Computer Science and Engineering Department
The Chinese University of Hong Kong

Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery

By Pat P. W. Chan

Supervised by Michael R. Lyu

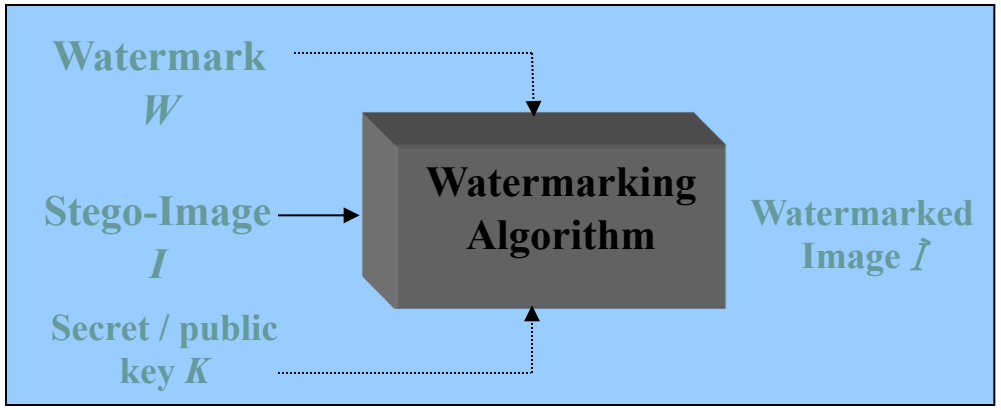
8/6/2004

Outline

- Introduction
- Review of watermarking schemes
- Comparison among current watermarking schemes
- Scene-based video watermarking scheme
- Possible improvements
  - Visual-audio watermarking scheme
    - Experimental results
  - Hybrid watermarking scheme
    - Experimental results
  - GA-based watermarking scheme
    - Experimental results
- 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.
- In this presentation, we will focus on the video watermarking scheme.



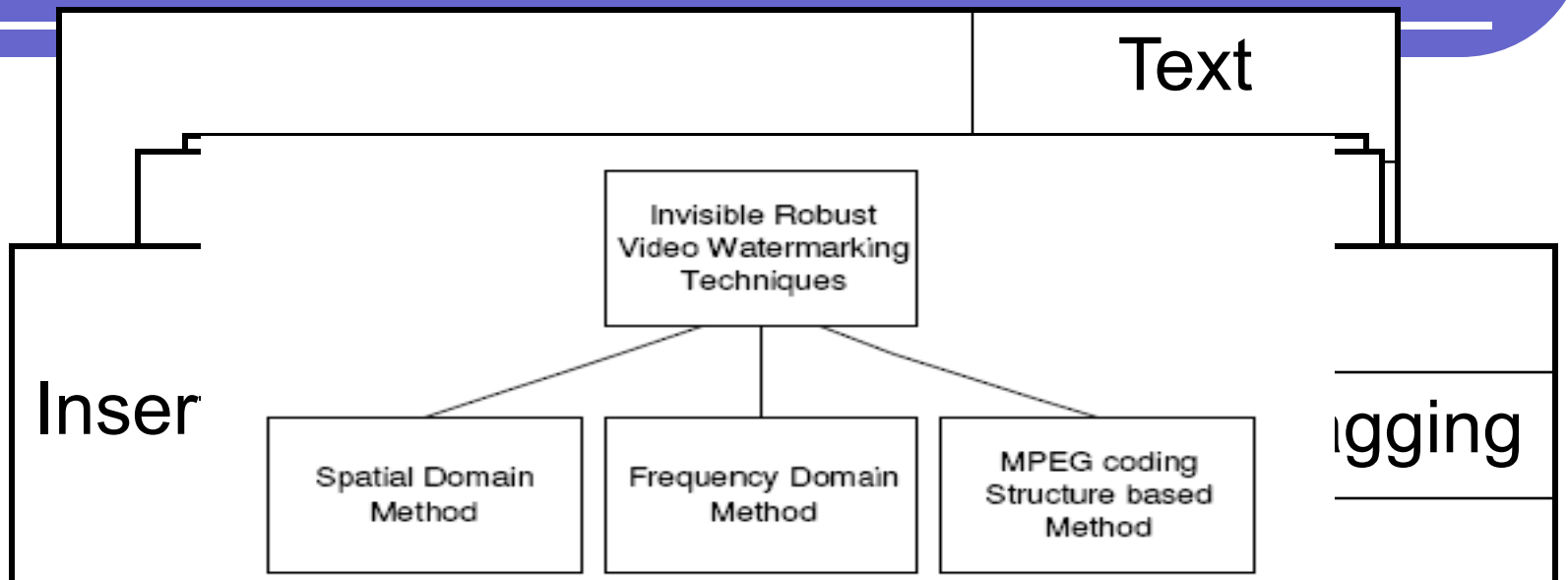
Introduction

- Video watermarking is challenging.
- 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.
- However, the currently proposed algorithms do not solve these problems effectively.

Introduction

- A novel hybrid digital video watermarking scheme with scene change analysis and error correction code will be introduced.
- The features of the video watermarking algorithm are:
  - Our scheme first embeds different parts of a single watermark into different scenes of a video based on scene change analysis;
  - Our video watermarking algorithm is robust against the attacks of frame dropping, averaging and statistical analysis;
  - To increase robustness, the watermark is refined by the error correcting code, while the correcting code is embedded as a watermark in the audio channel;
  - Apply a hybrid approach to form a super watermarking scheme that can resist most of the attacks;
  - To increase the fidelity, GA is employed to optimize the performance.
  - It allows blind retrieval of embedded watermark;
  - The watermark is perceptually invisible.

Review of Watermarking



- Least Significant Bit Modification
- Correlation-Based Techniques
- m-frame
- Spread Spectrum

- Discrete Cosine Transform (DCT)
- Discrete Wavelet Transform (DWT)
- Discrete Fourier Transform (DFT)
- Radon Transform

- Mpeg-4 Object-based
- Mpeg-2 Block-based

Comparison among different watermarking schemes

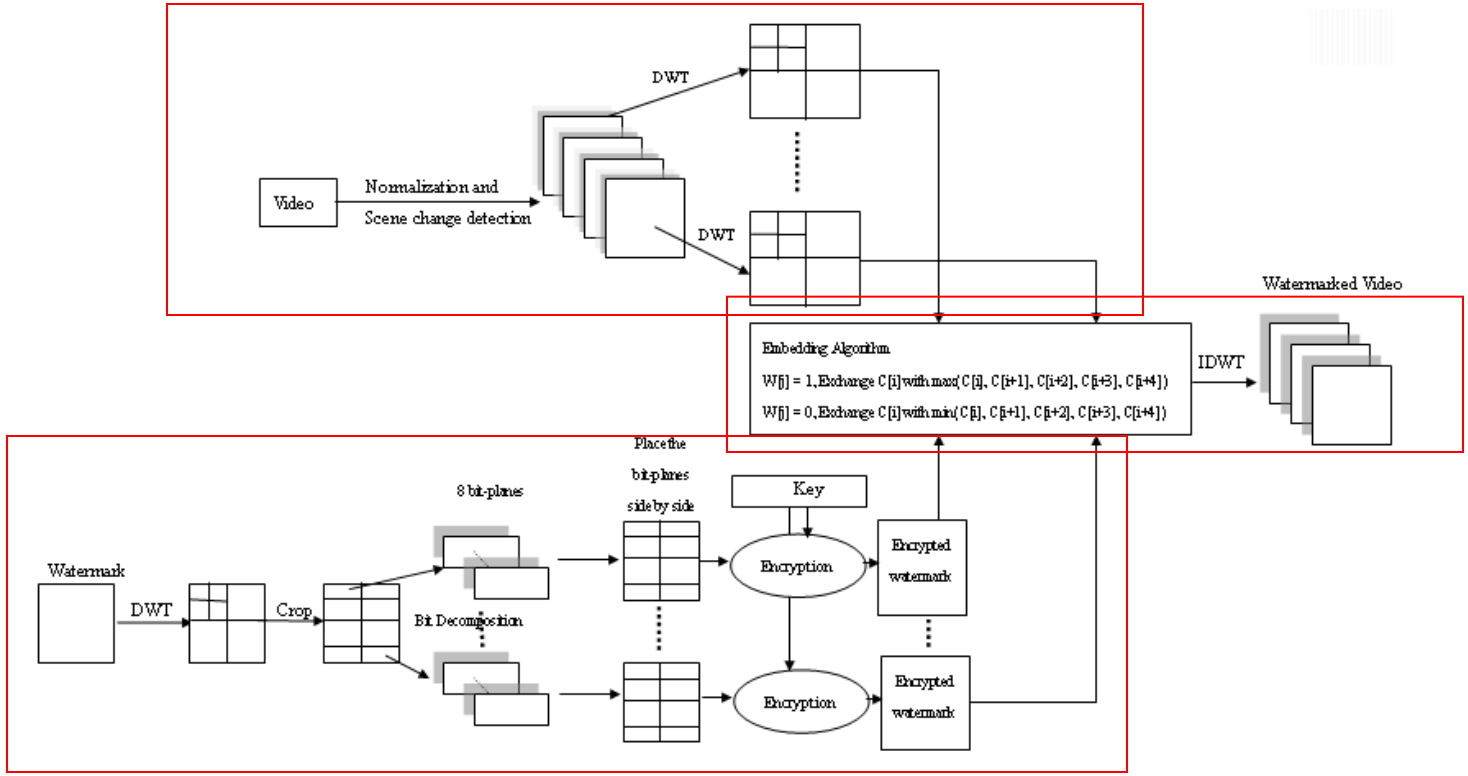
- Frequency domain watermarking is much more robust
- None of the currently proposed scheme is robust to all kind of attacks

Attack Class	LSB	Threshold - based Correlation	m-sequence / m-frame	Spread Spectrum
JPEG Lossy Compression	0.20	0.75	0.7	0.85
PSNR	0.13	0.82	0.89	0.9
Add Noise	0.10	0.7	0.75	0.89
Median Filter	0.21	0.4	0.4	0.35
Row / Column Removal	0.4	0.63	0.7	0.69
Cropping	0.49	0.65	0.75	0.78
Rescale	0.22	0.5	0.62	0.83
Rotation	0.14	0.52	0.61	0.85
Affine	0.15	0.46	0.56	0.76
Geometrical Distortions	0.25	0.42	0.5	0.62
Shearing	0.27	0.3	0.54	0.85

Attack Class	Mid-band DCT	Mid-band DWT	DFT template Matching	Radon Transform
JPEG Lossy Compression	1	0.75	0.74	0.83
PSNR	0.98	1	0.81	0.78
Add Noise	0.95	0.73	0.86	0.75
Median Filter	0.4	0.3	0.25	0.3
Row / Column Removal	0.65	0.5	1	0.75
Cropping	0.62	0.76	0.89	0.85
Rescale	0.53	0.75	0.78	1
Rotation	0.5	0.52	1	0.98
Affine	0.35	0.45	0.98	0.83
Geometrical Distortions	0.64	0.75	0.37	0.75
Shearing	0.35	0.42	1	0.6

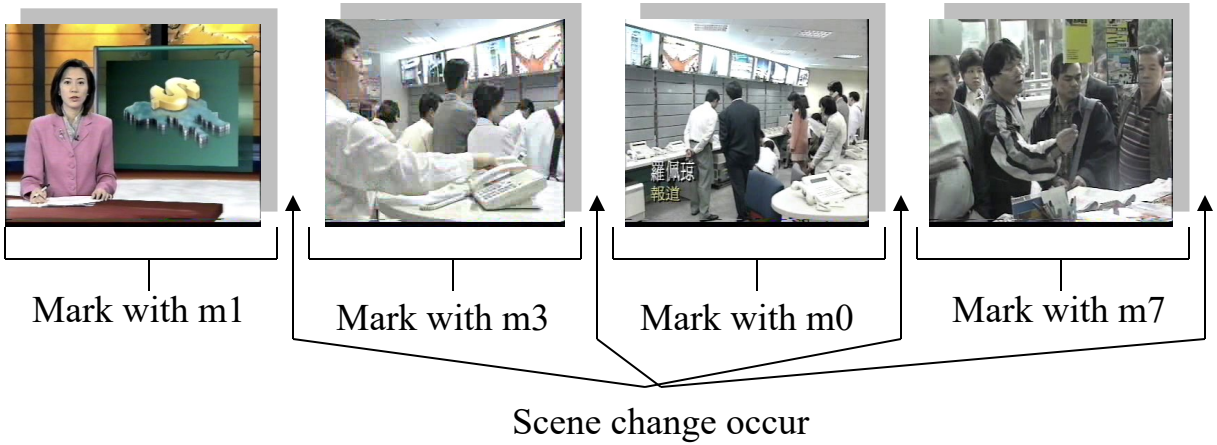
Scene-based Watermarking Scheme Overview

- Video Preprocess
- Watermark Preprocess
- Video Watermark Embedding
- Watermark Extraction



Video Preprocess: DWT & Scene Change Detection

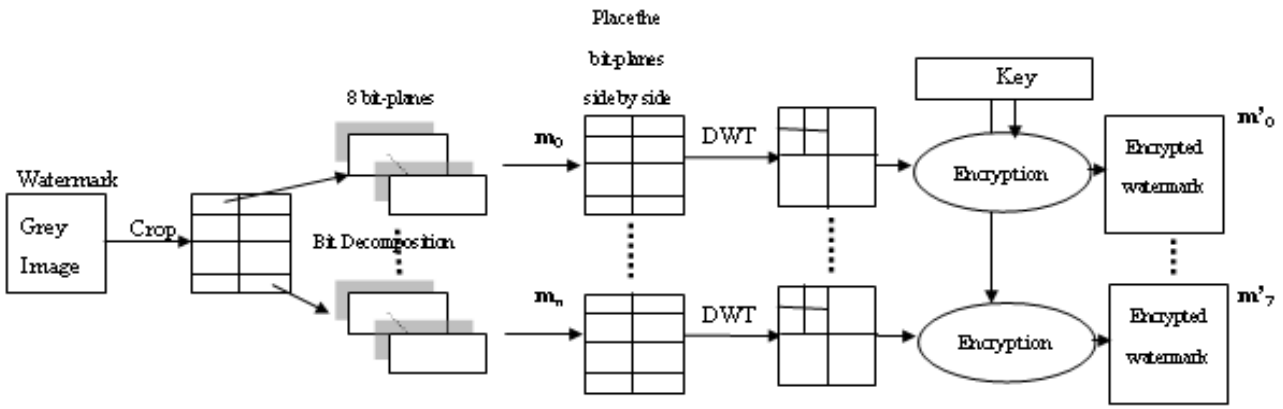
- Video frames are transformed to wavelet domain.
- Perform scene change detection.
- Each scene is embedded with the same watermark, so it can prevent attackers from removing the watermark by frame dropping.
- Different watermarks used for successive different scene can prevent attackers from colluding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



Watermark Preprocess

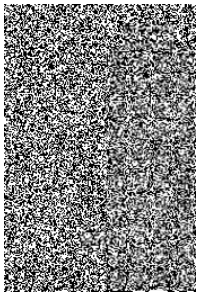
- Scale the watermark to a particular size with the following equations
  - $2^n \leqq m$, n>0
  - p + q = n , p and q > 0
  - Size of image = $64 \cdot 2^p$ X $64 \cdot 2^q$
- Divide the image into 2^n small images with size 64 X 64

m -- # of scene change of the video

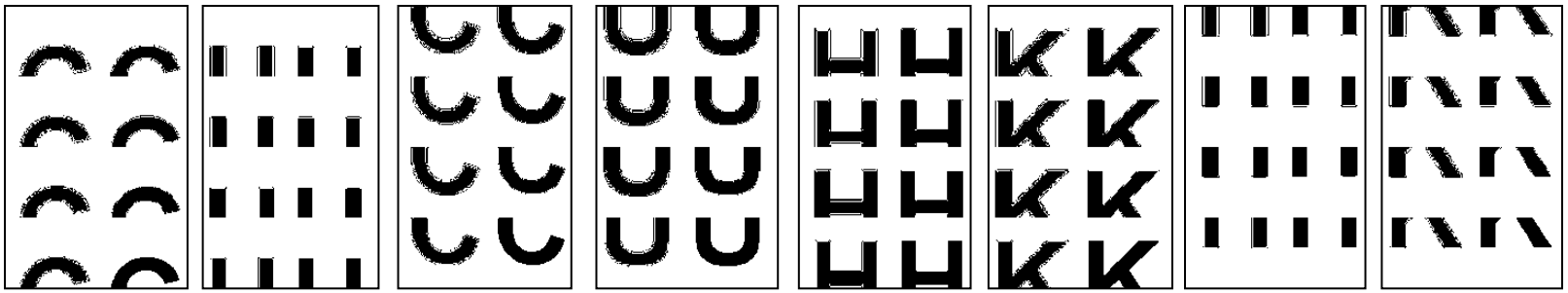


m=10, n=3, p=1, q=2

Watermark Preprocess



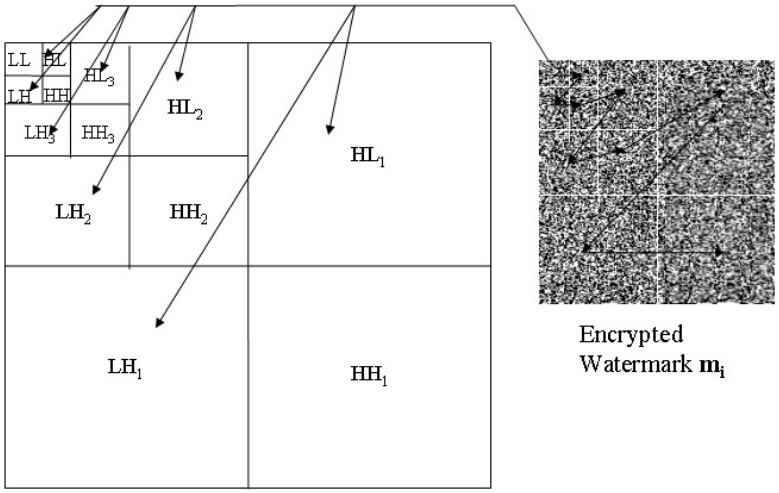
Original watermark **Encrypted watermark m'_0**



Preprocessed watermark m_0-m_7

Video Watermark Embedding

- *if W_j = 1,*
  - *Exchange C_i with max (C_i, C_{i+1}, C_{i+2}, C_{i+3}, C_{i+4})*
- *else*
  - *Exchange C_i with min (C_i, C_{i+1}, C_{i+2}, C_{i+3}, C_{i+4})*
- LL, HH coefficients are not watermarked



Video Watermark Extraction

- *if* $WC_i > median\ (WC_i, WC_{i+1}, WC_{i+2}, WC_{i+3}, WC_{i+4})$
  - $EW_j = 1$
- *else*
  - $EW_j = 0$

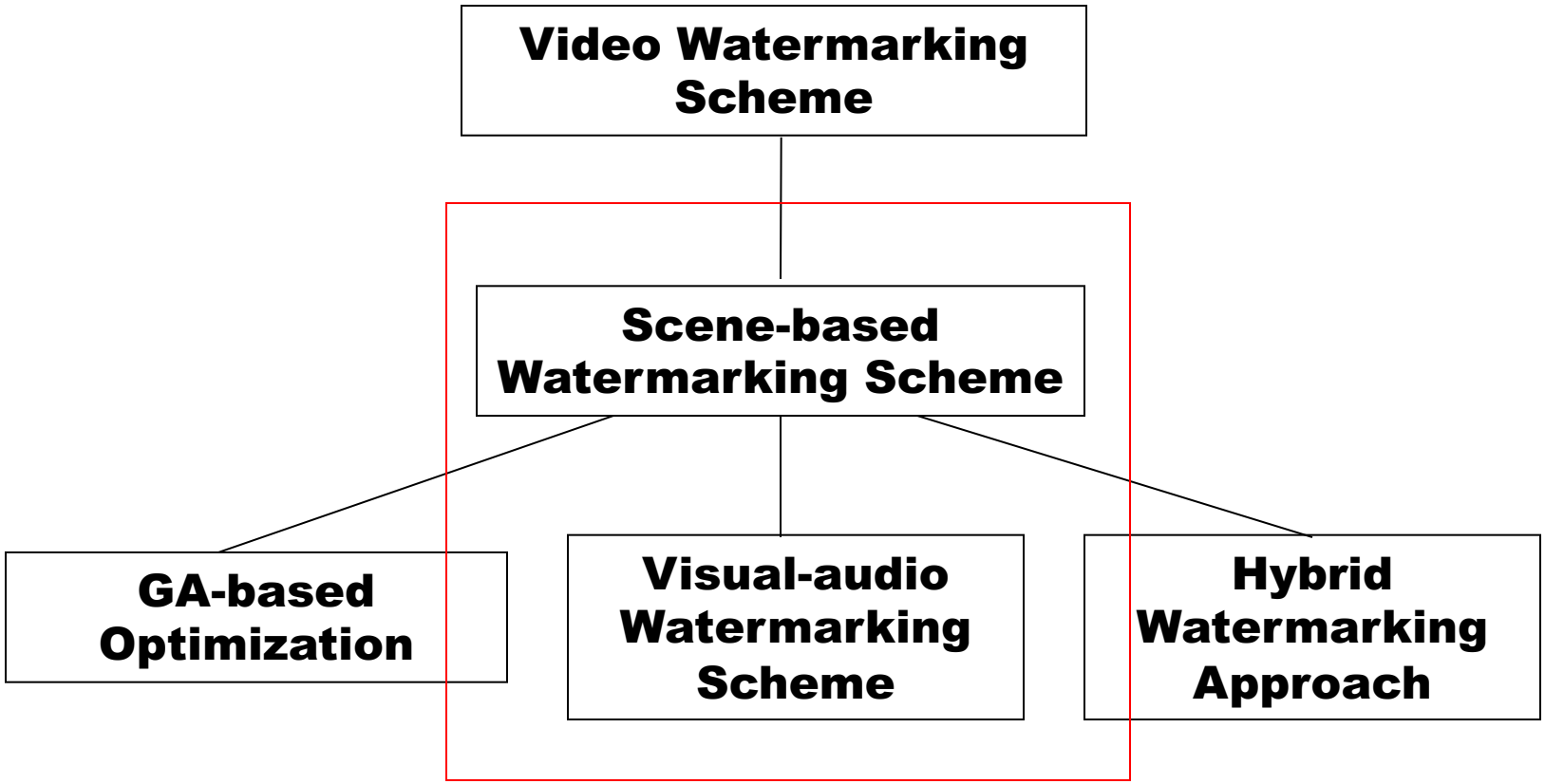
Original video frame

Watermarked video frame

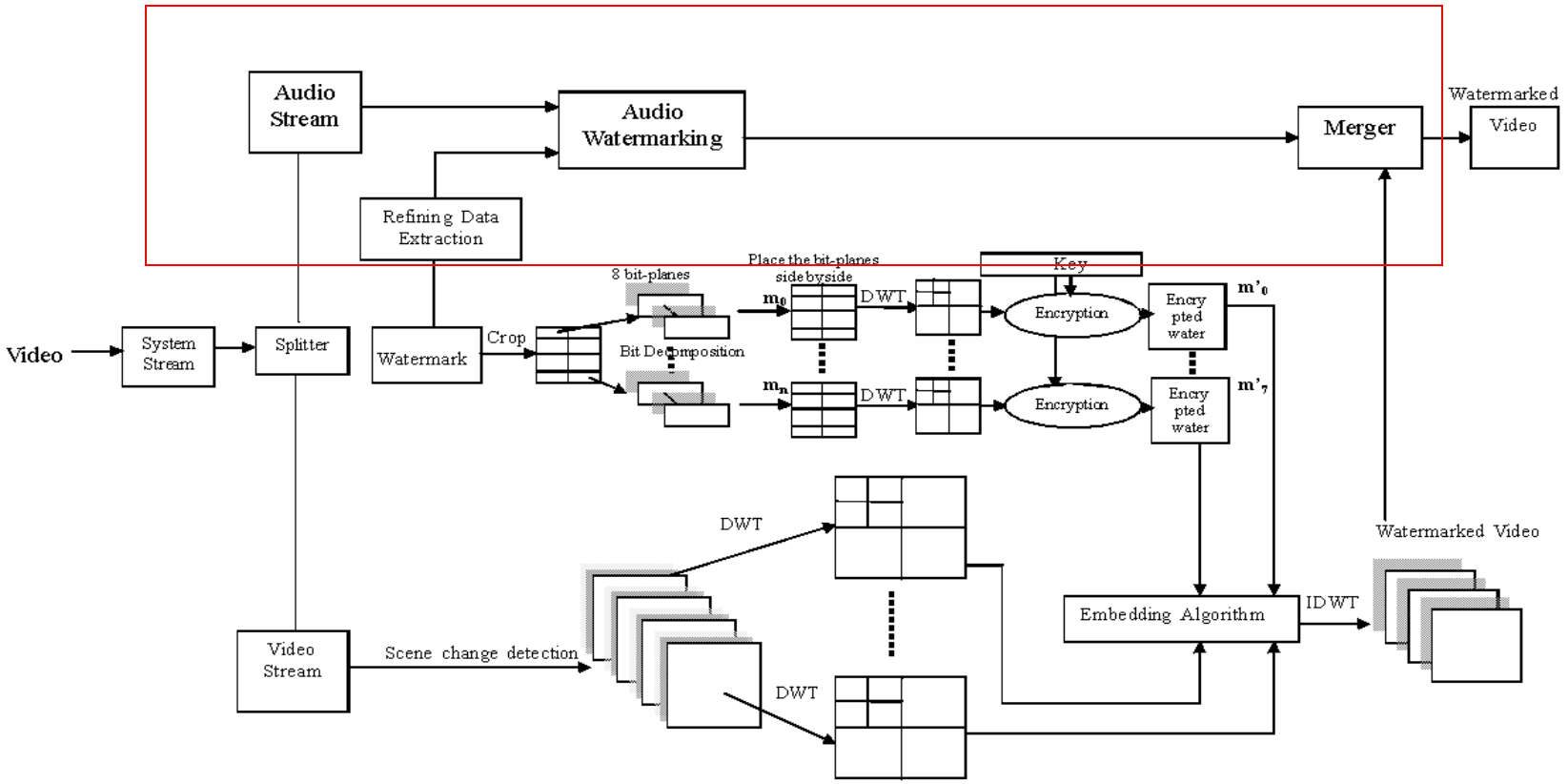
Extracted Watermark

Recovered Watermark

Possible Improvement



Visual-audio Watermarking Scheme Overview

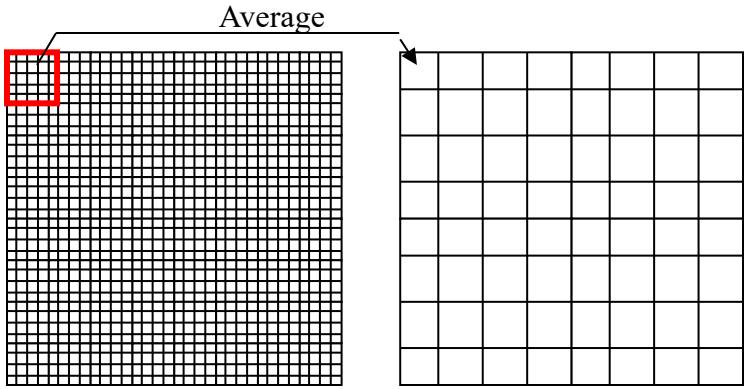


Audio Watermark

- Error correcting code is extracted from the watermark image

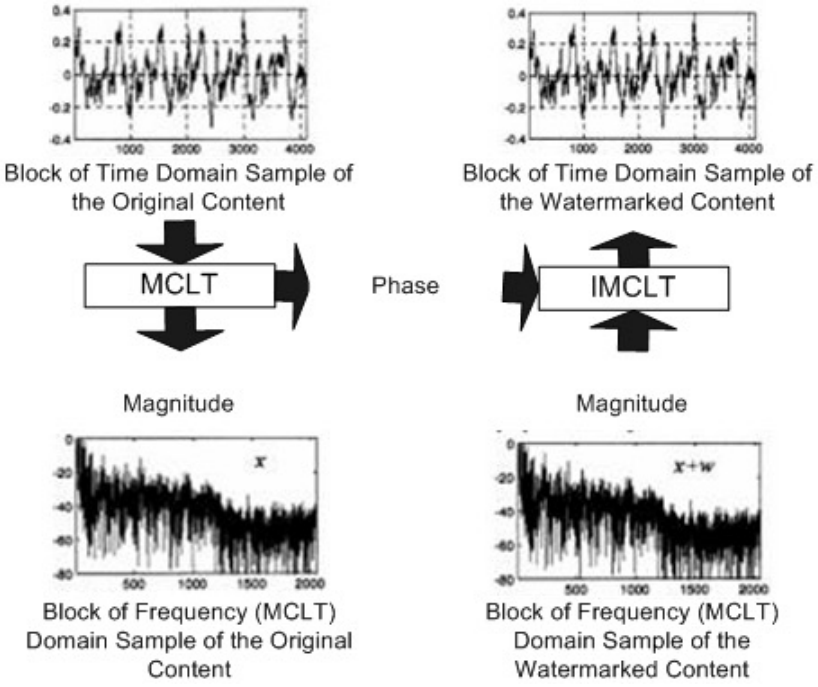
$$Avg_k = \sum_{i=0}^{x} \sum_{j=0}^{y} W_{j*z+r*x+s*y*z+i}$$

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



Audio Watermark Embedding

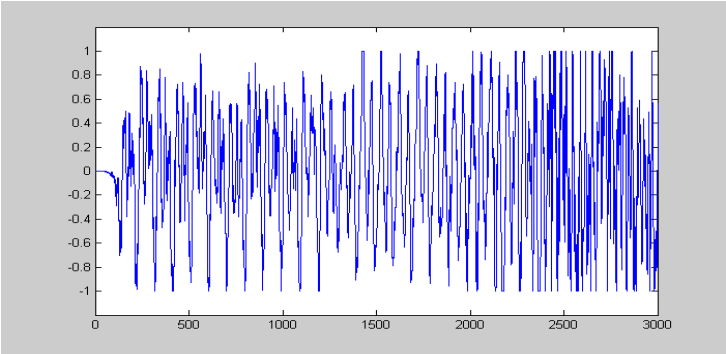
- Spread-Spectrum Watermarking
- Modulated Complex Lapped Transform (MCLT)

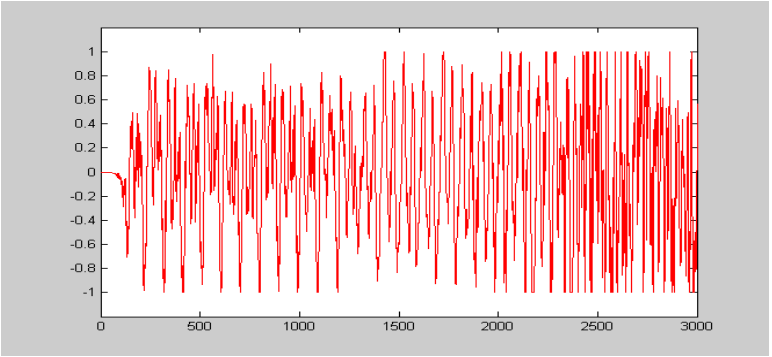


Watermarked Frame & Wave

Original video frame and wave

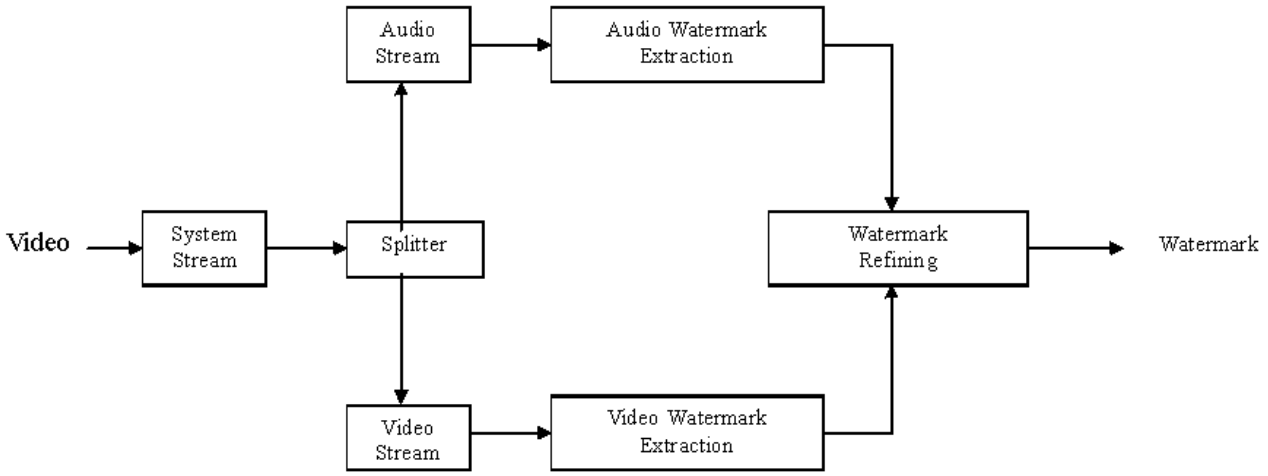
Watermarked video frame and wave





Watermark Extraction

- Video is split into video stream and audio stream.
- Watermarks are extracted separately by audio watermark extraction and video watermark extraction.
- Then the extracted watermark undergoes refining process



Watermark Refining

- Error correcting codes are extracted from the audio stream.
- The video watermark extracted is refined by this information with the following equation

$$RW_{ij} = \frac{(EW_{ij} \times f + Avg_k \times g)}{f + g}$$

  - RW_{ij} is the refined watermark
  - EW_{ij} is the extracted video watermark
  - Avg_k is the extracted audio watermark,
  - k is the k^{th} block of the average image,
  - (i, j) is coordinate of the video watermark,
  - f:g is a ratio of importance of the extracted video watermark to the audio watermark.

Performance & Capacity

- **m** = no. of scene, $\mathbf{n_1}$ **x** $\mathbf{n_2}$ = size of frame,
  T = no. of frame, $\mathbf{m_1}$ **x** $\mathbf{m_2}$ = size of watermark
- Performance = $O\left\{\max\left[\left(m_1, m_2\right), m\right]\right\} + O(n_1 n_2 T) + O(n_1 n_2 T)$
  = $O(n_1 n_2 T)$
- Capacity = $C_{\min} = \frac{1}{2}\log\left(2\pi e\right)^n \left| f\left(S\right) + E\left(ZZ^T\right)\right| - \frac{1}{2}\log\left(2\pi e\right)^n \left| E\left(ZZ^T\right)\right|$
  = $\frac{1}{2}\left| f\left(S\right) + E\left(ZZ^T\right)^{-1}\right| + I$
- When noise is Gaussian distribution, $C = \sum_{i=1}^{n} \frac{1}{2}\log\left(1 + \frac{P_i}{N_i}\right)$

Experimental Setup

- VirtualDub -- a video capture/processing utility (http://www.virtualdub.org/)
- A video clip with 1526 frames of size 352 X 288
- A DWT-based watermarking scheme for comparison
- Experiments:
  - Experiment with frame dropping
  - Experiment with frame averaging and statistical analysis
  - Experiment with lossy compression
  - Experiment with StirMark 4.0
- Measurement, Normalized Correlation:

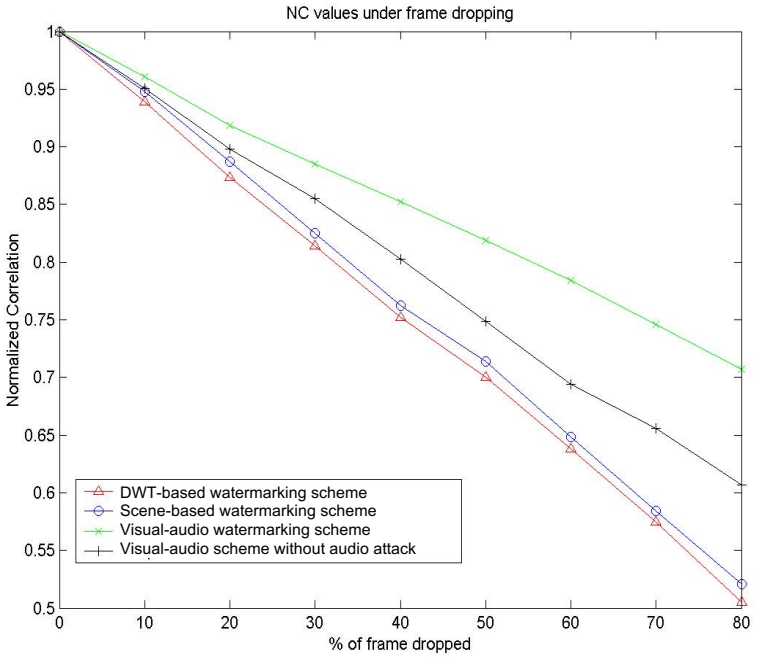
$$NC = \frac{\sum_i \sum_j W_{ij} \times RW_{ij}}{\sum_i \sum_j W_{ij}^2}$$

Experiment with Frame Dropping

- As a video contains a large amount of redundancies between frames, it may suffer attacks by frame dropping.
- This experiment is aimed to examine the robustness of the scheme under attack by frame dropping.

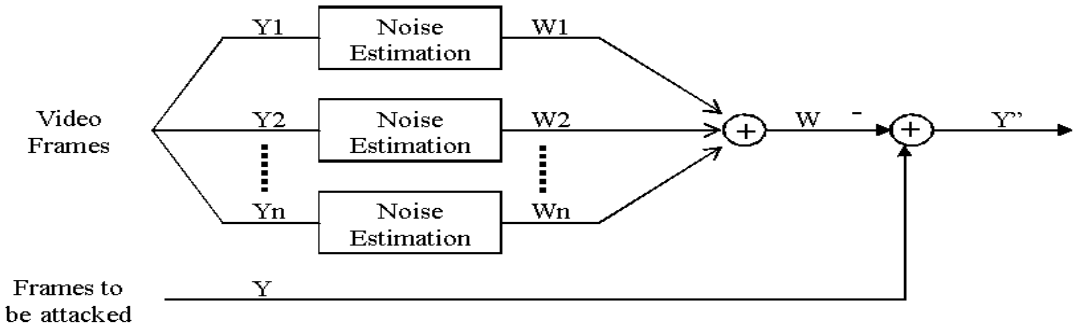
Experiment with Frame Dropping

- When frames are dropped, the error is only introduced to a corresponding small part of the watermark.
- The performance of the scheme is significantly improved by combining with an audio watermark, especially when the dropping rate of video frame is high.
- When the dropping rate increases, the error of the extracted watermark is increased. The error correcting code from the audio watermark provides information to correct the error and overcome the corrupted part of the video watermark.



Experiment with Frame Averaging and Statistical Analysis

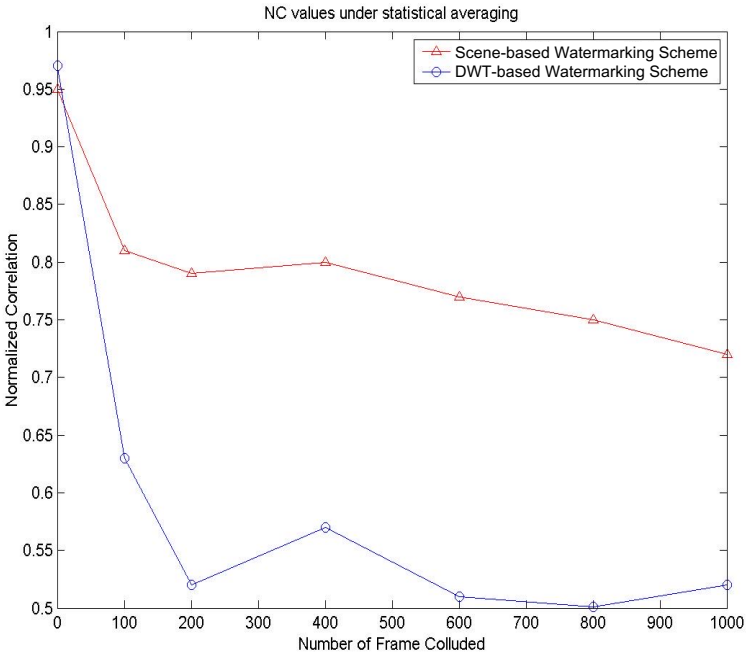
- Frame averaging and statistical analysis are other common attacks to the video watermark.
- When attackers collect a number of watermarked frames, they can estimate the watermark by statistical averaging and remove it from the watermarked video.



Scenario of statistical averaging attack

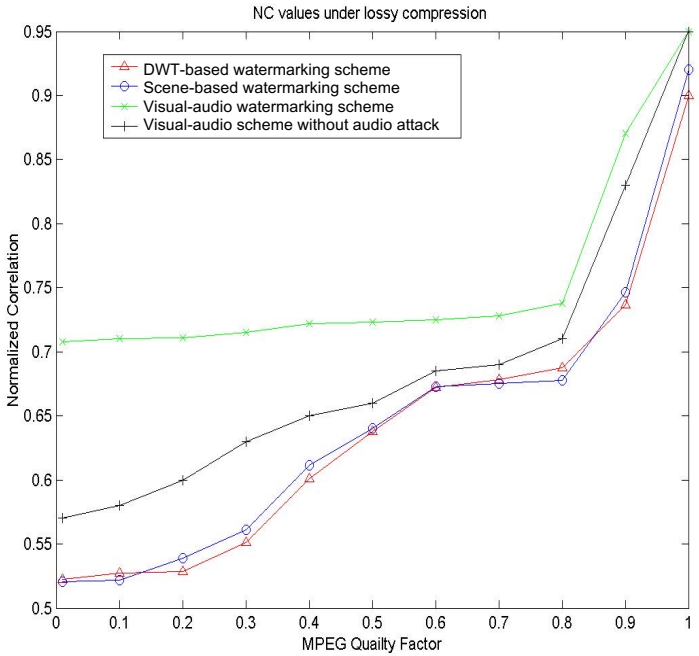
Experiment with Frame Averaging and Statistical Analysis

- The watermarked video is statistically analyzed by colluding a number of video frames and the watermarks are extracted and NC values are obtained.
- The identical watermark used within a scene can prevent attackers from taking the advantage of motionless regions in successive frames and removing the watermark by comparing and averaging the frames statistically.
- Independent watermarks used for successive, but different scenes can prevent attackers from colluding with frames from completely different scenes to extract the watermark.



Experiment with Lossy Compression

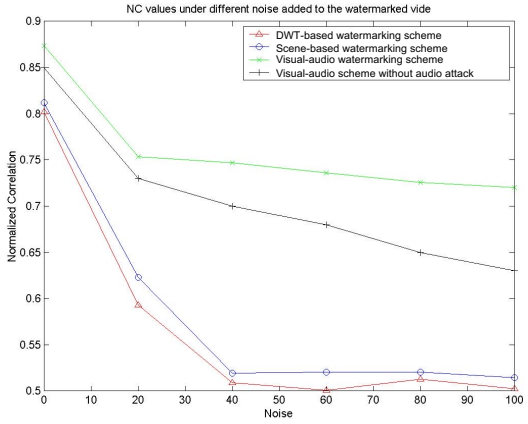
- The performance of the scheme is significantly improved by combining with audio watermark, especially when the quality factor of MPEG is low.
- When the quality factor of MPEG is low, the error of the extracted watermark is increased and the watermark is damaged significantly.
- As the error correcting code is provided from the audio watermark, it can survive the attack by lossy compression which is applied to the video channel.

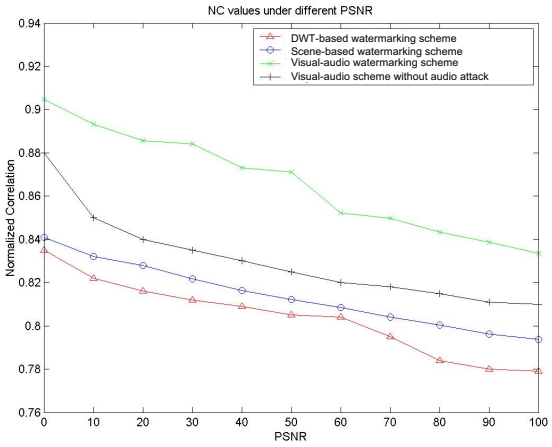


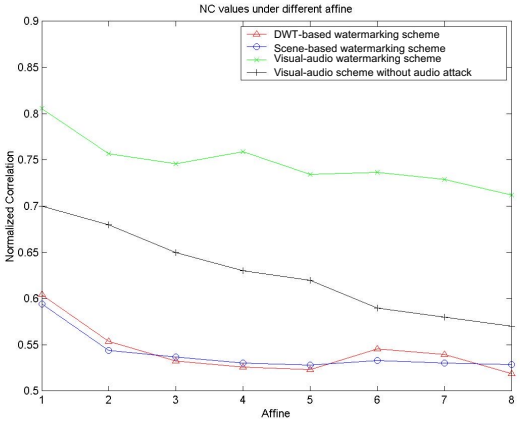
Experiment with StirMark 4.0

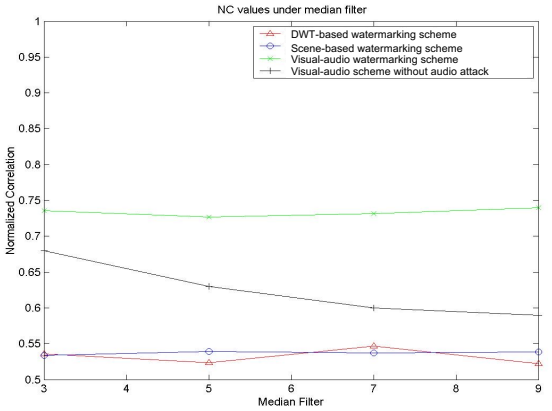
- The pervious experiments show the effectiveness of the proposed scene-based watermarking scheme when the specification of attacks to video's properties is applied, including frame dropping, averaging and statistical analysis.
- StirMark 4.0 is a benchmark to examine the robustness of the watermarking scheme against attacks by image processing.

Experiment with StirMark 4.0





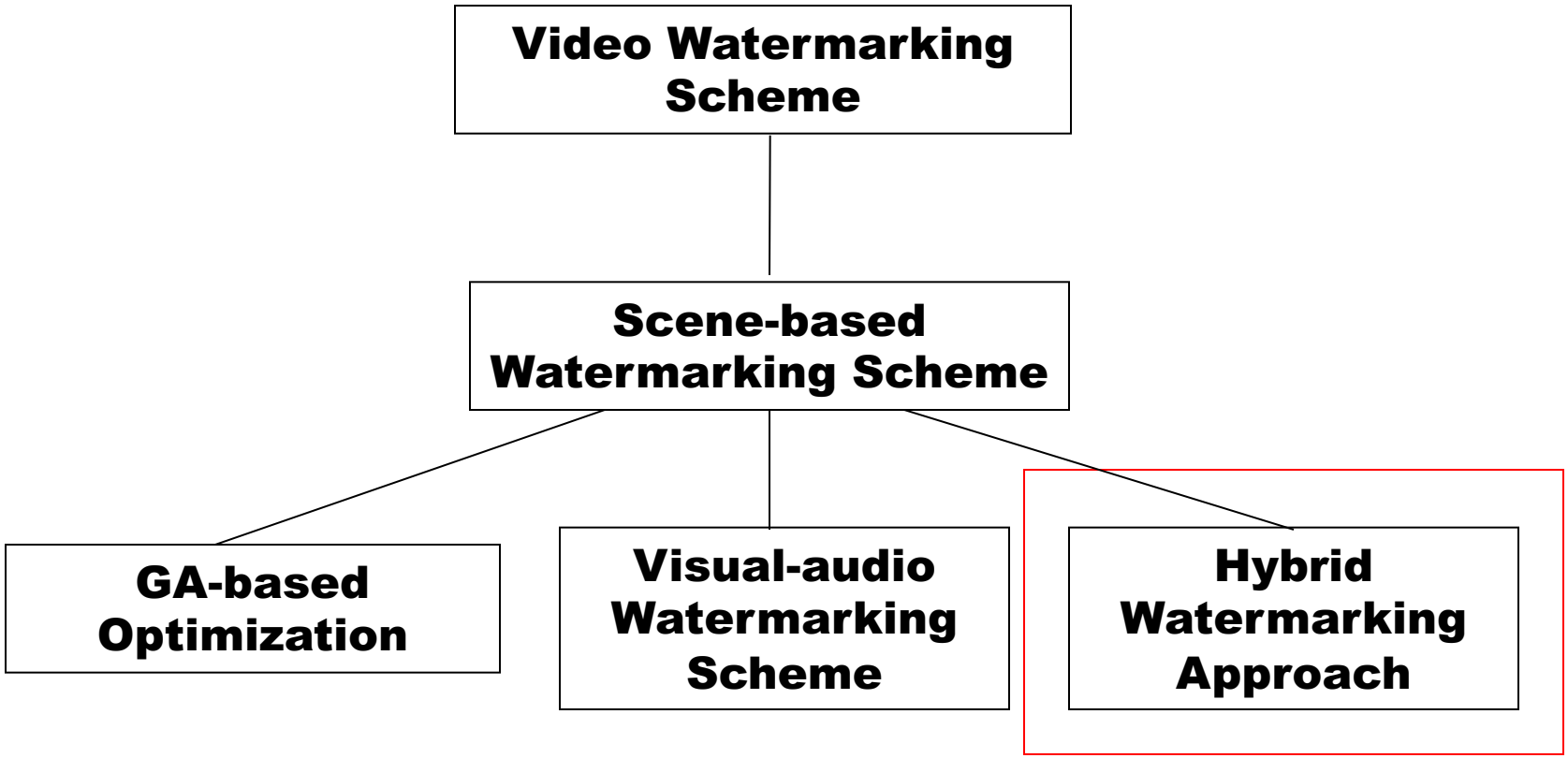




Experiment with StirMark 4.0

Attack Class	DWT-based Watermarking Scheme	Scene-based Watermarking Scheme	Visual-audio Watermarking Scheme	Visual-audio Watermarking Scheme with audio attack
Lossy Compression	0.61	0.62	0.82	0.69
PSNR	0.80	0.81	0.86	0.80
Add Noise	0.63	0.60	0.76	0.67
Median Filter	0.54	0.54	0.74	0.60
Row / Column Removal	0.75	0.73	0.85	0.75
Cropping	0.68	0.66	0.78	0.70
Rescale	0.63	0.62	0.75	0.69
Rotation	0.60	0.61	0.73	0.67
Affine	0.55	0.55	0.78	0.70

Possible Improvement

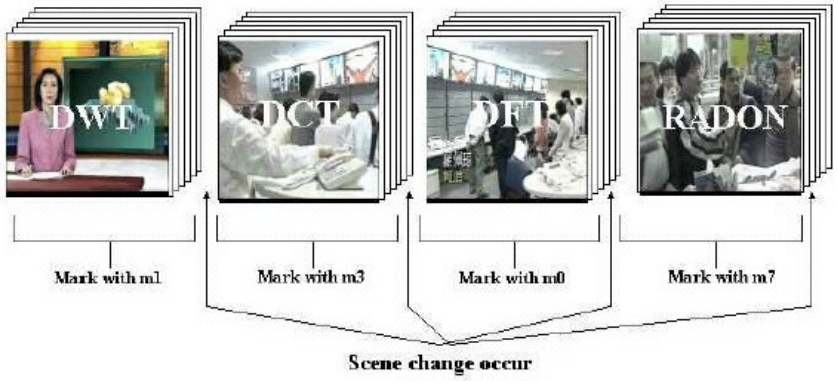


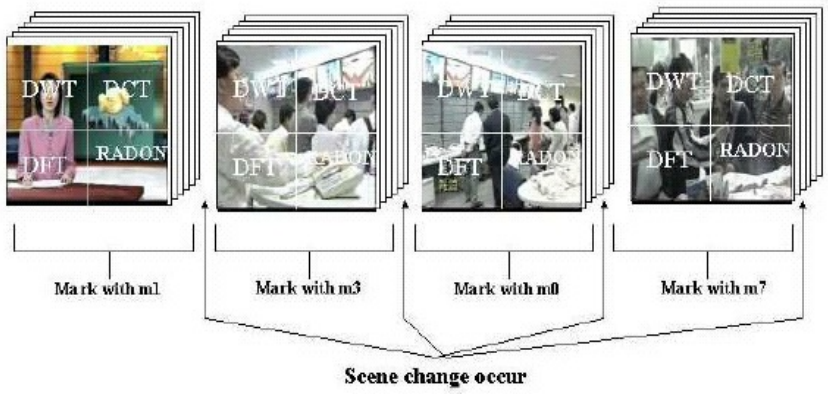
Hybrid Approach with Different Watermarking Scheme

- No watermarking scheme found in the current technologies is capable of resisting to all watermark attacks.
- We propose hybrid approach as the solution.
- It combines alien schemes in disparate ways.
- Four schemes are chosen, each of which strives a different set of attacks: Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and RADON Transform based watermarking schemes.
- We propose 2 approaches to combine the schemes, which can be classified into two types:
  - Independent watermarking scheme
  - Dependent watermarking scheme

Independent Hybrid Watermarking Scheme

- The watermarks are embedded into the frame with different watermarking scheme in various domains.
- The schemes are not affecting each other.
- There are two approaches to combine the schemes:
  - Different schemes for different scenes
  - Different schemes for different parts of frames





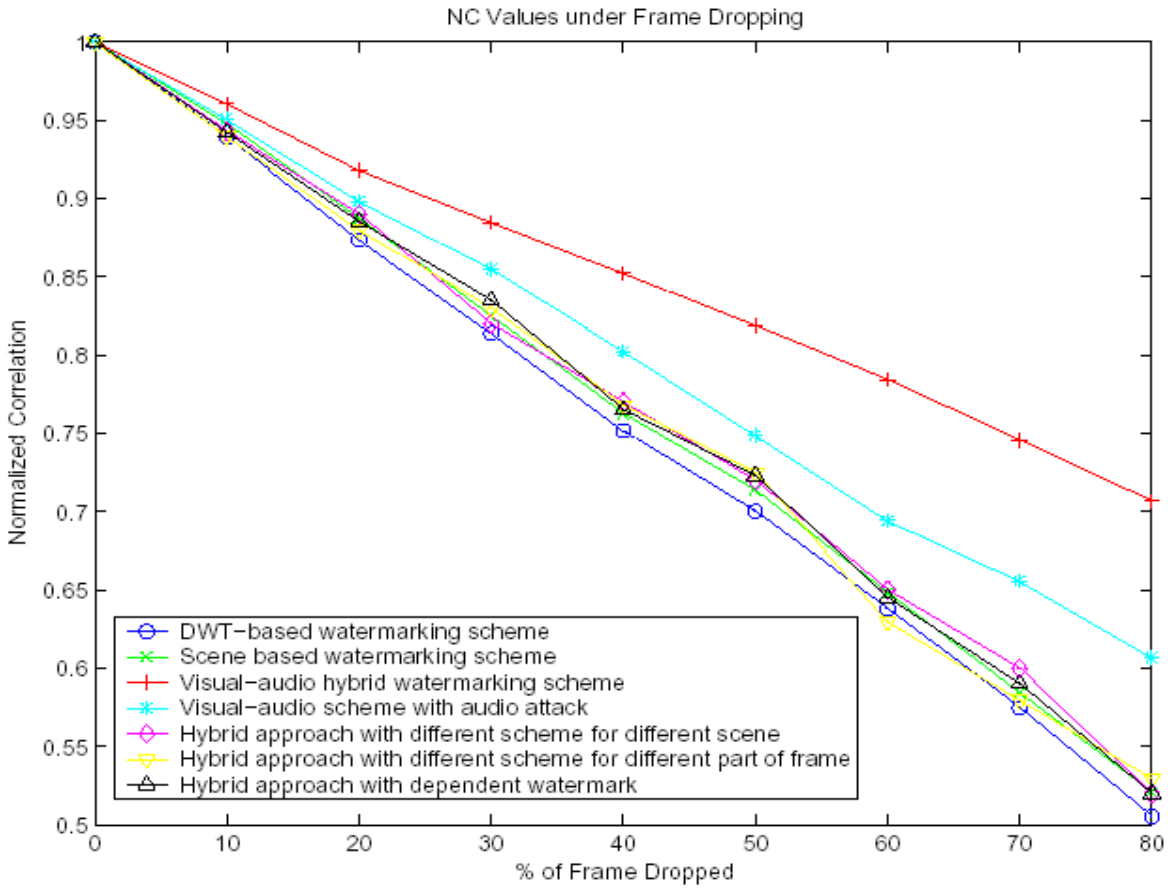
Independent Hybrid Watermarking Scheme

- When there is an attack on the watermarked video, different watermarking schemes are resistant against various attacks.
- Consequently, some parts of the watermark still survive after the attack. This approach enhances the chance of survival of the watermark under several attacks.

Dependent Hybrid Watermarking Scheme

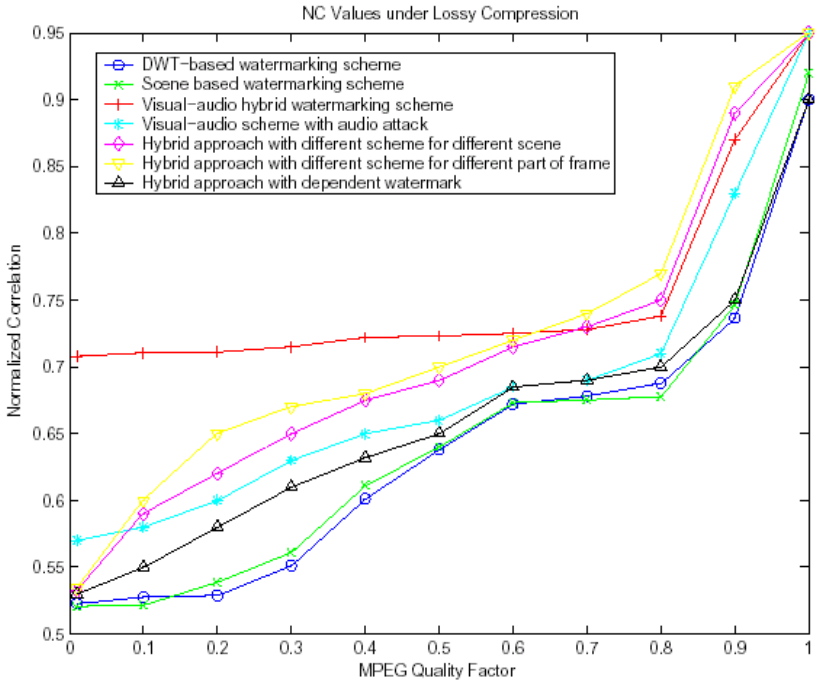
- The same watermark is embedded serially in a frame with different watermarking scheme in various domains.
- For each frame, four different watermarking schemes are applied.
- DWT→ DFT→DCT→Radon Transform

Experiment with Frame Dropping

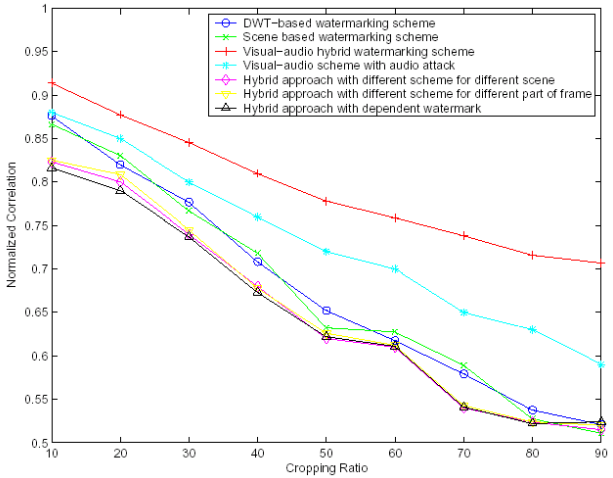


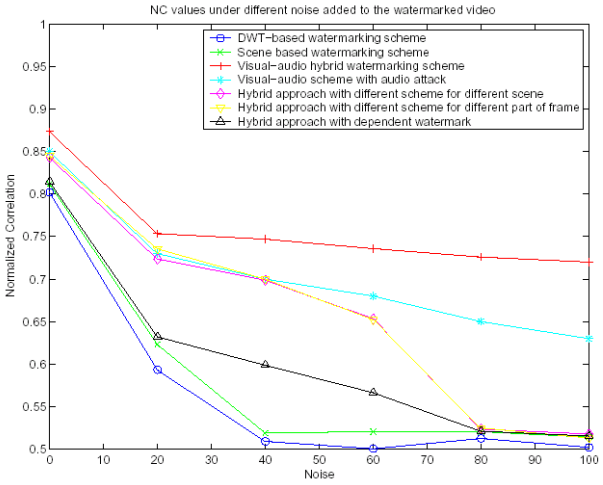
Experiment with Lossy Compression

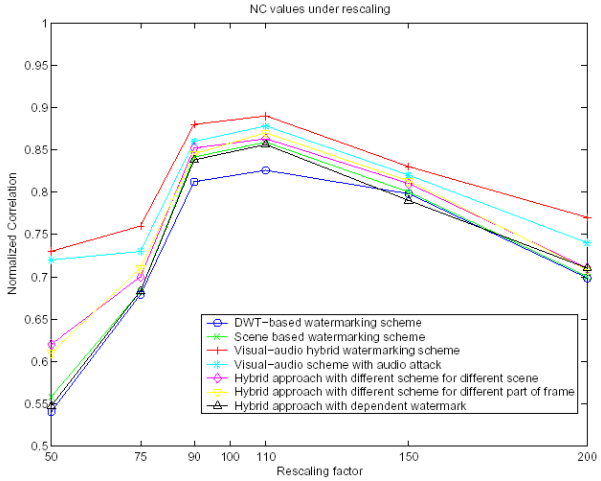
- The performance of the scheme is significantly improved by combining with audio watermark, especially when the quality factor of MPEG is low.
- However, when there is audio attack, the NC value is not improved much.
- The performance of the scheme is improved by hybrid approach with different watermarking schemes.
- When compression is applied to the watermarked video, the watermark embedded in the video with DCT-based watermarking scheme is survived. Therefore, at least one forth of the watermark can be retrieved from the video.

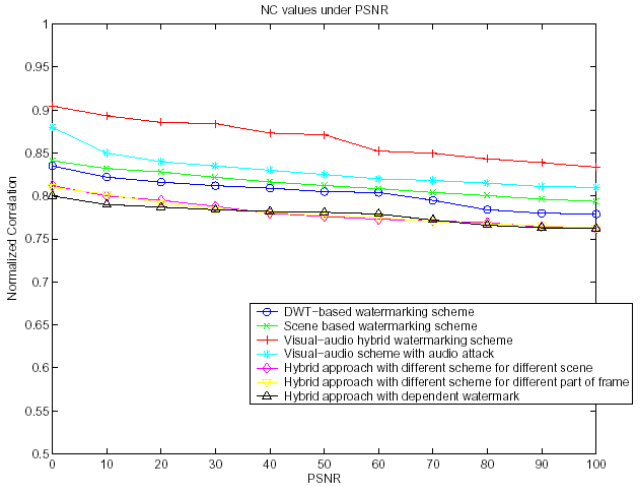


Experiment with StirMark 4.0





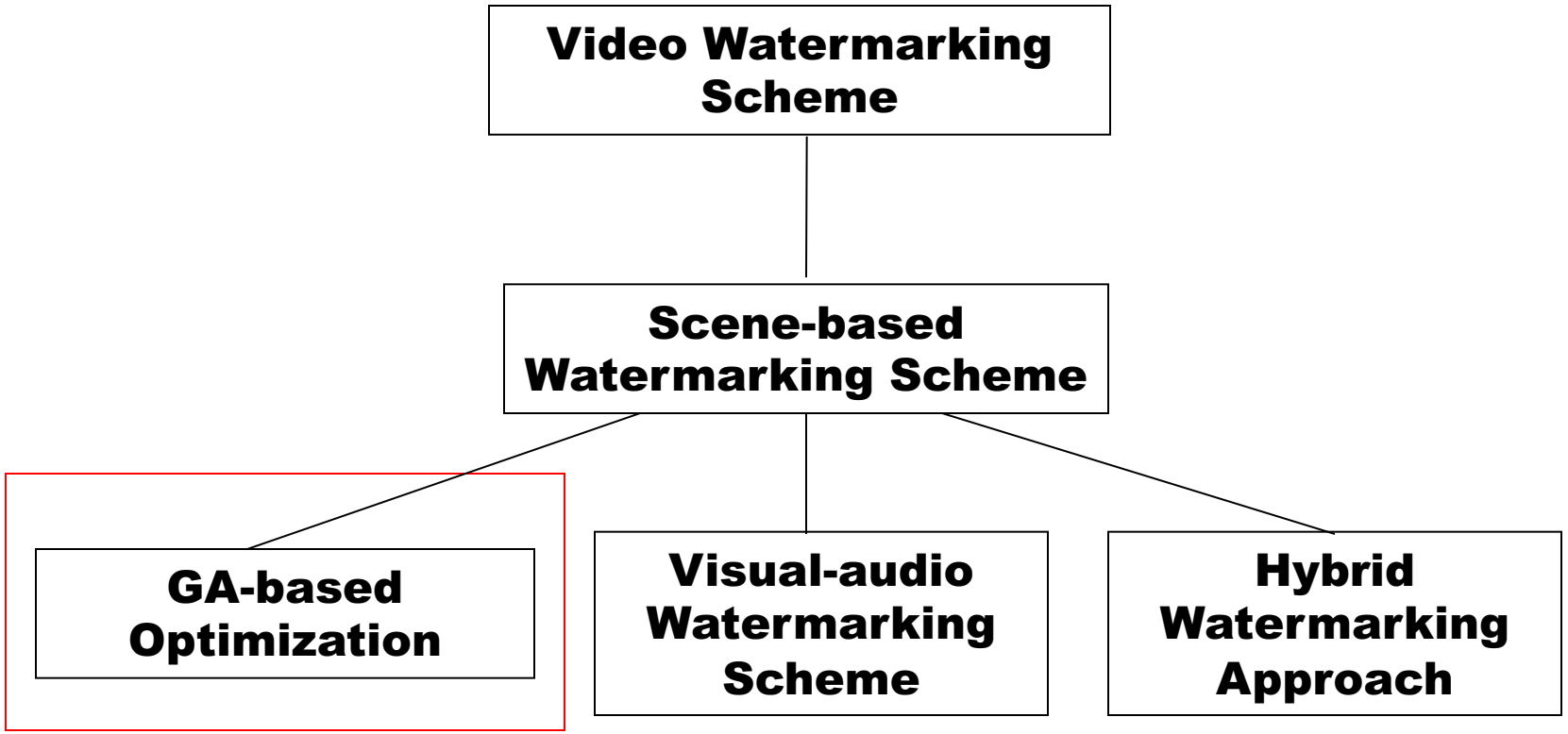




Experiment with StirMark 4.0

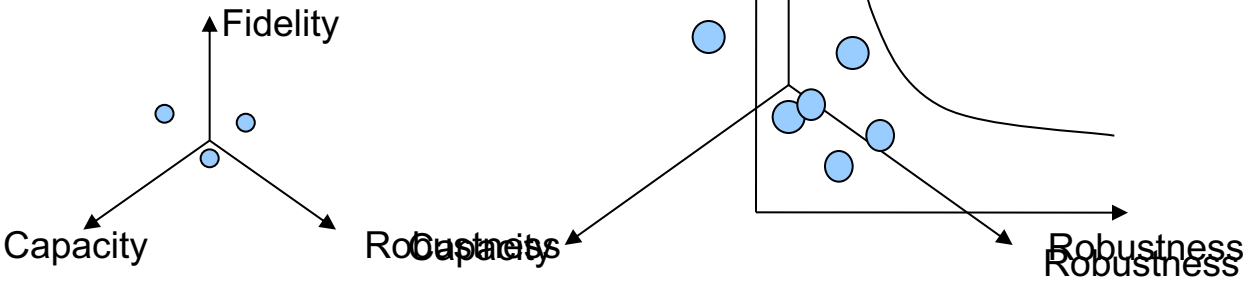
Attack Class	DWT-based Scheme	Scene-based Scheme	Visual-audio Scheme	Visual-audio Watermarking Scheme with audio attack	Hybrid approach with different scheme for different scene	Hybrid approach with different scheme for different part of frame	Hybrid approach with dependent watermark
Lossy Compression	0.61	0.62	0.82	0.69	0.71	0.72	0.68
PSNR	0.80	0.81	0.86	0.80	0.82	0.81	0.81
Add Noise	0.63	0.60	0.76	0.67	0.70	0.69	0.64
Median Filter	0.54	0.54	0.74	0.60	0.55	0.52	0.52
Row / Column Removal	0.75	0.73	0.85	0.75	0.77	0.78	0.74
Cropping	0.68	0.66	0.78	0.70	0.72	0.69	0.67
Rescale	0.63	0.62	0.75	0.69	0.71	0.68	0.63
Rotation	0.60	0.61	0.73	0.67	0.69	0.66	0.64
Affine	0.55	0.55	0.78	0.70	0.73	0.71	0.63
Overall	0.62	0.63	0.78	0.69	0.71	0.70	0.66

Possible Improvement



A Genetic Algorithm-based Video Watermarking Scheme

- The problem of designing a feasible watermarking scheme can be viewed as an optimization problem with three conflicting goals:
  - higher fidelity (media quality index),
  - better robustness (watermark strength),
  - larger data capacity.



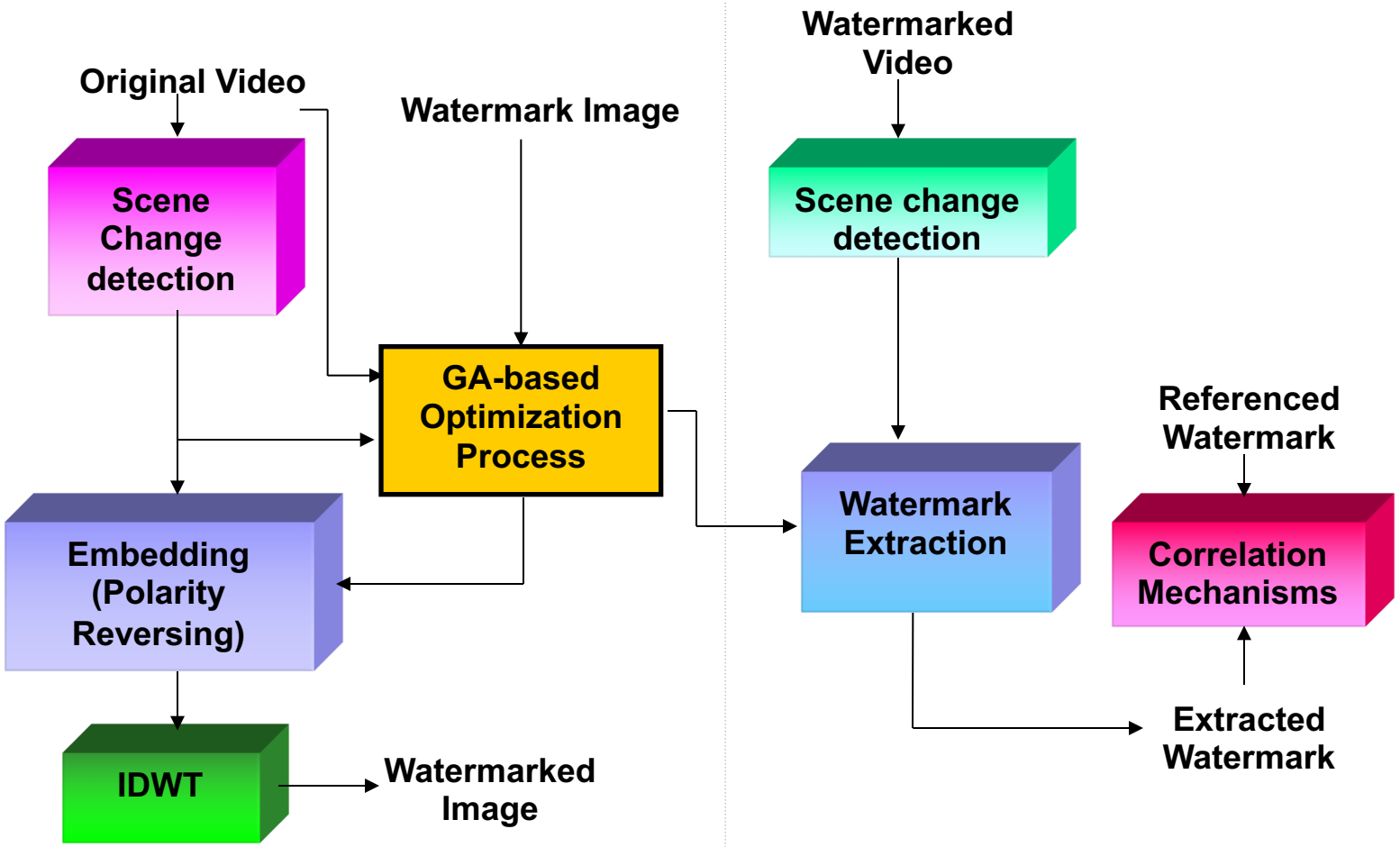
- The fidelity requirement often limits the strength of embedded signals, which consequently constrains the robustness of a watermarking scheme against common or malicious manipulations.

Problem Modeling

- Apply Genetic Algorithm (GA) to the scene-based video watermarking scheme.
- Embedding positions within a video are simulated as chromosomes.
- Find the best positions to embed watermark such that
  - Video keeps good quality
  - Watermark is robust against attacks
- Mean Absolute Difference (MAD) to measure the objective function values during optimization

$$f = \frac{1}{\sum_{x=0}^{7}\sum_{y=0}^{7}\left|I'(x,y) - I(x,y)\right|}$$

System Architecture



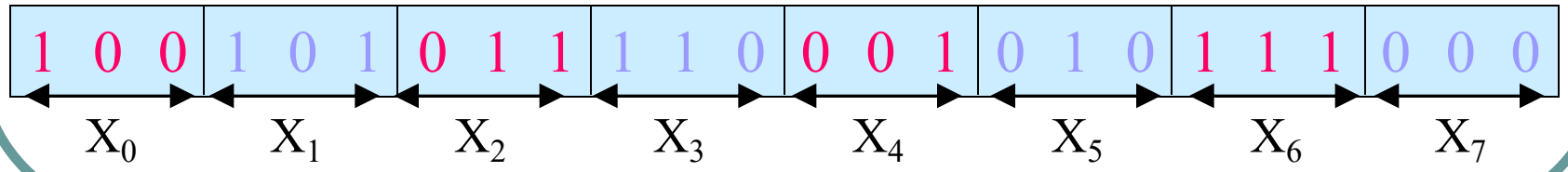
The GA-based watermarking algorithm

Chromosome Encoding

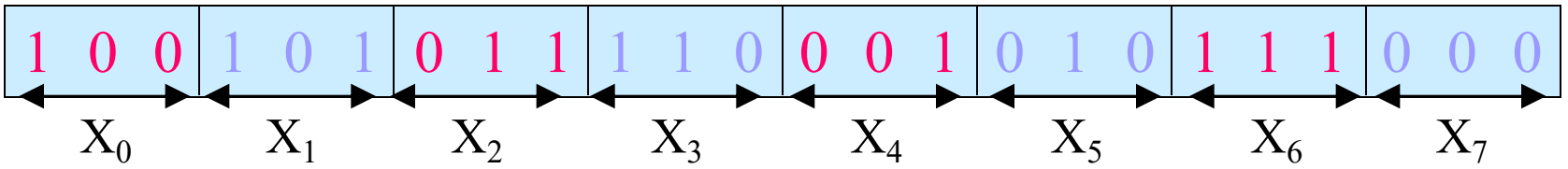
- Positions for each part of watermark;
- The i^{th} watermark to be embedded into which scene change can be defined as:

$$\{(Xi) \mid 0 \leqq Xi < M, \quad Xi \neq Xj \quad \text{if } i \neq j \text{ and } M > 1\}$$

- The last two constraints imply:
  - In a video, scenes which have been embedded should not be embedded again.
  - There are at least two scene changes.
- M = 8



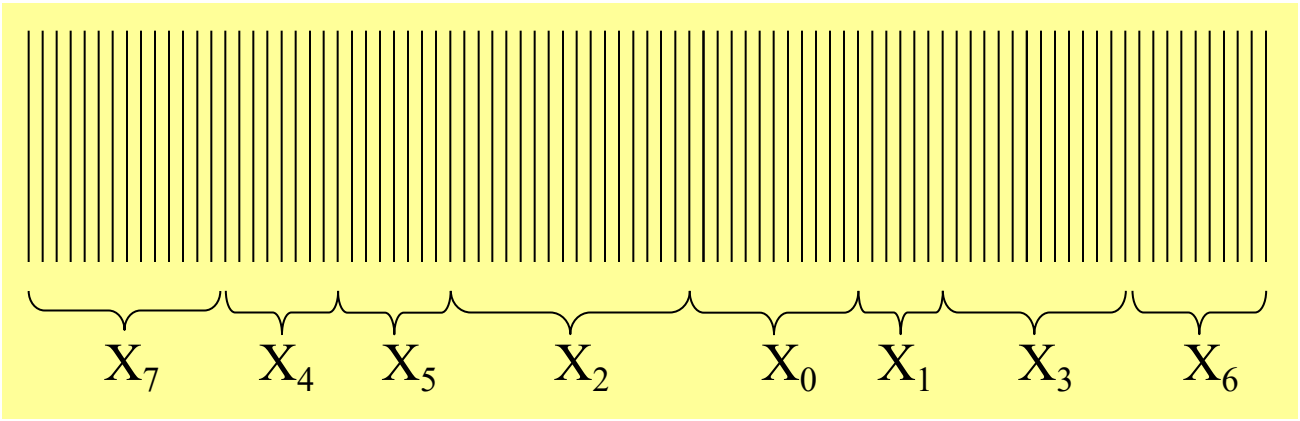
Chromosome Encoding



Chromosome

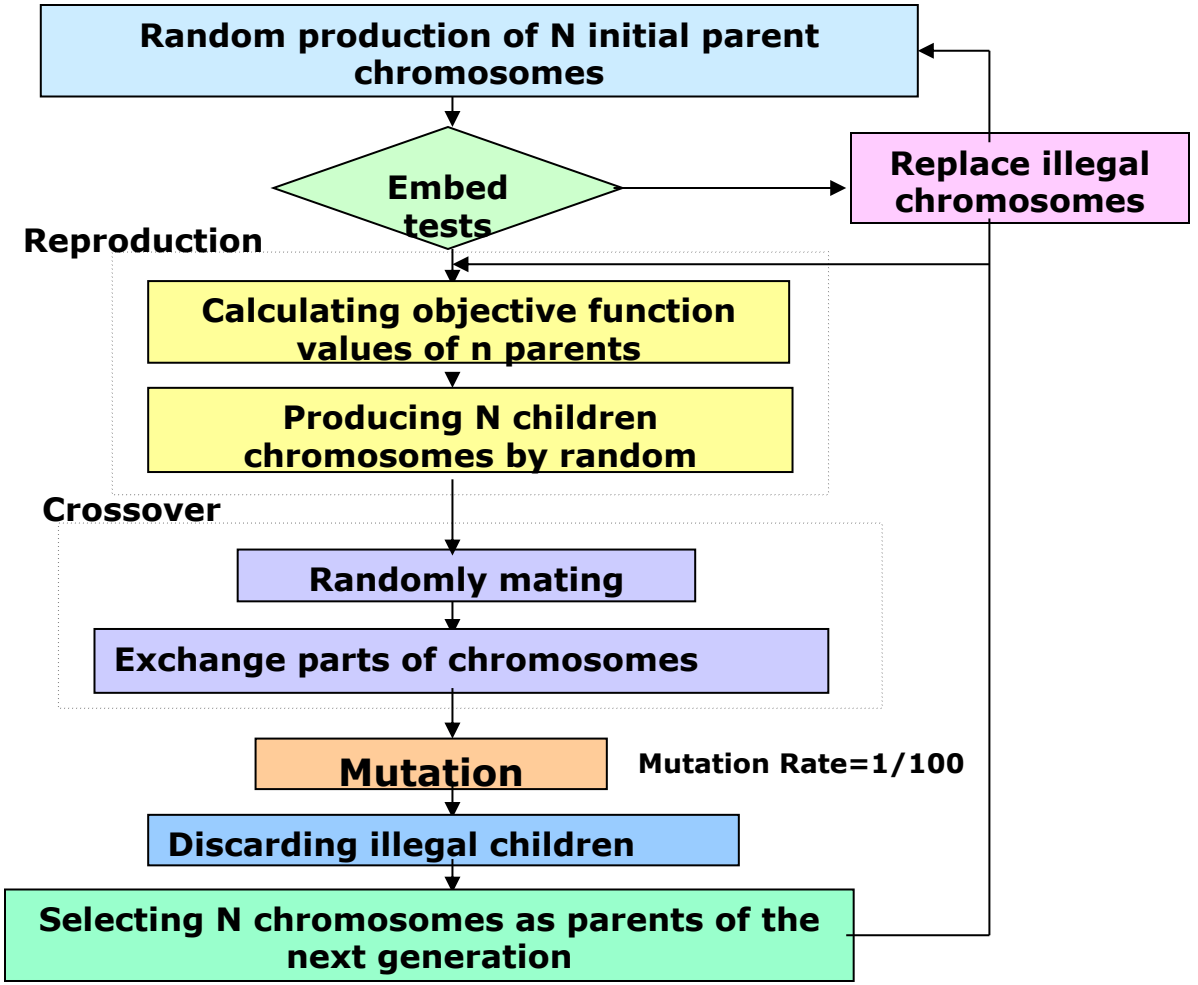
X_0	X_4
X_1	X_5
X_2	X_6
X_3	X_7

Watermark



Video Scenes

The GA-based Optimization Process



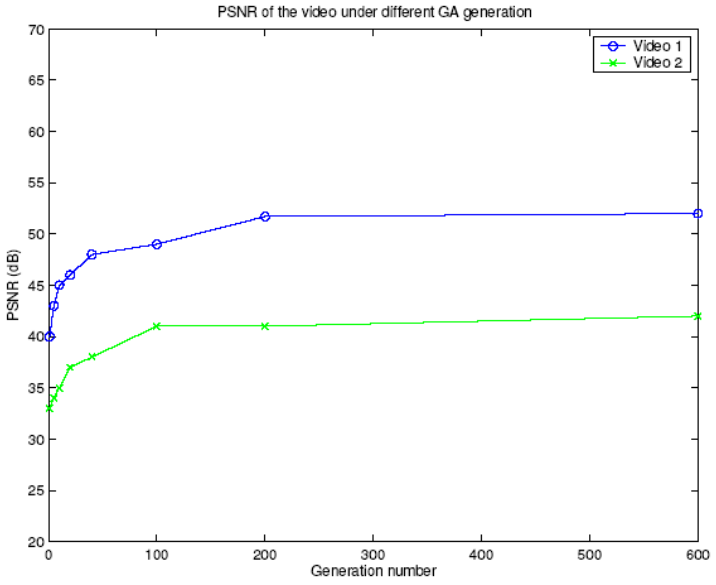
Experimental Setup

- GAlib -- the software for developing GA-related project. (http://lancet.mit.edu/ga/)
- 2 video clips 1. 1526 frames of size 352 x 288
  2. 4236 frames of size 352 x 288
- To evaluate the fidelity,
  - peak signal-to-noise ratio (PSNR) $PSNR = 10\log_{10}\frac{255^2}{\sigma_q^2}[dB]$
  - maximum absolute difference (MAD) $MAD = \sum_{x=0}^{7}\sum_{y=0}^{7}\left|I'(x,y) - I(x,y)\right|$
- Parameters setting for GA-based experiment

Parameter	Value
Population size	100
Mutation probability	0.05
Crossover probability	0.9
Score frequency	1
Flush frequency	25
Number of generations	In the experiment,we have used 0, 1, 5, 10, 20, 40, 100, 200, 400 and 600

Evaluation with PSNR

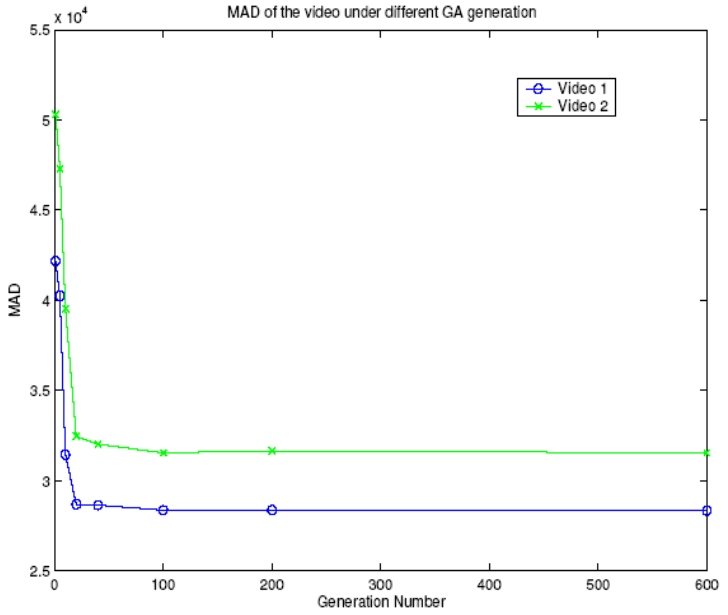
- PSNR measures the signal to noise ratio of the watermarked video.
- The GA-based algorithm successfully reduces the video frame distortion.
- As the number of generations increases, the improvement of video quality gradually approaches to a saturation value.
- The PSNR of the video is ¼ more than other schemes after GA is applied.
- It shows that the GA-based optimization effectively improves the performance of the scheme.



Watermarking scheme	PSNR of Video 1	PSNR of Video 2
Scene-based Watermarking scheme	40	33
Visual-audio hybrid watermarking	41	33
Hybrid approach with different scheme for different scene	43	34
Hybrid approach with different scheme for different part of frame	42	36
Hybrid approach with dependent watermark	35	27
GA-based watermarking scheme watermark scheme	52	42

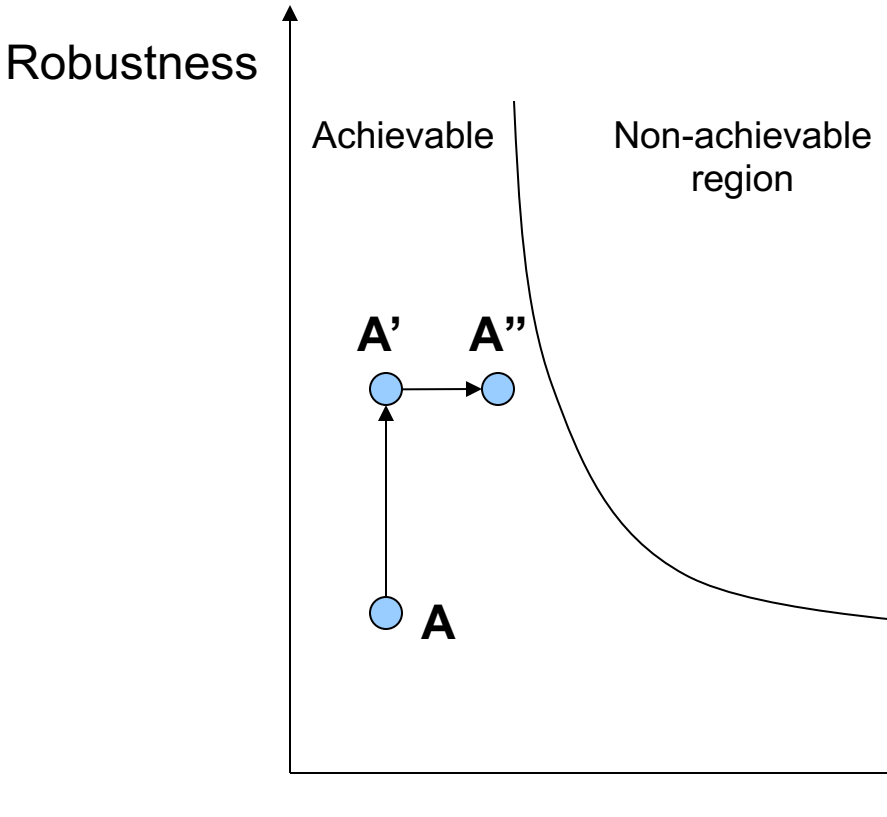
Evaluation with MAD

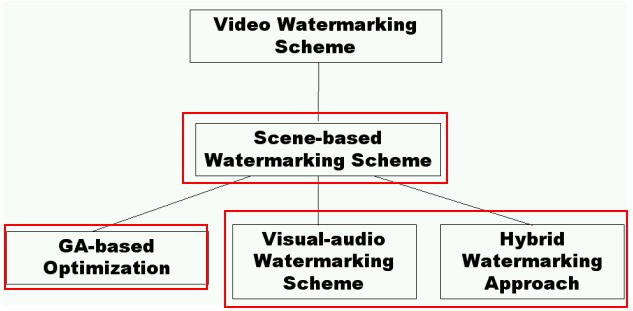
- MAD measures the difference between the original video and the watermarked video,
- The MAD of the watermarked video is decreased with the GA generation number.
- The optimization performance saturates after about 200 generations.
- The performance of the scheme quickly converges to an optimal value.
- The MAD of the video is reduced to 3/5 after GA is applied to optimize the fidelity of the scheme.



Watermarking scheme	MAD of Video 1	MAD of Video 2
Scene-based Watermarking scheme	42168	50325
Visual-audio hybrid watermarking	42189	50489
Hybrid approach with different scheme for different scene	43984	52695
Hybrid approach with different scheme for different part of frame	43798	52786
Hybrid approach with dependent watermark	48652	55785
GA-based watermarking scheme watermark scheme	28346	31546

Summary of Our Approach





Conclusion

- Video watermarking is needed since copyright protection is essential.
- A hybrid digital video watermarking scheme based on scene change analysis is proposed.
- Other possible improvements are presented and verified through different experiments.
- Our approach cultivates an innovative idea in embedding different parts of a watermark according to scene changes, in embedding its error correcting codes as an audio watermark, in applying hybrid approaches to enhance the scheme, and in employing the GA to improve the fidelity.
- Although the concept is quite simple, this approach is never explored in the literature, and its advantages are clear and significant.
- The effectiveness of this scheme is verified through a number of experiments.