INT 307
Multimedia Security System

Digital Forensics

Sichen.Liu@xjtlu.edu.cn

XJTLU

Xi'an Jiaotong-Liverpool University
西交利物浦大学

Outline

- Digital Forensics – HASH function
- Watermarking – Introduction
- Basic information hiding method – Least Significant Bit (LSB) Methods
- Spread Spectrum Watermarking
- Application of digital watermarking

Aim of Digital Forensics

The application of investigating methodologies of forensics to the field computer crimes or multimedia infringement.

- Source Identification
- Integrity / Authenticity
- Enhancement
- Interpretation and Content Analysis

Means of Attack

- Disguise identity
- Tampering with content
- Modify the order
- Change the time
- Deny sending
- Deny acceptance

Types of Multimedia Forensics

- Active Multimedia Forensics
  - Known the media should be protected
  - Add embedded information in the multimedia file
  - HASH Function

- Passive Multimedia Forensics
  - Showing the metadata of the content
  - Using information retrieval methods

Hash Function

A way to demonstrate data integrity is HASH function.

- Hash function maps a variable length message to a fixed length message: $y = h(x)$
- If h is a 64-bit has function, then y always fits in 64 bits i.e. $0 \leq y < 2^{64}$
- A hash is a keyless algorithm
- Anyone can compute $h(x)$ if x is known

Example

Alice sends Bob $C = \text{Encrypt}(M), h(M)$. Bob receives $C, h(M)$ and checks

- $M' = \text{Decrypt}(C)$
- $h(M')$

Cryptographic Hash Functions

- Collision resistance: difficult to find any M, $M' \neq M$ such that $h(M) = h(M')$
- Preimage resistance: given $h(M)$, difficult to find M' such that $h(M') = h(M)$
- Second preimage resistance: given M, difficult to find M' such that $h(M') = h(M)$, $M' \neq M$

Namely, h is secure meaning

- Easy to compute in one direction
- Very difficult to compute in the other direction (i.e. computational secure)
- Very difficult to find two messages that have the same hash value

HASH in Industry

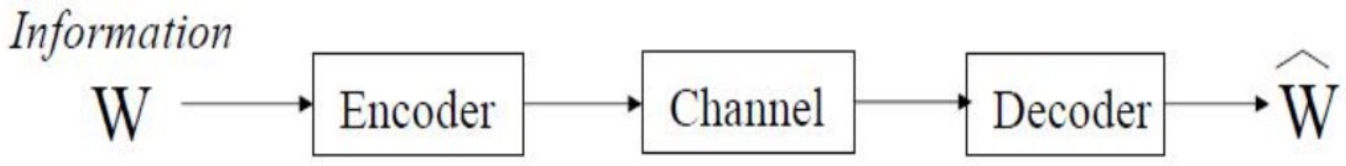
- Industrial Standards: SHA-256, SHA-3, MD4, MD5

HASH application in Blockchain

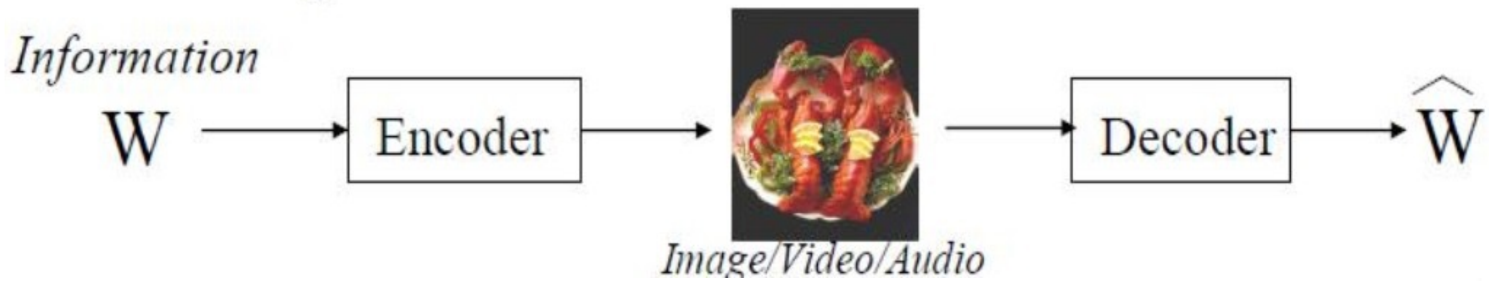
- Blockchain is a decentralised dataset
- HASH function is used as one step of packaging information

Watermarking

- Basic communication system:



- Channel: air, wire, water, space,
- Watermarking:



- Embedding Visible / Invisible Codes in Multimedia Data for Security Purpose

Watermarking

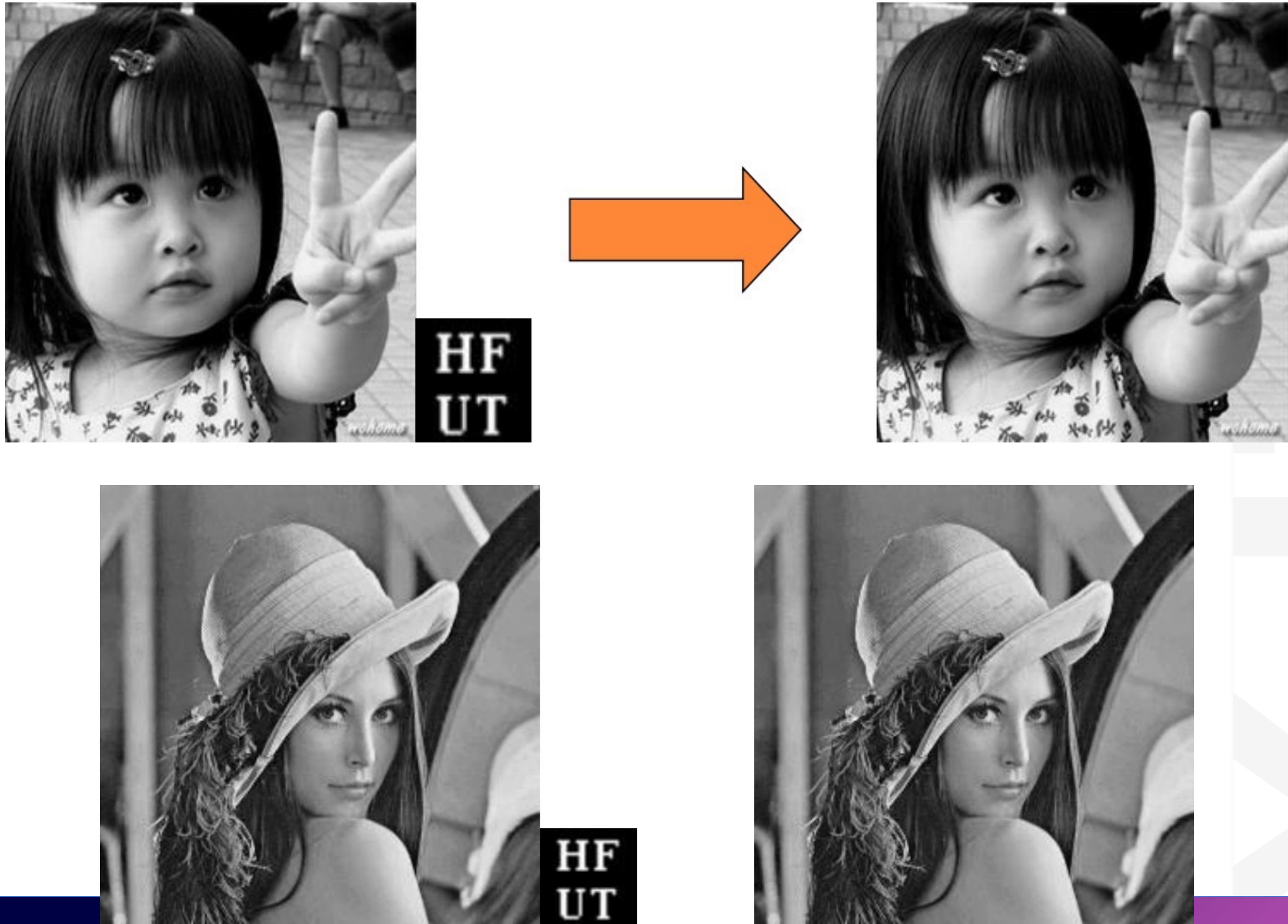
- The art of actively modifying audio-visual content such that the modifications
  - Are imperceptible (who is the listener?),
  - Carry retrievable information,
  - That survives under transformations of the content,
  - And is difficult to remove & change by unauthorized user (cryptography).
- Watermarking types: Visible vs Invisible; Robust vs Fragile; Referenced vs Unreferenced

Main Principles of Water Marking

- Transparency - the watermark is not visible in the image under typical viewing conditions
- Robustness to attacks - the watermark can still be detected after the image has undergone linear and/or nonlinear operations (this may not be a good property - fragile watermarks), such as: Compression Scheme, Geometric operations, Signal Processing Operations, Printing and rescanning, Re-watermarking, forgery
- Capacity - the technique is capable of allowing multiple watermarks to be inserted into the image with each watermark being independently verifiable

- Application Scenario: copyright protection, finger printing, content authentication, broadcast monitoring, indexing

Example I



Robustness Test

Robustness Testing

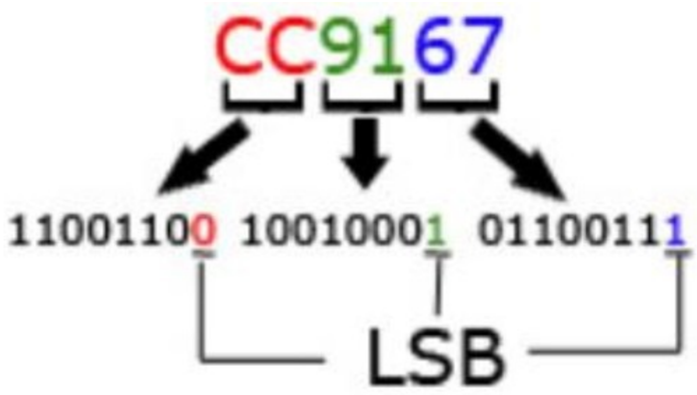
Gaussian Noise 0.1

Robustness Test

JPEG Compression

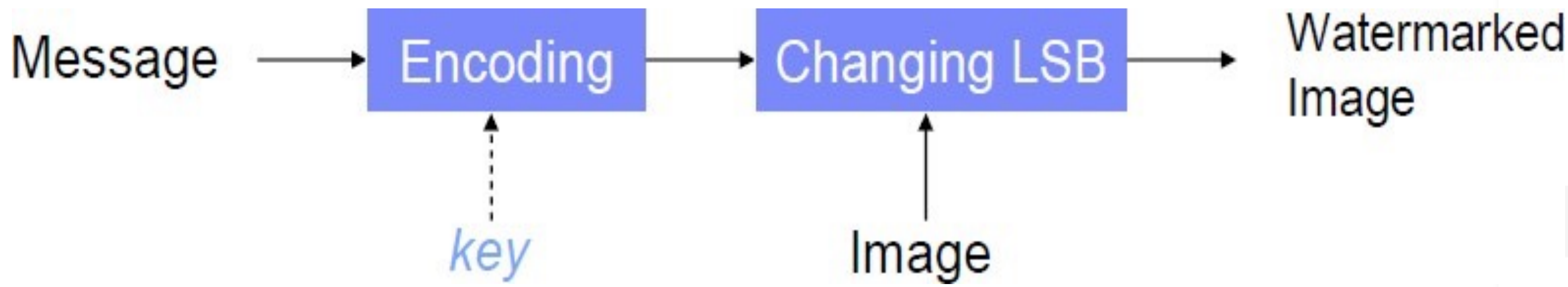
Simplest Watermark – Changing Least Significant Bits

- LSB are bits which if modified will not significantly affect the colors produced by the combination of the three RGB color components

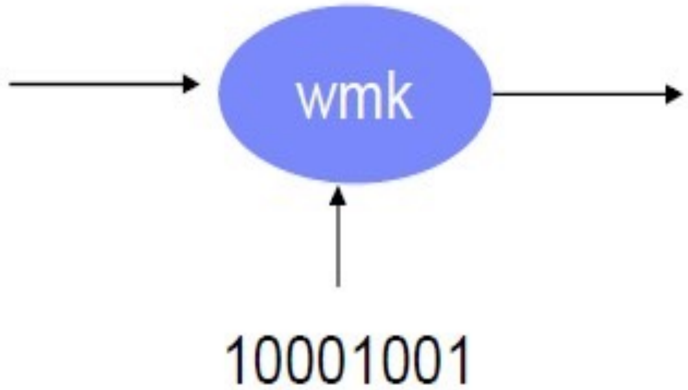


Preliminary data, three pixels of the image 24-bit
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
The binary value of the character 'A' is
10000011.
Data after planting the character 'A'
(0010011**1** 1110100**0** 1100100**0**) → 100
(0010011**0** 1100100**0** 1110100**0**) → 000
(1100100**1** 0010011**1** 11101001) → 11

Simplest Watermark – Changing Least Significant Bits



158	165	158	158	158	158	155	158
155	161	155	150	155	155	158	151
150	155	155	150	161	161	174	174
171	167	171	159	151	151	134	117
96	94	90	102	102	108	108	101
108	108	96	108	108	108	108	108
108	108	103	108	108	120	110	117
110	117	117	123	125	129	124	127



159	164	158	158	159	158	154	159
155	160	154	150	155	154	158	151
151	154	154	150	161	160	174	175

....

LSB Example

(a) Original Image

(b) Watermark

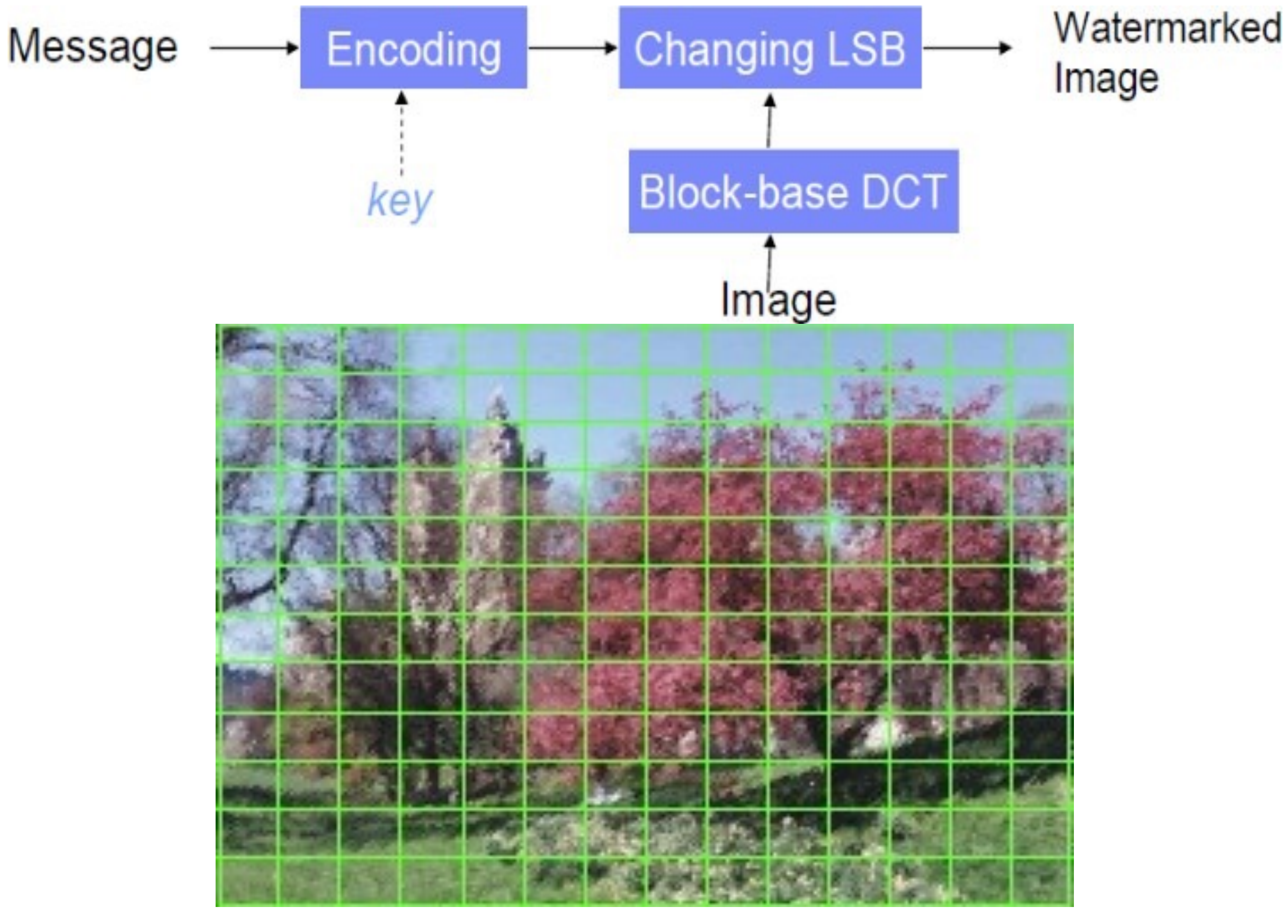
(c) Image with embedded watermark

(d) Extracted watermark

(e) Difference between (a) and (c)

Changing LSB in the block-based frequency domain

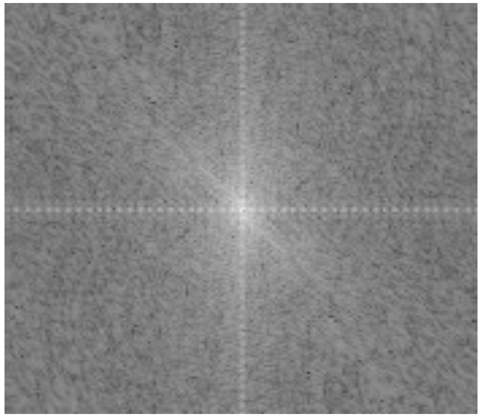
- Embed one bit at one DCT coefficient
- Extension-1: embed one bit at one DCT coefficient after quantization
- Extension-2: embed one bit per DCT block



Changing LSB in the global frequency domain

- Convert Image to the global frequency domain
- Select some band for embedding coefficients
- Changing the least significant bit of the Original Image selected bands

Original Image



Properties of LSB

- imperceptible (modify only LSBs)
- secure (encrypt embedded information)
- not robust (e.g., randomly set LSBs to 0 or 1)
- more accurate: secure info-hiding method

Spread Spectrum Watermarking: Embedding

- Spread Spectrum: $T(S_w) = T(S) + T(X)$
  - T can be any spatial-frequency transforms.
  - E.g. Fourier Transforms (DFT, DCT), Wavelet Transforms
- Objectives
  - Detect the existence of a specific code, which is served as the copyright information.
  - Watermark detection needs the original source.
- Implementation
  - Add a specific code on the 1000 largest or the 1000 lowest frequency DCT coefficients of the image.
  - The watermark is a random binary sequence.
    $T(x) = 1\ 1\ -1\ 1\ -1\ -1\ -1\ 1$

Spread Spectrum Watermarking: Detection

- DCT of original image S is computed
- DCT of watermarked image S_w is computed
- The difference between the two DCT gives the watermark
- Compute the correlation of the c = $S(T(S_w) - T(S), T(X))$
- If c is larger than the user-defined threshold, they belongs to the owner.

Spread Spectrum Watermarking: Example

Original image

Watermarked image

Application of Digital Watermarking

Broadcasting Monitoring

- Alice is an advertiser who embeds a watermark in each of her radio commercials before distribute them to 600 radio stations.
- Alice monitors radio station broadcasts with a watermarking detector.
- She matches her logs with the 600 invoices.
- ATTACK: Bob secretly embed Alice's watermark into his own advertisement and airs it in place of Alice's commercial.

- Being able to obtain a pre-composed legitimate message and embeds this message in a Work
  - e.g., in Scenario 1, Bob extract the reference pattern and then use it to his work - called copy attack
  - Possible Solution: using content-related watermarks

Application of Digital Watermarking

Web Reporting

- Alice owns a watermarking service that, for a nominal fee, adds an owner identification watermark to images that will be accessed through the Internet.
- Alice provides an expensive reporting service to inform her customers of all instances of their watermarked images found on the Web.
- ATTACK: Bob builds his own web crawler that detects watermarks embedded by Alice and offers a cheaper reporting service.

Application of Digital Watermarking

Copy Control

- Alice owns a movie studio, and she embeds a copy control watermark in her movies before they are distributed.
- She trusts that two digital recorders capable of copying these movies contain watermark detectors and will refuse to copy her movie.
- ATTACK: Bob is a video pirate who has a device designed to remove the copy protection watermark.

- Possible ways of attack:
  - Elimination attacks, where watermark is truly gone
  - Masking attacks, where watermark is still present but weakened

Exemplar Operation Table for Digital Watermarking

	Embed	Detect	Remove
Broadcast Monitoring			
Advertiser	Y	Y	-
Broadcaster	N	N	-
Public	N	N	-
Web Reporting			
Marking Service	Y	Y	-
Reporting Service	-	Y	-
Public	N	N	N
Copy Control			
Content Provider	Y	Y	-
Public	-	Y	N

Y: must be allowed, N: must not be allowed, - : don't care

Evaluation of System Performance

- Transparency: PSNR & SNR
- Capacity: the ratio between the size of original media and the size of hidden information carried
- Payload: with the hidden information, the file size increase over original size
- Robustness
  - Crop
  - Resize
  - Rotation
  - Mirror
  - Compression
  - Noise

THANK YOU

VISIT US

WWW.XJTLU.EDU.CN

FOLLOW US

@XJTLU

Xi'an Jiaotong-Liverpool University
西交利物浦大学

XJTLU