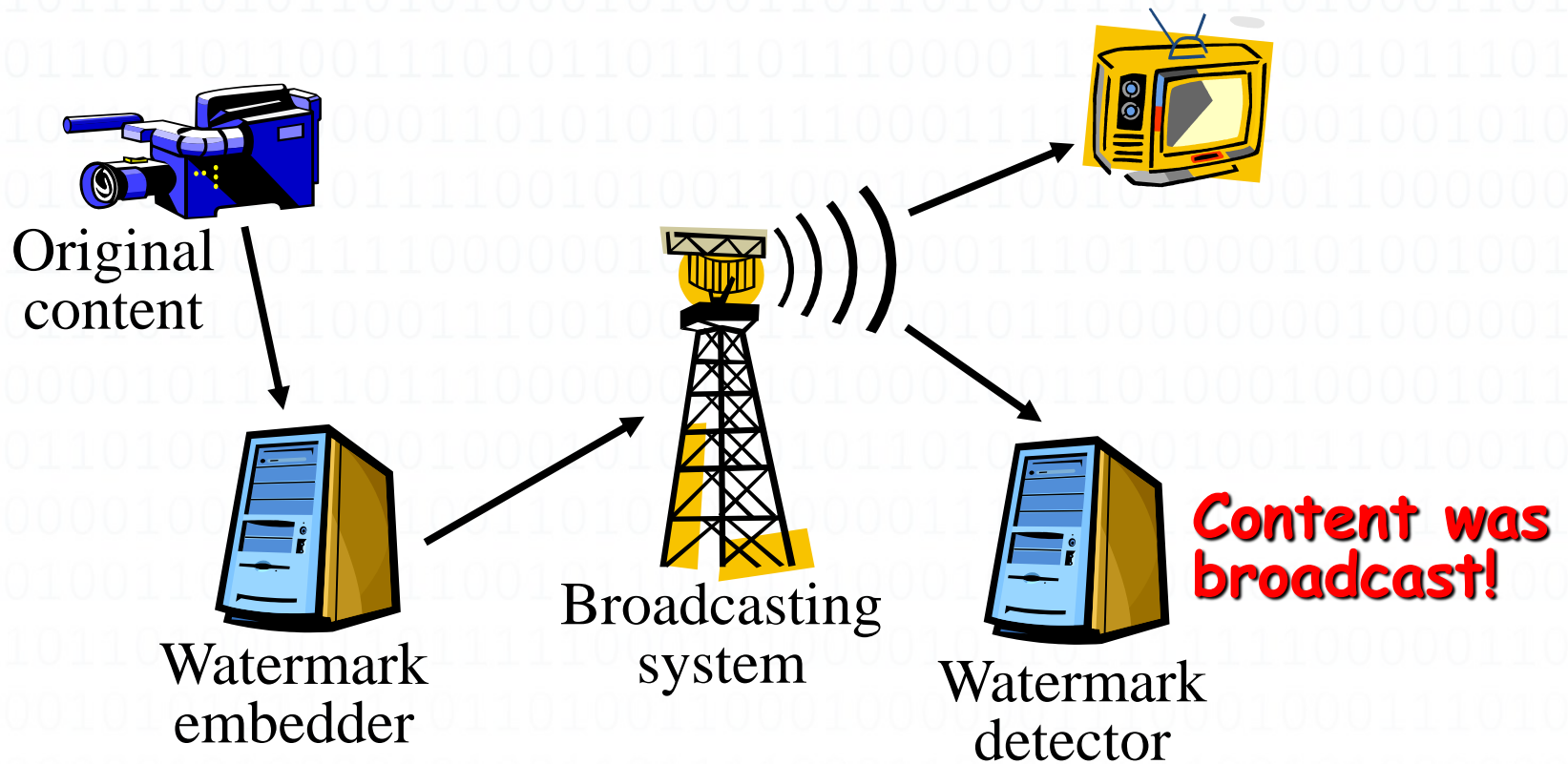
Applications of Digital Watermarking

- Owner identification



Applications of Digital Watermarking

- Broadcast Monitoring



Applications of Digital Watermarking

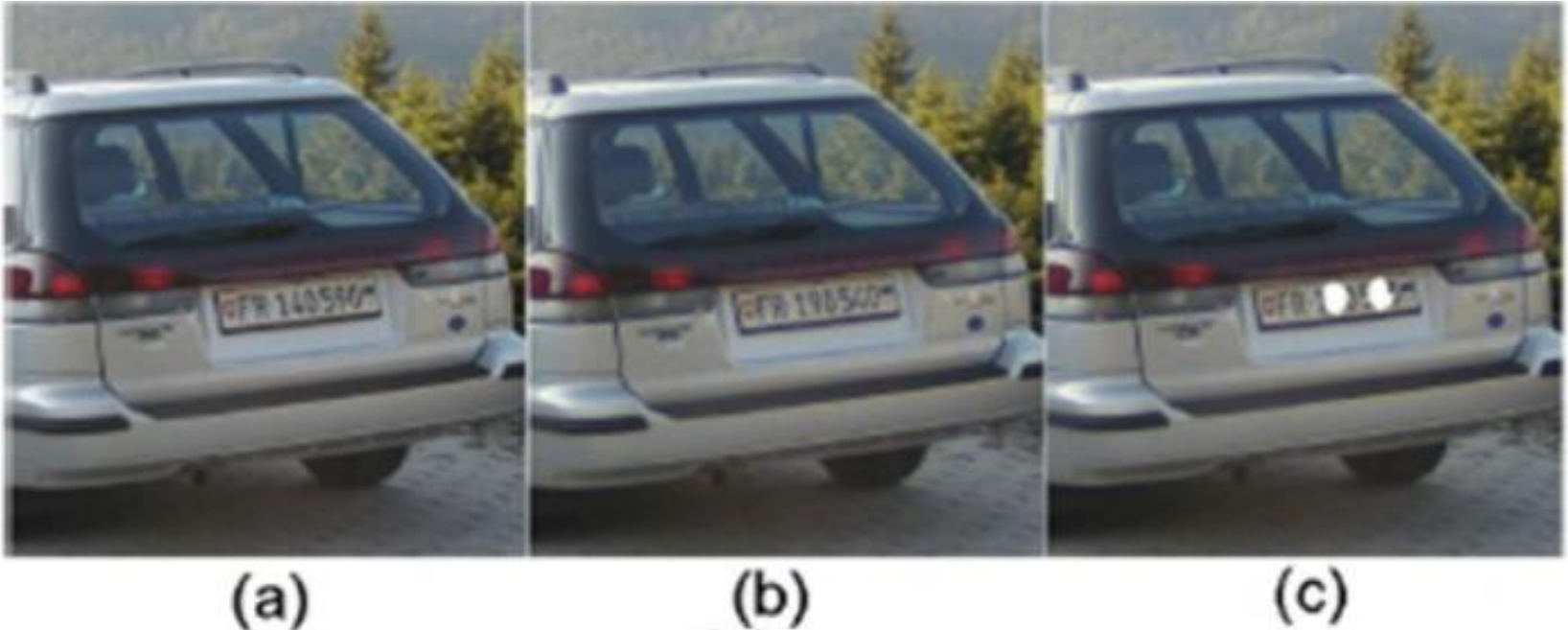


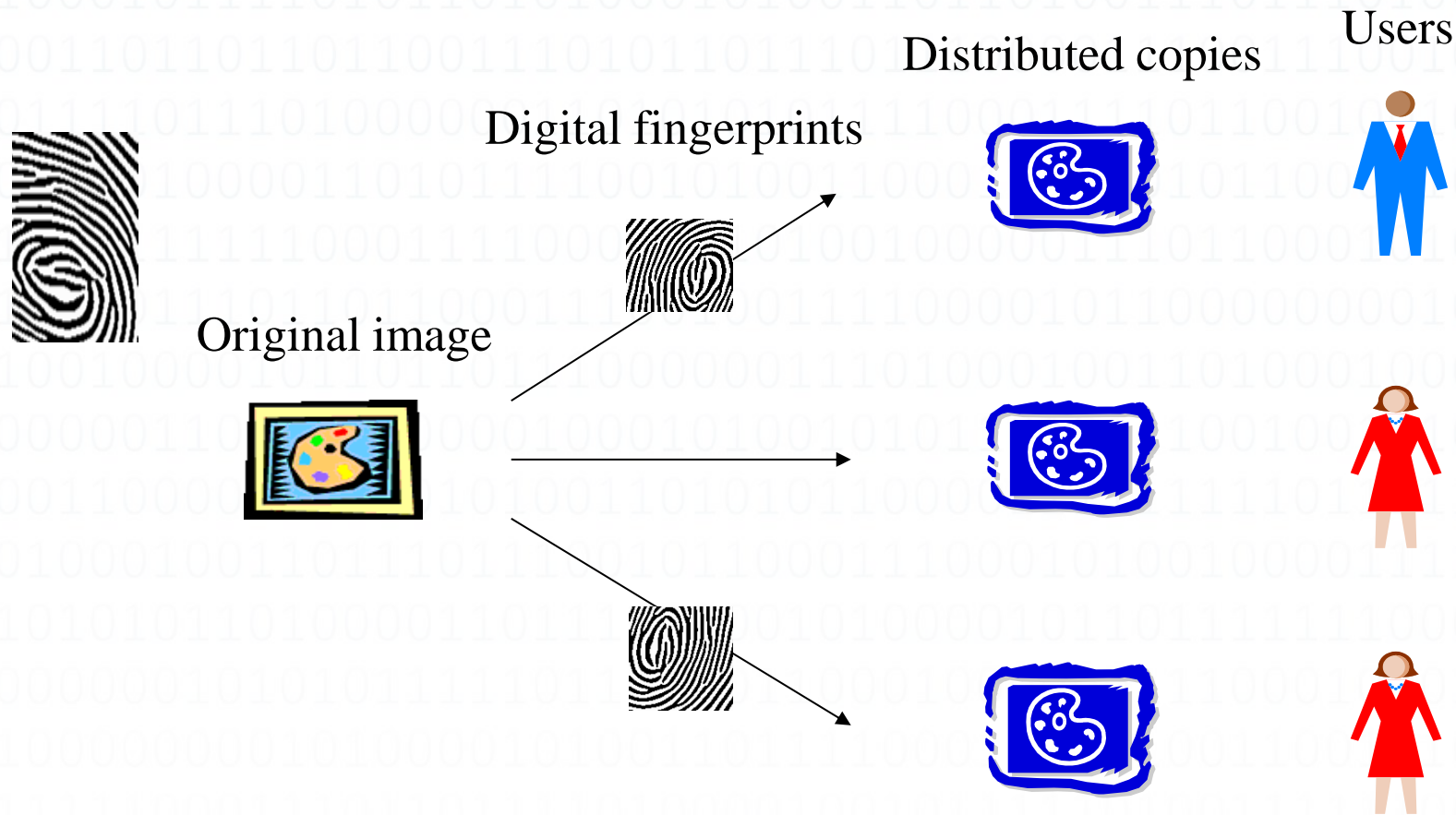
Figure : Using digital watermarks for integrity verification. The protected image is on the left. A modified image is obtained by swapping the numbers 9 and 4. Watermarking technology allows to detect and highlights the modified areas, as shown on the right.

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



PA

Applications of Digital Watermarking



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

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

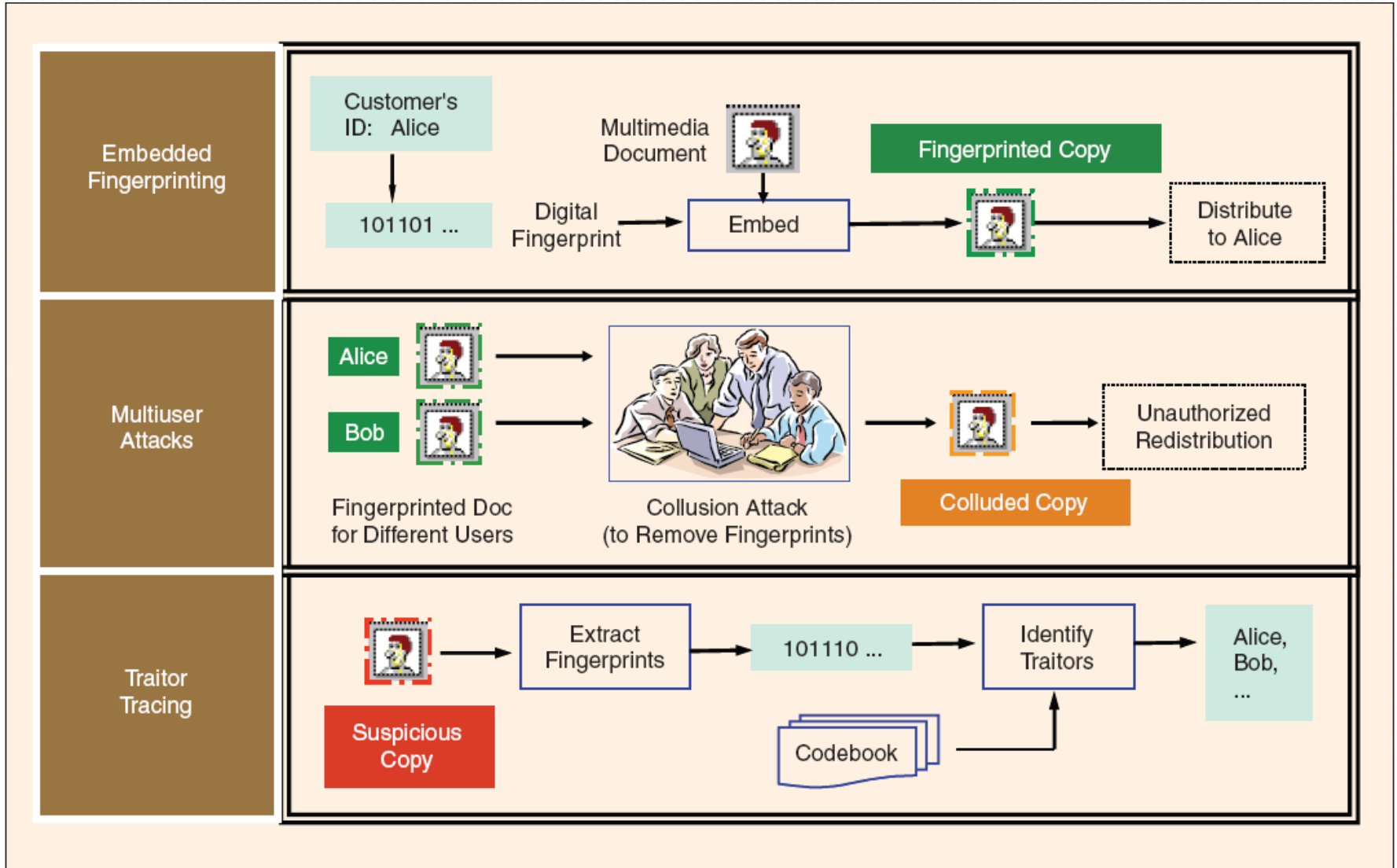


Now is the time for all men/women to ...

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

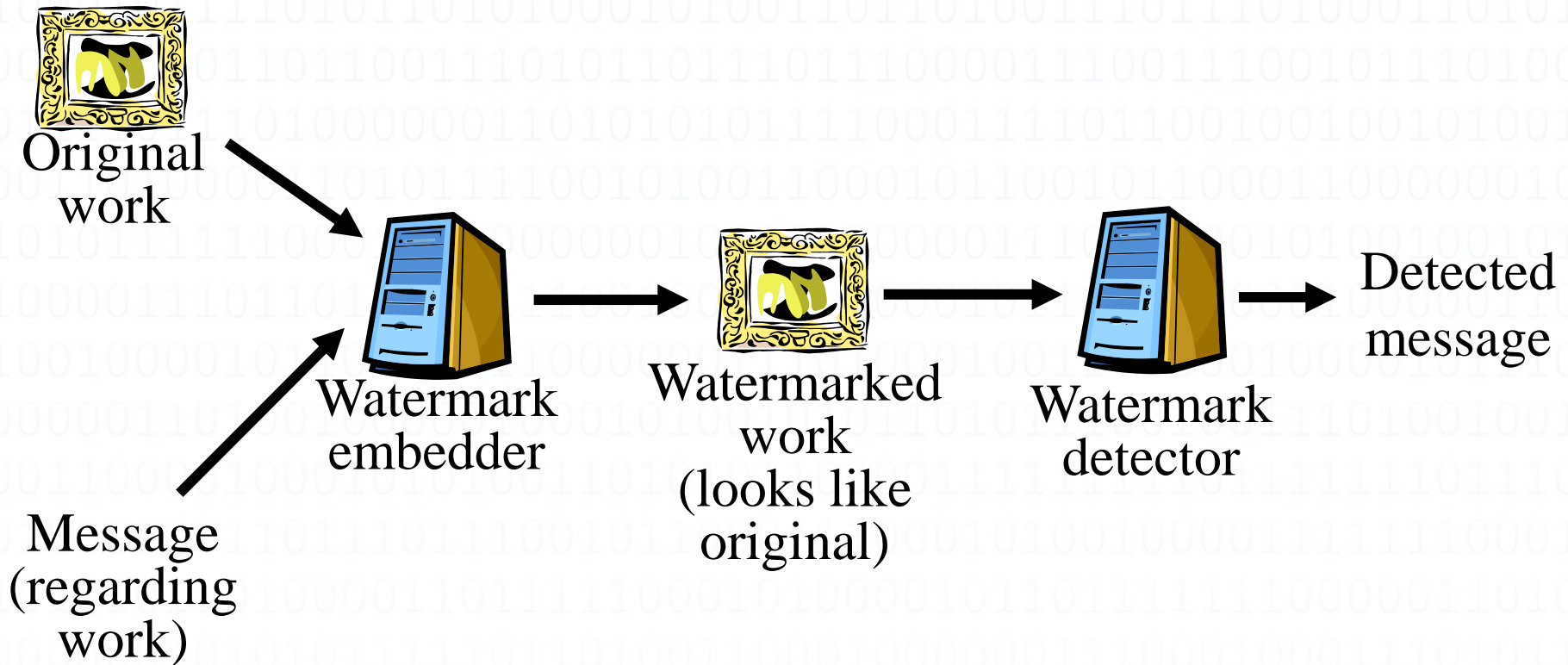
Applications of Digital Watermarking

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

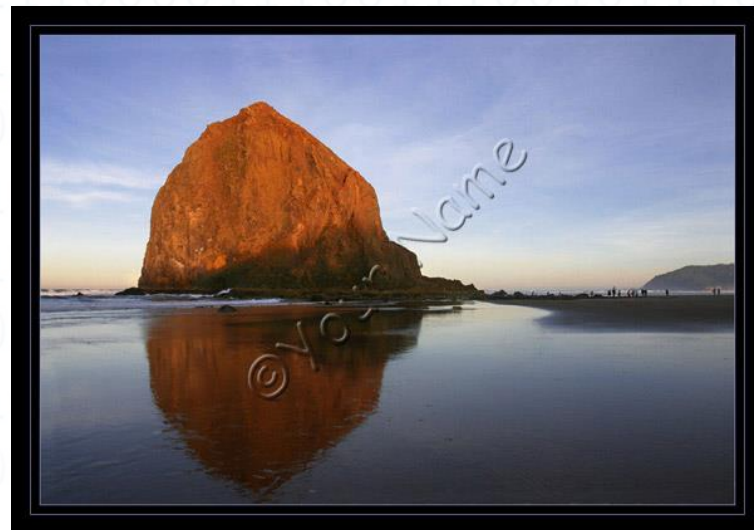
For tamper proofing, e.g. losing watermark implies tampering.

- 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.

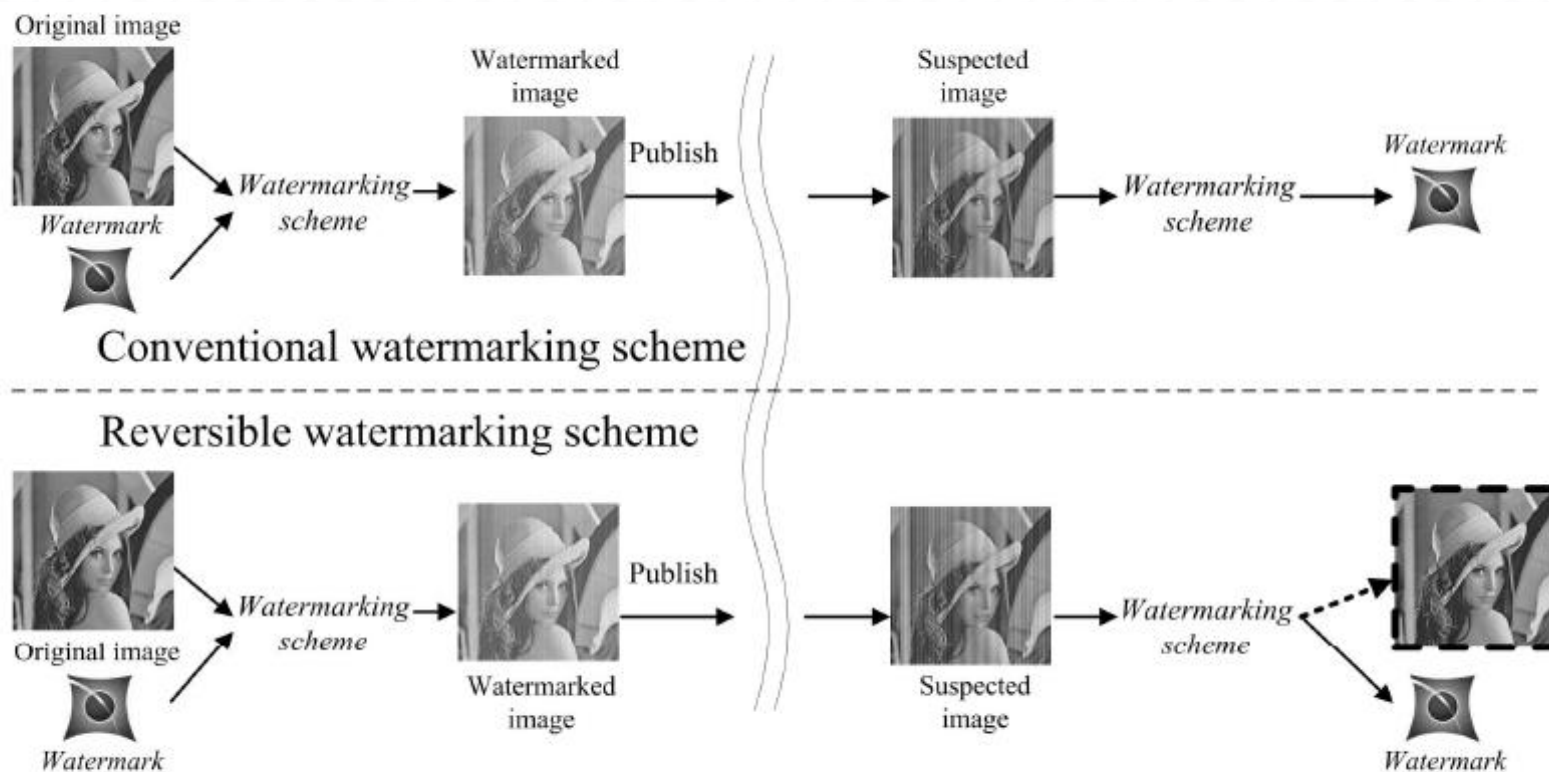
- 半盲检测 Semi-blind/Informed detection

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



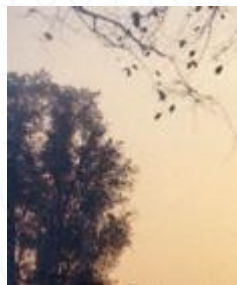
Terminology

- 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:



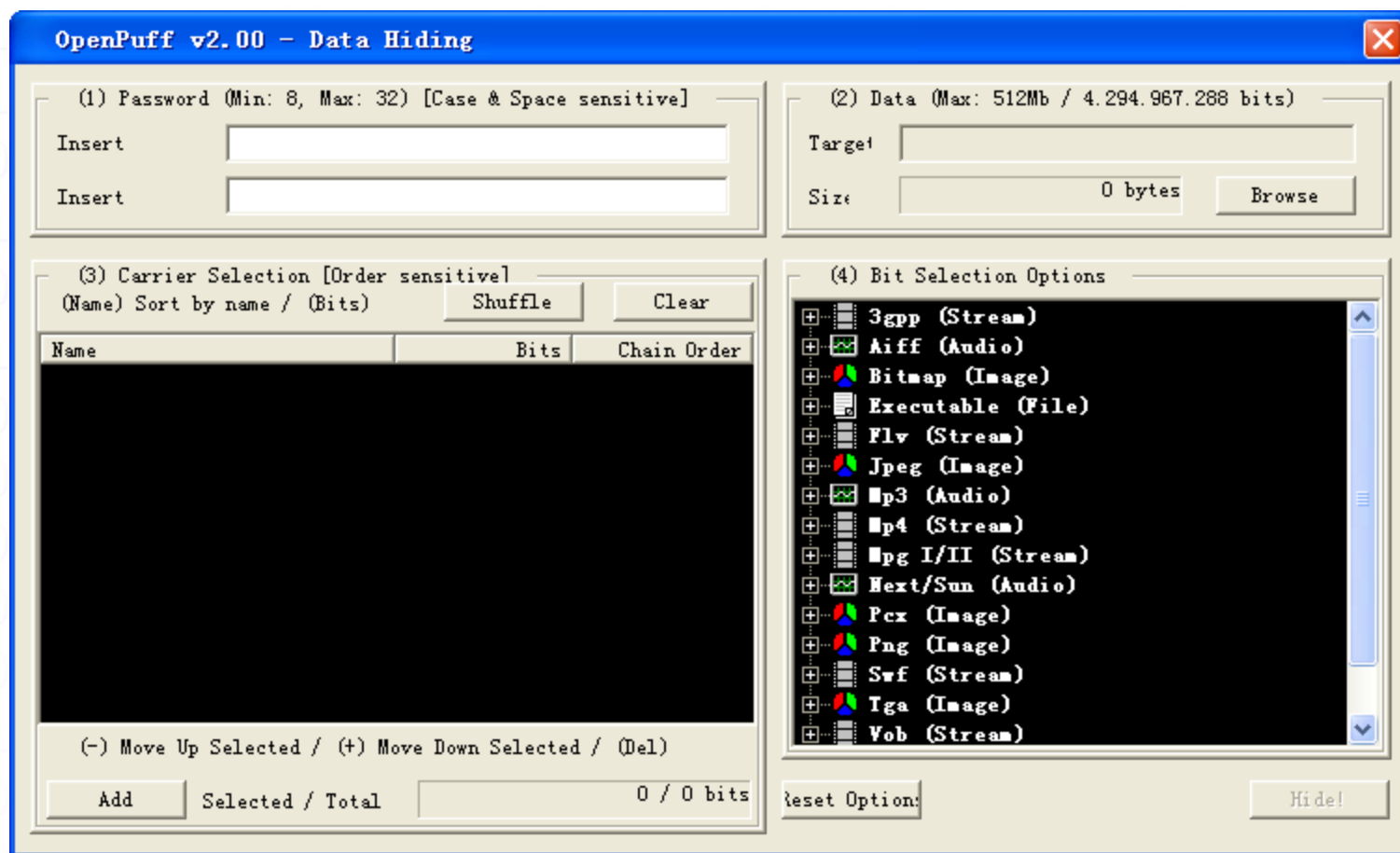
「 Part Five 」



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

The screenshot shows a Microsoft Internet Explorer browser window displaying the 'Digital Watermarking World: Research Links' page. The address bar shows the URL 'http://www.watermarkingworld.org/research.html'. The page features a navigation menu on the left with categories like WATERMARKING, MAILINGLIST, CONFERENCES, BENCHMARKING, BOOKS, LINKS, WEBRING, and DISCLAIMER. The main content area is titled 'Research Related Watermarking Links' and includes a search bar, a contact email 'wmwlinks@watermarkingworld.org', and a list of new links on top of the list. The list contains various research groups and individuals, such as Mercan Topkara, Prof. XingMing Sun, Wojciech Mazurczyk, Dr. Jeffrey A. Bloom, Dr. Ingemar J. Cox, Philips Research Labs, University of Surrey, Dr. Neil F. Johnson, Institute of Information Science, Academia Sinica, Dr. Chun-Shien Lu, Computer Vision Group, University of Geneva, Sviatoslav Voloshynovskiy, Shelby Pereira, Joe Ruanaidh, Dept. of Engineering, Univ. of Cambridge, Prof. Ross Anderson, Dr. Fabien Petitcolas, Dr. Markus Kuhn, Telecommunication Engineering, University of Erlangen, Prof. Bernd Girod, Dr. Frank Hartung, Dr. Jonathan Su, Dr. Joachim Eggers, Robert Baeuml, Roman Tzschoppe, EPFL-Signal Processing Laboratory, Prof. Murat Kunt, Dr. Martin Kutter, Dr. Fred Jordan, AlpVision SA, Università degli Studi di Firenze, Dr. Alessandro Piva, Dr. Franco Bartolini, EURECOM, IMAGE and VIDEO Group, Dr. Jean-Luc Dugelay, and Dr. Gabriella Khedari Csurka.

Digital Watermarking World: Research Links - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 前进 停止 刷新 搜索 收藏夹 打印 邮件 聊天 共享 任务栏

地址(A) http://www.watermarkingworld.org/research.html 转到 链接

Watermarking World

NEWS ABOUT PARTNERS CONTACT

Search [HELP](#)

WATERMARKING

- Biography
- FAQ

MAILINGLIST

- Management
- Archive

CONFERENCES

- Calls

BENCHMARKING

- StirMark
- CheckMark
- OptiMark

BOOKS

LINKS

- Companies
- Research
- Others

WEBRING

DISCLAIMER

Research Related Watermarking Links

To have your link added, please send us an email wmwlinks@watermarkingworld.org.

New links on top of the list

- [Mercan Topkara - Computer Sciences Department of Purdue University](#), West Lafayette, IN, USA. Information hiding into natural language text.
- [Prof. XingMing Sun - Network & Information Security Lab](#), Hunan University, Yuelu Mountain, Changsha, China
- [Wojciech Mazurczyk - Security Research Group](#), Warsaw University of Technology, Warszawa, Poland
- [Dr. Jeffrey A. Bloom](#) - Thomson Corporate Research, Multimedia Security Group, Princeton, USA
- [Dr. Ingemar J. Cox](#) - University College, London, UK
- [Philips Research Labs, Information and System Security group, Eindhoven, The Netherlands](#) - Dr. A.N. Lemma, Dr. Michiel van der Veen
- [University of Surrey - School of Electronics and Physical Sciences - Department of Computing](#) - Dr. Anthony T.S. Ho.
- [Dr. Neil F. Johnson's watermarking and steganography pages](#).
- [Institute of Information Science, Academia Sinica, Taipei, Taiwan: Prof. Mark Liao](#)
 - [Dr. Chun-Shien Lu](#)
- [Computer Vision Group - University of Geneva: Prof. Thierry Pun](#)
 - [Sviatoslav Voloshynovskiy](#): Papers with good theory and excellent results.
 - [Shelby Pereira](#): Work on channel coding and currently benchmarking (Checkmark 1.0).
 - [Joe Ruanaidh](#): Interesting work in invariant domain watermarking.
- [Dept. of Engineering: Univ. of Cambridge - Prof. Ross Anderson](#)
 - [Dr. Fabien Petitcolas](#): A must! The creator of stirmark and a lot of other excellent work.
 - [Dr. Markus Kuhn](#): He started the work on stirmark.
- [Telecommunication Engineering - University of Erlangen: Prof. Bernd Girod \(Professor Girod is currently at Stanford University, USA\)](#)
 - [Dr. Frank Hartung](#) (now with Ericsson, Herzogenrath, Germany): A pioneer in video watermarking.
 - [Dr. Jonathan Su](#) (now with MIT Lincoln Labs, Boston, USA): "Power spectrum complicity" comes from him.
 - [Dr. Joachim Eggers](#) (now with Siemens, Erlangen, Germany): Activities on quantization and DCT watermarking.
 - [Robert Baeuml](#): Activities on Synchronization and Information Theoretic Aspects of Watermarking.
 - [Roman Tzschoppe](#): Activities on Digital Watermarking, Steganography, and Communications.
- [EPFL-Signal Processing Laboratory: Prof. Murat Kunt](#)
 - [Dr. Martin Kutter](#), [Dr. Fred Jordan](#) (both with [AlpVision SA](#), Switzerland): Mailinglist, Webring, Papers(link dead)
- [Università degli Studi di Firenze](#)
 - [Dr. Alessandro Piva](#): Many online papers and links.
 - [Dr. Franco Bartolini](#)
- [EURECOM - IMAGE and VIDEO Group for MultiMedia Communications and Applications](#)
 - [Dr. Jean-Luc Dugelay](#).
 - [Dr. Gabriella Khedari Csurka](#).

Internet Resource

Digital watermarking - Wikipedia, the free encyclopedia - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 前进 搜索 收藏夹 历史记录 打印 邮件 聊天 共享 帮助

地址: http://en.wikipedia.org/wiki/Digital_watermarking 转到 链接

Log in / create account

Interested in contributing to Wikipedia?

[article](#) [discussion](#) [edit this page](#) [history](#)

Digital watermarking

From Wikipedia, the free encyclopedia

It has been suggested that this article or section be merged into [Watermark \(data file\)](#). (Discuss)

Digital watermarking is the process of embedding information into a digital signal. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy.

In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark.

In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such. An important application of invisible watermarking is to copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. [Steganography](#) is an application of digital watermarking, where two parties communicate a secret message embedded in the digital signal. Annotation of digital photographs with descriptive information is another application of invisible watermarking. While some file formats for digital media can contain additional information called [metadata](#), digital watermarking is distinct in that the data is carried in the signal itself.

The use of the word of watermarking is derived from the much older notion of placing a visible [watermark](#) on paper.

Contents [hide]

- 1 Instance of a Digital Watermarking Scheme
- 2 Watermarking Life-Cycle Phases
- 3 Watermark Parameters
 - 3.1 Capacity
 - 3.1.1 Embedding Capacity
 - 3.1.2 Retrieval Capacity
 - 3.2 Complexity
 - 3.3 Invertibility
 - 3.4 Robustness
 - 3.4.1 Detection Success
 - 3.4.2 Watermark Robustness
 - 3.5 Security
 - 3.6 Transparency
 - 3.7 Verification
- 4 Classification
 - 4.1 Robustness
 - 4.2 Perceptibility
 - 4.3 Capacity
 - 4.4 Embedding method
- 5 Applications
- 6 Evaluation / Benchmarking
- 7 See also
- 8 External links
- 9 References

navigation

- [Main page](#)
- [Contents](#)
- [Featured content](#)
- [Current events](#)
- [Random article](#)

search

interaction

- [About Wikipedia](#)
- [Community portal](#)
- [Recent changes](#)
- [Contact Wikipedia](#)
- [Donate to Wikipedia](#)
- [Help](#)

toolbox

- [What links here](#)
- [Related changes](#)
- [Upload file](#)
- [Special pages](#)
- [Printable version](#)
- [Permanent link](#)
- [Cite this page](#)

languages

- [Česky](#)
- [Deutsch](#)
- [Español](#)
- [Français](#)
- [Italiano](#)
- [日本語](#)
- [Norsk \(bokmål\)](#)
- [Polski](#)
- [Русский](#)
- [ไทย](#)
- [中文](#)

An image with visible digital watermarking. The text "Brian Kell 2006" can be seen across the center of the image.

Internet

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>



杭州电子科技大学
HANGZHOU DIANZI UNIVERSITY

Thank you!
