Department of Computer Science and Engineering

The Chinese University of Hong Kong

Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery

Supervised by Prof. LYU, Rung Tsong Michael

Presented by Chan Pik Wah, Pat

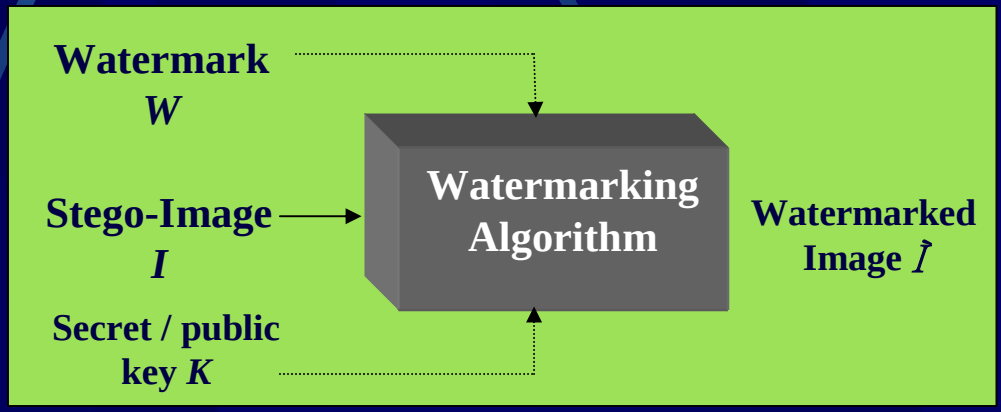
April 28, 2002

Outline

- Introduction
- Motivation
- Research objective
- Background
- New Video Watermarking Algorithm
- Experimental Results
- Future Direction
- Conclusion

Introduction

- Watermarking is a concept of embedding a special pattern, *watermark*, into a document
- Watermarking is a key process for the protection of copyright ownership of electronic data



Introduction

- A new scheme for robust blind digital video watermarking will be introduced
- The features of the video watermarking algorithm are:
  - video and audio watermark are combined;
  - it is robust against the attack of frame dropping, averaging and statistical analysis;
  - it allows blind retrieval of embedded watermark which does not need the original video;
  - the watermark is perceptually invisible;
  - it is resistant to lossy compression.

Why Is Multimedia Security Needed?

- Easier to transfer multimedia documents across the Internet
- Copyright protection of content
- Multimedia Security and Multimedia Copyright Protection
- Encryption and control access
- Digital Watermarking

Why Digital Watermark?

- Cryptography ensures confidentiality, authenticity, and integrity
- It cannot help after decryption
- Digital Watermarking can help
  - Prove ownership
  - Identify a misappropriating person
  - Trace the marked document's dissemination through the network

Why Video Watermark?

- Different interesting watermarking approaches have been proposed
- Most of Video Watermarking is based on the techniques of the image watermarking
- Video watermarking introduces some issues not present in image watermarking
- Due to large amounts of data and inherent redundancy between frames, video signals are highly susceptible to pirate attacks, including frame averaging, frame dropping, frame swapping, statistical analysis, etc

Research objective

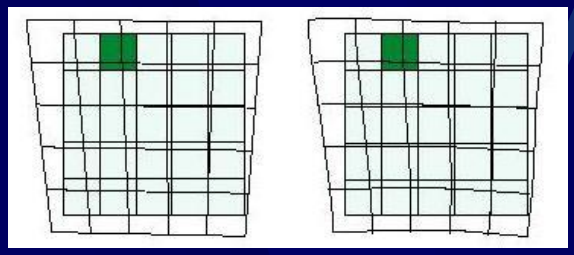
- Survey and investigation on multimedia security issues and multimedia watermarking scheme.
- Compare and evaluate various watermarking scheme
- A new approach and procedures for multimedia security based on watermarking are proposed.
- Experiment will be done on this proposed approach

Properties of Watermark

- Invisibility
- Blind or Informed Detection
- Capacity (Number of bits that can be hidden)
- Low error probability
- Robustness
  - Image watermarking (filtering, resizing, contrast enhancement, cropping, rotation...)
  - Video watermarking (frame averaging, frame dropping, frame swapping, statistical analysis, interpolation...)

Attacks on Watermarking

- Processing operation
- Compression
- Rescaling
- Cropping
- Multiple watermarks



- Frame averaging
- Frame dropping
- Frame swapping
- Statistical analysis
- Interpolation

Video Watermarking

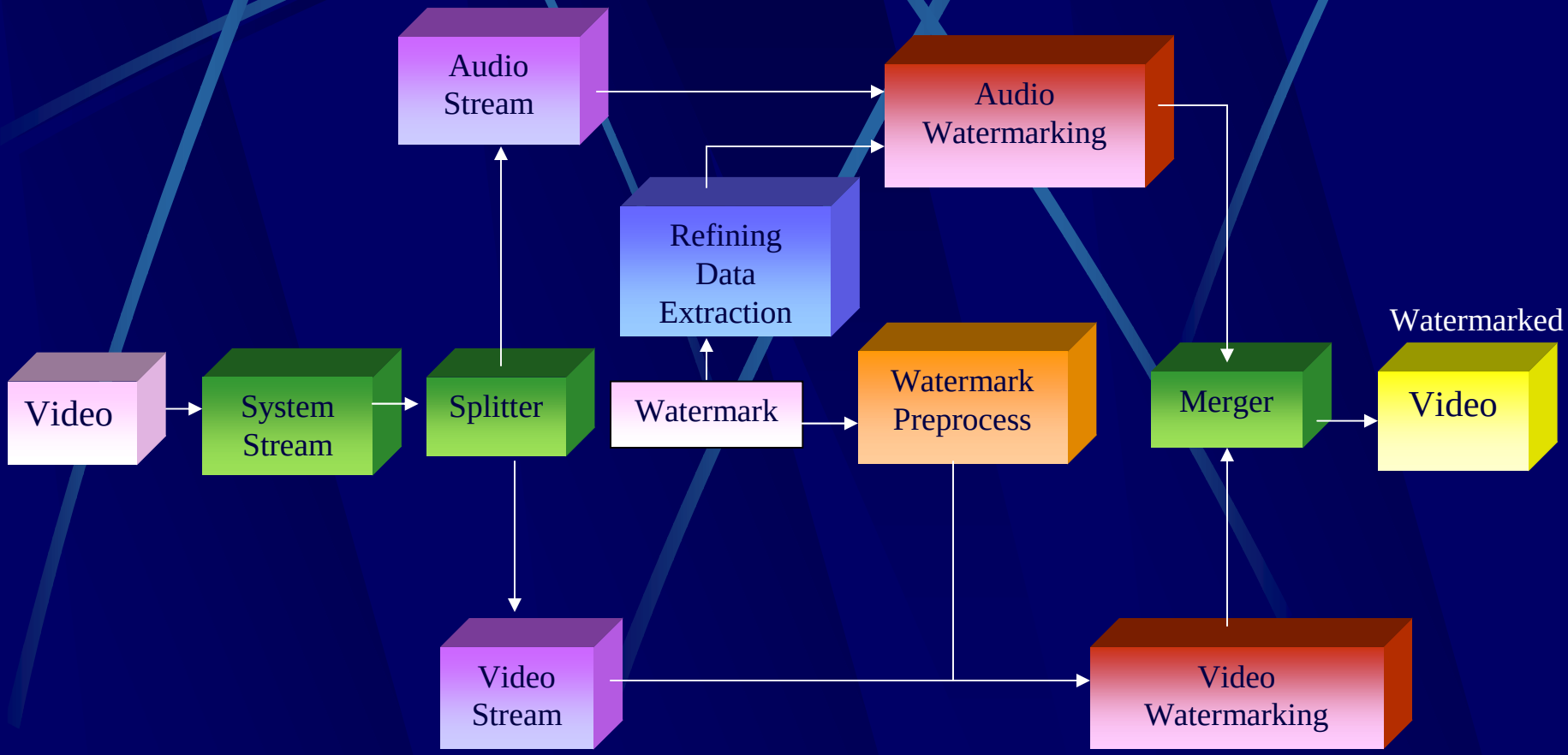
- Raw video watermarking
  - Spatial domain
  - Frequency domain
    - DFT
    - DCT
    - DWT
- Watermarking I-frame (Mpeg-1,2)
- Video object watermarking (Mpeg-4)

DWT-based Blind Video Watermarking Scheme with Scrambled Watermark

Introduction

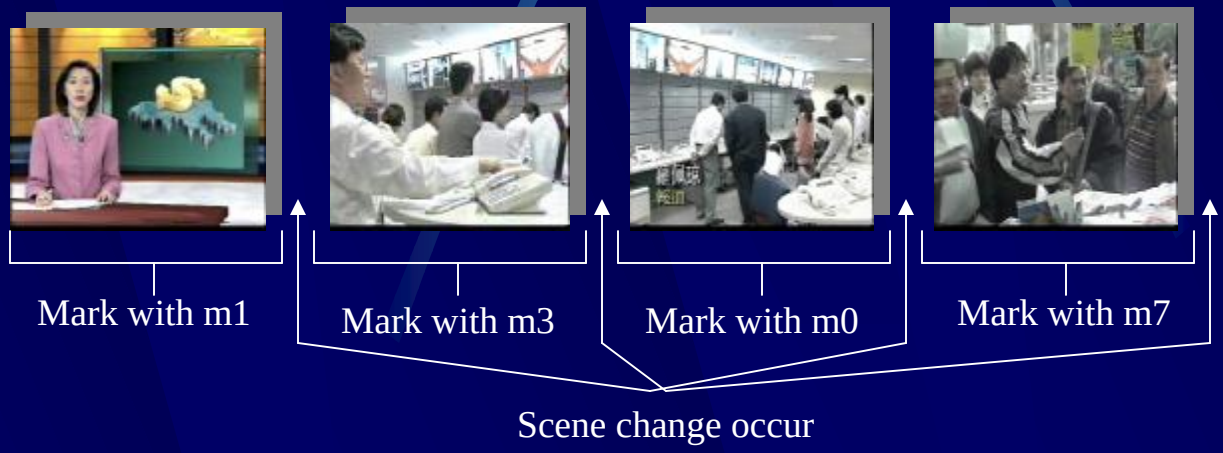
- Focus on problems only exist in video watermarking
  - Frame averaging
  - Frame dropping
  - Frame swapping
  - Statistical analysis
- Scrambled the watermark & scene change
- Visual-audio watermark
  - Error-correction
  - refining

Overview of the watermarking process



Video Preprocess
DWT & Scene Change Detection

- Video frames are transformed to wavelet domain
- Perform scene change detection
- Each scene is embedded with a same watermark, so it can prevent attackers from removing the watermark by frame dropping
- Independent watermark used for successive different scene can prevent attackers from colluding with frames from completely different scenes



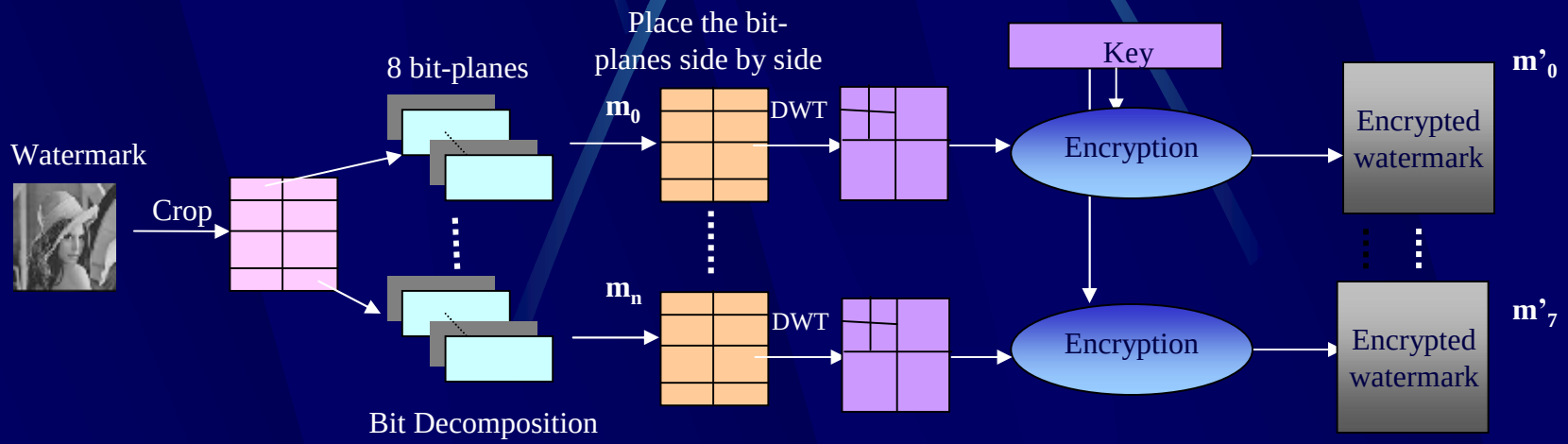
Watermark Preprocess

- Scale the watermark to a particular size with the following equations
  - $2^n \leqq m$, n>0
  - p + q = n , p and q > 0
  - Size of image = $64 \bullet 2^p$ X $64 \bullet 2^q$

m -- # of scene change of the video

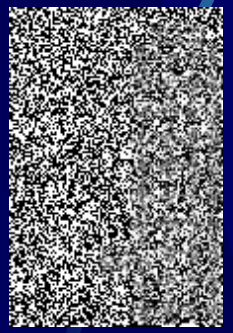
- Divide the image into 2^n small images with size 64 X 64

m = 10, n = 3, p = 1, q = 2

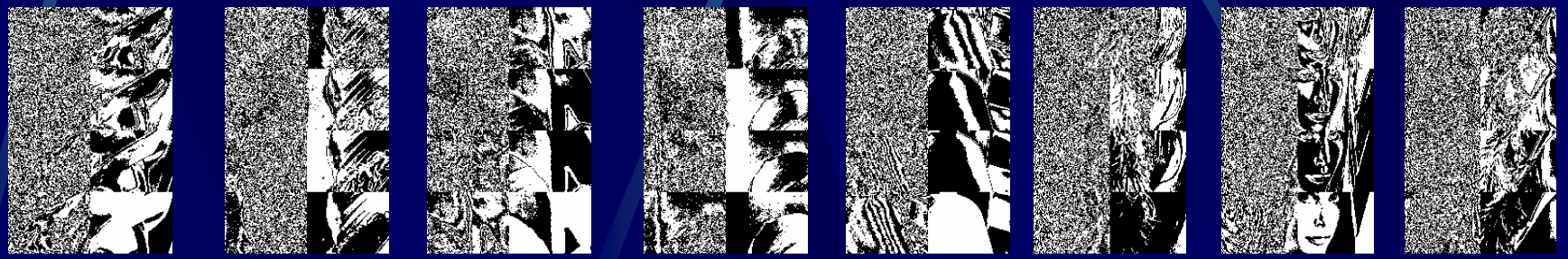


Watermark Preprocess

Original watermark



Encrypted watermark m'_0



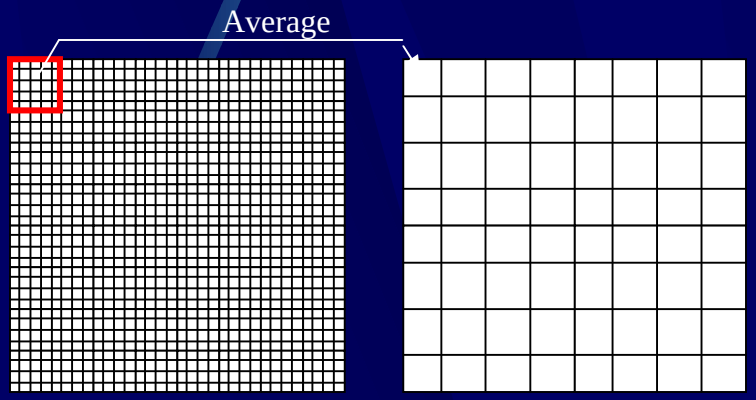
Preprocessed watermark m_0-m_7

Audio Watermark

- Error correcting code is extracted from the watermark image

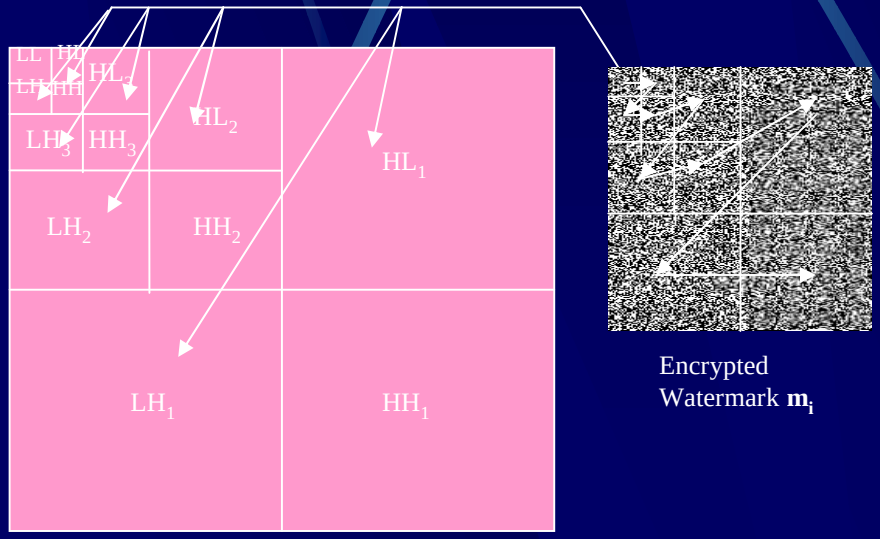
$$Avg_k = \sum_{i=0}^{x} \sum_{j=0}^{y} W_{j^*w+q^*x+p^*y^*w+i}$$

- Embedded in audio channel as an audio watermark
- This watermark can provided the error correction and detection capability for the video watermark



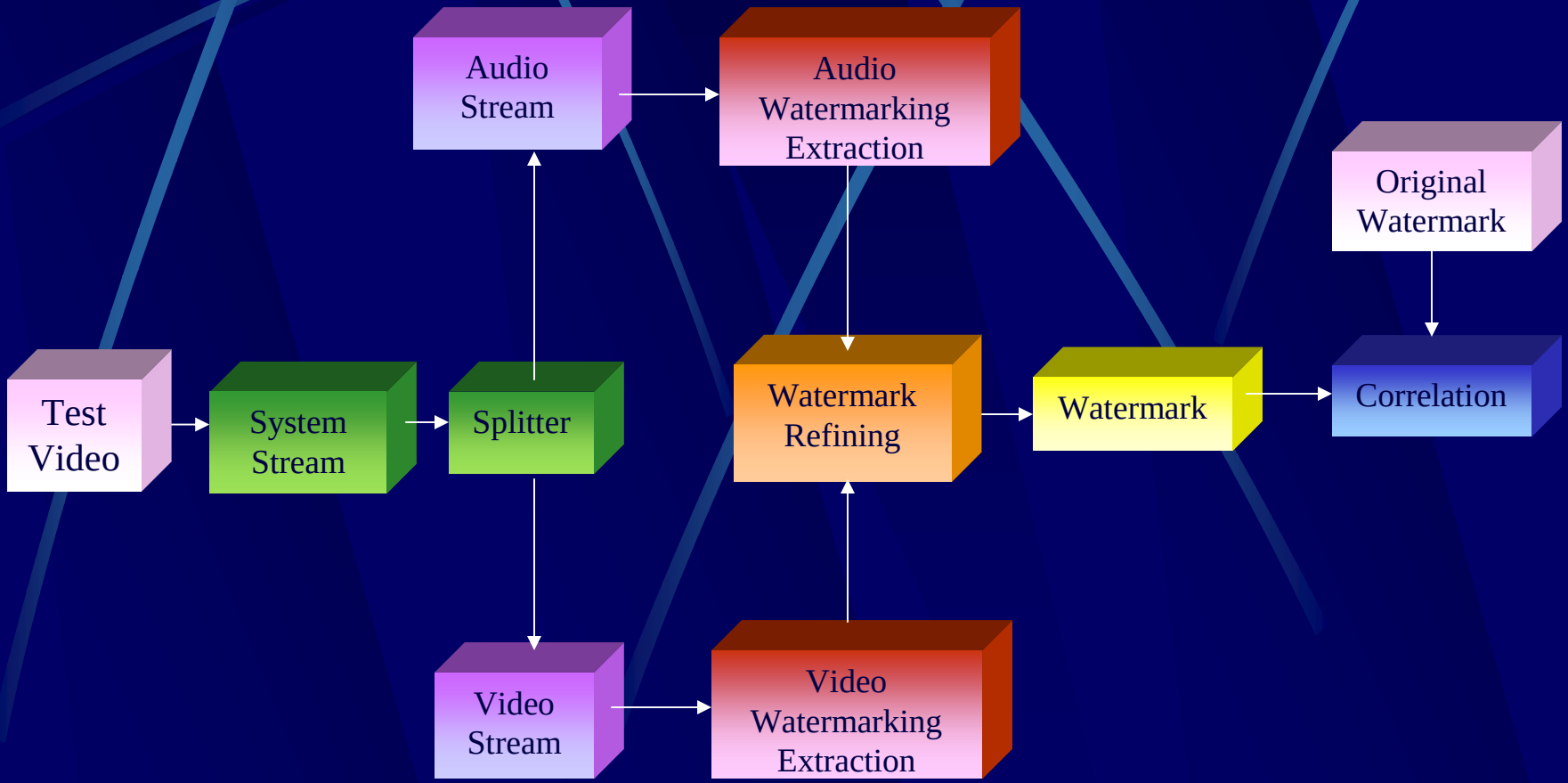
Watermark Embedding

- Exchange C[i] with max(C[i], C[i+1], C[i+2], C[i+3], C[i+4]) while W[j] = 1
- Exchange C[i] with min(C[i], C[i+1], C[i+2], C[i+3], C[i+4]) while W[j] = 0
- LL, HH coefficients are not watermarked



Encrypted Watermark $\mathbf{m}_i$

Watermark Detection



Watermark Detection

```
if WC[i] > median(WC[i], WC[i+1],WC[i+2], WC[i+3],
   WC[i+4])
        W[j] = 1
else
        W[j] = 0
```

Original video frame

Watermarked video frame

Extracted Watermark

Recovered Watermark

Watermark Refining

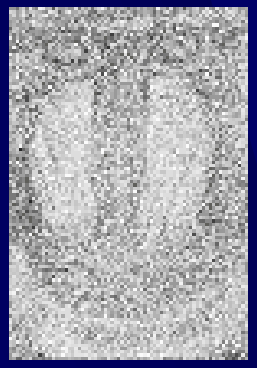
$$\widehat{W}_{ij} = (\widehat{W}_{ij} * P + Avg_k * Q)/(P+Q) \qquad \left|W_{ij} - \widehat{W}_{ij}\right| \geq T$$

$$\widehat{W}_{ij} = \widehat{W}_{ij} \qquad \text{Otherwise}$$

k = kth block of the average image
i = x- coordinate of video watermark
j = y-coordinate of video watermark
T = Threshold that the pixel need to correct
P: Q = the ratio of importance of extracted watermark to average

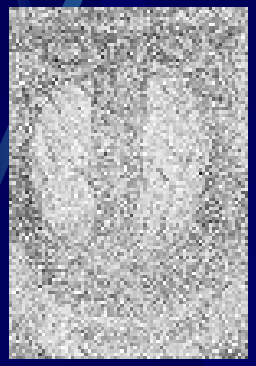
Experimental results

Extracted watermark from different attacks

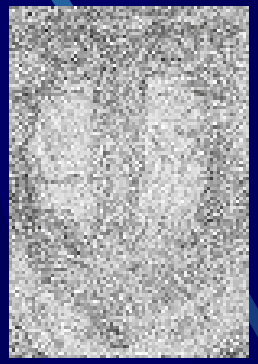


Dropping and averaging

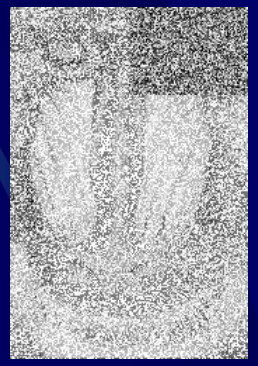
Compression



Increase brightness



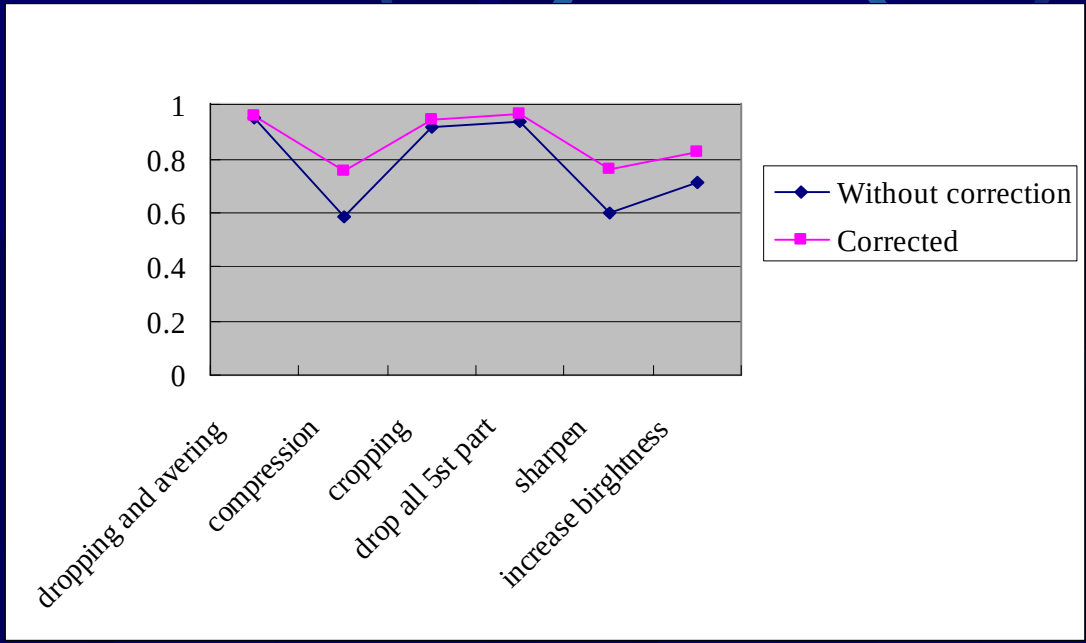
Cropping some regions



Dropping all frames with the 5th part of watermark

Experimental results

$$\text{Normalized correlation: NC} = \frac{\sum_i \sum_j W(i,j)\widehat{W}(i,j)}{\sum_i \sum_j [W(i,j)]^2}$$



Evaluation

- Blind watermarking scheme
- Invisibility
- Resist to frame dropping, averaging and statistical analysis
- Resist to lossy compression
- Visual-audio watermark

Future Direction

- Increase robustness against lossy compression
- Use better error correction coding
- Change the way to combine the visual and audio watermark.
- Making use of the information from the video, such as time information to increase the robustness of the watermark.
- Extend the watermark techniques to wireless environment

Conclusion

- Video Watermarking is needed since copyright protection is essential
- Video watermarking is different from image watermarking
- DWT-based Blind Video Watermarking Scheme with Scrambled Watermark is proposed
- Use visual-audio watermark to increase the robustness of the scheme

The End