A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code

Pik-Wah Chan and Michael R. Lyu*

Department of Computer Science and Engineering
The Chinese University of Hong Kong
Shatin, Hong Kong
{pwchan, lyu}@cse.cuhk.edu.hk

Abstract. In this paper, a digital video watermarking algorithm is proposed. We present a novel DWT-based blind digital video watermarking scheme with scrambled watermark and error correcting code. Our scheme embeds different parts of a single watermark into different scenes of a video under the wavelet domain. To increase robustness of the scheme, the watermark is refined by the error correcting code, while the correcting code is embedded as watermark in audio channel. Our video watermarking algorithm is robust against the attacks of frame dropping, averaging and statistical analysis, which were not solved effectively in the past. Furthermore, it allows blind retrieval of embedded watermark which does not need the original video; and the watermark is perceptually invisible. The algorithm design, evaluation, and experimentation of the proposed scheme are described in this paper.

1 Introduction

We have seen an explosion of data change in the Internet and the extensive use of digital media. Consequently, digital data owners can transfer multimedia documents across the Internet easily. Therefore, there is an increase in the concern over copyright protection of digital content [1, 2, 3]. In the early days, encryption and control access techniques were employed to protect the ownership of media. They do not, however, protect against unauthorized copying after the media have been successfully transmitted and decrypted. Recently, the watermark techniques are utilized to maintain the copyright [4, 5, 6]. In this paper, we focus on engaging the digital watermarking techniques to protect digital multimedia intellectual copyright and propose a new algorithm for video 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 [4]. However, the currently proposed algorithms do not solve these problems effectively. In our scheme, we attack this

* The work described in this paper was fully supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. CUHK4182/03E).

S. Qing, D. Gollmann, and J. Zhou (Eds.): ICICS 2003, LNCS 2836, pp. 202–213, 2003.

problem by applying scene change detections and scrambled watermarks in a video. The scheme is robust against frame dropping, as the same part of the watermark is embedded into the frames of a scene. For different scenes, different parts of the watermark are used, making the scheme robust against frame averaging and statistical analysis. At the same time, an audio watermark is included to enhance the robustness of the scheme. Error correcting code of a video watermark can be embedded as an audio watermark and used for refining the embedded watermark during detection.

Our approach cultivates an innovative idea in embedding different parts of a watermark according to scene changes, and in embedding its error correcting code as an audio watermark. 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.

This paper is organized into four sections. The next section presents the details of the novel video watermark scheme and the experimental results are shown in Section 3. Section 4 provides a conclusion and the further improvement of this scheme.

2 A Video Watermarking Scheme

The new watermarking scheme we propose is based on Discrete Wavelet Transform. Fig. 1 shows an overview of our watermarking process. In our scheme, an input video is split into audio and video stream and undergoes watermarking respectively. On the other hand, a watermark is decomposed into different parts which are embedded in corresponding frames of different scenes in the original video.

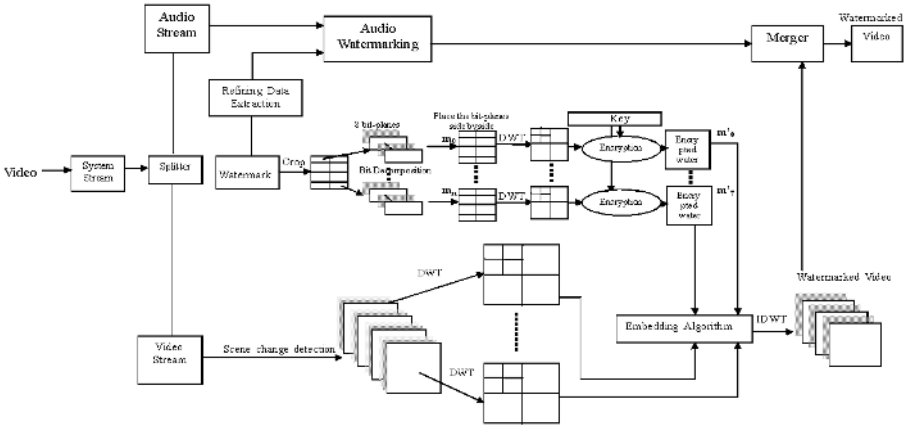


Fig. 1. Overview of the watermarking process

As applying a fixed image watermark to each frame in the video leads to the problems in maintaining statistical and perceptual invisibility [7], our scheme employs independent watermarks for successive but different scenes. Applying independent watermarks to each frame also presents a problem: Regions in each video frame with little or no motion remain the same frame after frame. These motionless

regions may be statistically compared or averaged to remove independent watermarks [8,9], so we use an identical watermark within each motionless scene. With these mechanisms, the proposed method is robust against the attack of frame dropping, averaging, swapping, and statistical analysis. At the same time, error correcting codes are extracted from the watermark and embedded as an audio watermark in the audio channel, which in turn makes it possible to correct and detect the changes from the extracted watermarks. This addition protection mechanism enables the scheme to overcome the corruption of a watermark, thus the robustness of the scheme is increased under certain attacks.

This newly proposed scheme consists of four parts, including: watermark preprocess, video preprocess, watermark embedding, and watermark detection. Details are described in the following sections.

2.1 Watermark Preprocess

Watermark preprocess consists of two parts, video watermark and audio watermark. After both watermarks are preprocessed, they will be embedded into video channel and audio channel, respectively.

Video Watermark. A Watermark is scrambled into small parts in preprocess, and they are embedded into different scenes so that the scheme can resist to a number of attacks specified to the video. A 256-grey-level image is used as a watermark, as shown in Fig. 3a, so 8 bits can represent each pixel. The watermark is first scaled to a particular size with the following equation

$$p + q = n \qquad , p \text{ and } q > 0 \tag{1}$$

where m is the number of scene changes and n, p, q are positive integers. And the size of the watermark should be

$$64 \cdot 2^{p} \times 64 \cdot 2^{q} \tag{2}$$

Then the watermark is divided into 2^n small images with size 64 × 64. Fig. 2 and 3 show the procedure and the result of watermark preprocess with m = 10, n = 3, p = 1, and q = 2.

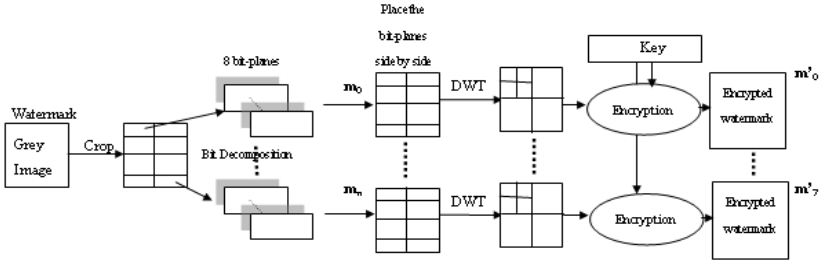


Fig. 2. Overview of watermark preprocess.

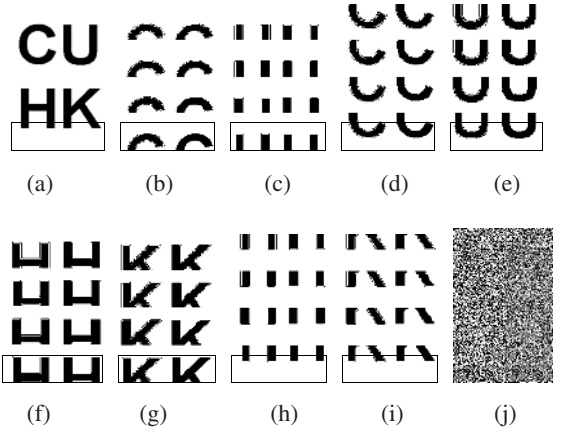


Fig. 3. (a) Original watermark (b-i) Preprocessed watermark m_0-m_7 (j) Encrypted watermark m'_0

In the next step, each small image is decomposed into 8 bit-planes, and a large image m_n can be obtained by placing the bit-planes side by side only consisting of 0's and 1's. These processed images are used as watermarks, and totally 2^n independent watermarks are obtained. To make the scheme more robust, the processed watermarks m are transformed to the wavelet domain and encrypted [10]. Sample preprocessed watermarks are shown in Fig. 3, where (a) is the original watermark, (b)-(i) represent the scrambled watermarks in the spatial domain, and (j) shows the encrypted watermark of (b), i.e., m'_0.

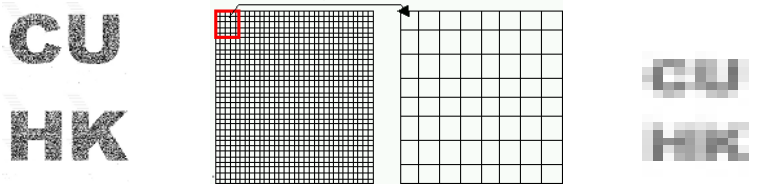
Audio Watermark. Error correcting code is extracted from the watermark image and embedded in the audio channel as an audio watermark. This watermark provides the error correcting and detection capability for the video watermark. In detection phase, it would be extracted and used for refining the video watermark. Different error correcting coding techniques can be applied such as Reed-Solomon Coding Techniques [11] and Turbo Coding [12].

Error correcting code plays an important role to a watermark, especially when the watermark is corrupted, i.e., when it is damaged significantly. Error correcting code overcomes the corruption of a watermark, and can make the watermark survive through serious attacks. Moreover, the scheme also takes advantages of watermarking the audio channel, because it provides an independent channel for embedding the error correcting code, which gives extra information for watermark extraction. Therefore, the scheme is more robust than other schemes which only used video channel alone.

The key to error correcting is redundancy. Indeed, the simplest error correcting code is simply repeated everything several times. However, in order to keep the audio watermark inaudible, we cannot embed too much information into an audio channel. In our scheme, we apply averaging to achieve the error code. Within a small region of an image, the pixels are similar. Therefore, an average value of a small region can be used to estimate the pixels within that particular region. The average value of the pixels in each region is calculated as follows:

$$Avg_k = \sum_{i=0}^{x} \sum_{j=0}^{y} W_{j*w+q*x+p*y*w+i} \tag{3}$$

where k is the k^{th} block of the average image, (p, q) is coordinate of region k, (x, y) is the coordinate of the pixel in region k and x × y is the size of a block. A sample is shown in Fig. 4.



(a) (b) (c)

Fig. 4. (a) Original video watermark (b) Visualization of averaging (c) Audio watermark (average of a)

2.2 Video Preprocess

Our watermark scheme is based on 4 levels DWT. All frames in the video are transformed to the wavelet domain. Moreover, scene changes are detected from the video by applying the histogram difference method on the video stream.

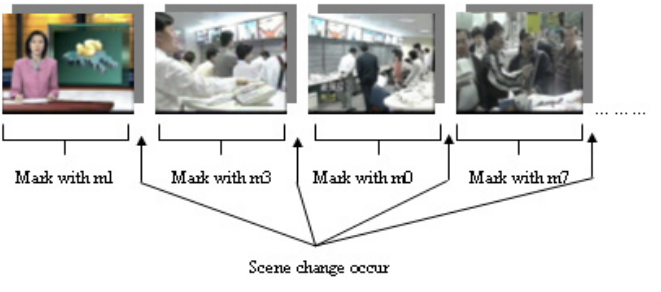


Fig. 5. After scene change detection, watermark m_1 is used for the first scene. When there is a scene change, another watermark m_3 is used for the next scene.

After scene change detection, as shown in Fig. 5, independent watermarks are embedded in video frames of different scenes. Within a motionless scene, an identical watermark is used for each frame. The watermark for each scene can be chosen with a pseudo-random permutation such that only a legitimate watermark detector can reassemble the original watermark.

2.3 Watermark Embedding

Watermark is then embedded to video frames by changing position of some DWT coefficient with the following condition:

if W[j] = 1,
Exchange C[i] with max(C[i], C[i+1], C[i+2], C[i+3], C[i+4])
else (4)
Exchange C[i] with min(C[i], C[i+1], C[i+2], C[i+3], C[i+4])

where **C[i]** is the i^{th} DWT coefficient of a frame, and **W[j]** is the j^{th} pixel of a certain watermark [13]. The sequence of watermark coefficients used is stated in Fig. 6.

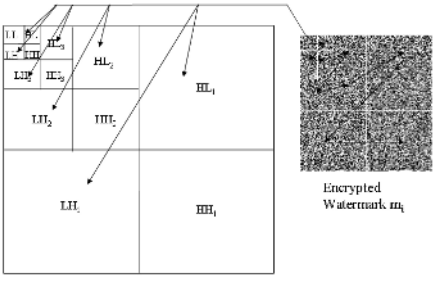


Fig. 6. Embedding watermarks in a frame. Higher frequency coefficients are embedded to higher frequency part of the video frame. Also, only the middle frequency wavelet coefficient of the frame (middle frequency sub-band) is watermarked [9].

The emphasis of this scheme is the video watermark. The audio watermark is used to help the video watermark and make it more robustness. Namely, the audio watermark is used for refining the video watermark in detection phase, so the error coding code is stored in the audio channel. We have applied a simple audio watermarking technique, the spread spectrum which is proposed in [16], in this scheme.

2.4 Watermark Detection

The watermark is detected through the following process, where overview is shown in Fig. 7.

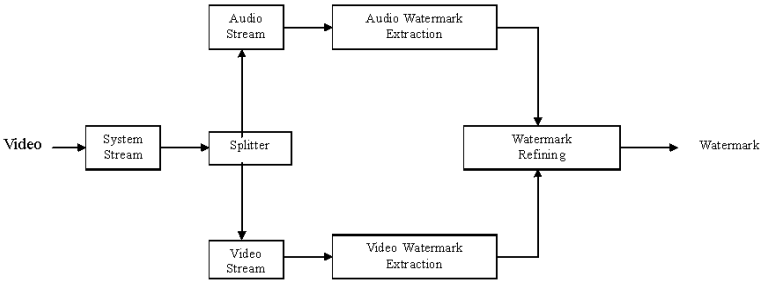


Fig. 7. Overview of detection of the watermark

A test video is split into video stream and audio stream and watermarks are extracted separately by audio watermark extraction and video watermark extraction. Then the extracted watermark undergoes refining process.

Video Watermark Detection. The video stream is processed to get the video watermark. In this step, scene changes are detected from the tested video. Also, each video frame is transformed to the wavelet domain with 4 levels. Then the watermark is extracted with the following condition:

```
if WC[i] > median(WC[i], WC[i+1], WC[i+2], WC[i+3], WC[i+4])
      W[j] = 1
else                                                          (5)
      W[j] = 0
```

where **WC[i]** is the i^{th} DWT coefficient of a watermarked video frame, and **W[j]** is the j^{th} pixel of an extracted watermark [13].

As an identical watermark is used for all frames within a scene, multiple copies of each part of the watermark may be obtained. The watermark is recovered by averaging the watermarks extracted from different frames. This reduces the effect if the attack is carried out at some designated frames. Then we can combine the 8 bit-planes and recover the 64×64 size image, i.e., $1/2^n$ part of the original watermark.

If enough scenes are found and all parts of the watermark are collected, the original large watermark image can be reconstructed. This can be shown in Fig. 8, where the original frame, the watermarked frame, and the extracted watermark are depicted. Moreover, if some of the watermark part is lost, the final watermark can still survive. We will show this later.

(a) (b) (c) (d)

Fig. 8. (a) Original frame (b) Watermarked frame (c) Extracted watermark corresponding to Fig. 3(g) (d) Recovered watermark

Audio Watermark Detection and Refining. At the same time, error correcting codes are extracted from the audio stream and the video watermark extracted is refined by this information with the following equation

$$\widehat{W}_{ij} = (\widehat{W}_{ij} * P + Avg_k * Q)/(P+Q) \tag{6}$$

where k is the k^{th} block of the average image, (i, j) is coordinate of the video watermark, and P: Q is a ratio of importance of extracted video watermark to audio watermark.

After extracting and refining the watermark, a similarity measurement of the extracted and the referenced watermarks is used for objective judgment of the extraction fidelity and it is defined as:

$$\text{Normalized correlation: NC} = \frac{\sum_i \sum_j W(i,j)\widehat{W}(i,j)}{\sum_i \sum_j [W(i,j)]^2} \tag{7}$$

which is the cross-correlation normalized by the reference watermark energy to give unity as the peak correlation [14]. We will use this measurement to evaluate our scheme in our experiment.

3 Experimental Results

To evaluate the performance of the new video watermarking scheme, several experiments have been done. They are: the experiment with various dropping ratio, the experiment with various number of frame colluded, the experiment with various quality factor of MPEG, and the experiment with various cropping ratio. Another DWT-based watermarking scheme which embeds an identical watermark in all frames is used to compare with the proposed scheme. A video clip with 1526 frames of size 352×288 is used in our experiment. The video consists of 10 scene changes. The NC values are retrieved when the watermarked video is under different attacks. The experimental results are described in details in the following.

3.1 Experiment with Frame Dropping

As a video contains large amount of redundancy 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. Different percentages of frames are dropped and obtained result is shown in Fig. 9.

Our scheme achieves better performance. It is because in each scene, all frames are embedded with the same watermark. This prevents attackers from removing the watermark by frame dropping. If they try to remove one part of the watermark, they need to remove the whole trunk of frames (i.e., the whole scene) and this would lead to a significant damage to the video. In addition, when frames are dropped, the error is only introduced to a corresponding small part of the watermark. For the DWT-based scheme (i.e., non-scene-based), however, the error is introduced to the whole watermark and it makes the performance worse.

The performance of the scheme is significantly improved by combining with a audio watermark, especially when the dropping rate of video frame is high. The improvement is increased with the dropping rate of the frame. This is because when the dropping rate increases, the error of the extracted watermark is increased and it significantly damages the watermark. The error correcting code from the audio watermark provides information to correct the error and overcome the part of the corruption of the video watermark, thus the NC values of the watermark is higher than the one without the error correcting code. Moreover, the error correcting code is

embedded in the audio channel. Frame dropping would not affect the audio channel much. Our scheme can take advantages of this to avoid destroying the information, and error correcting code can still be used to refine the watermark in improving the NC value.

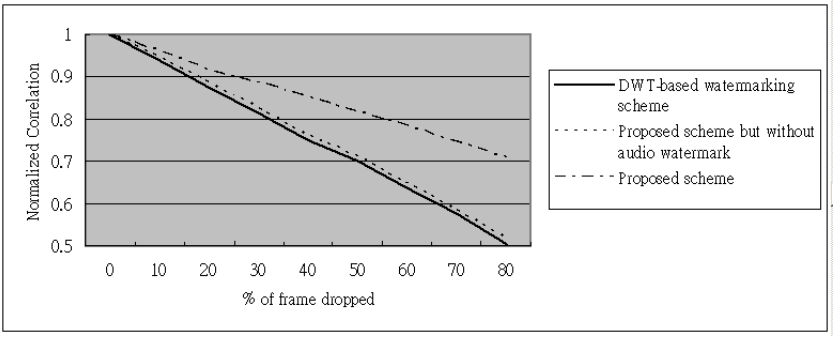


Fig. 9. NC values under frame dropping. From the experiment, we found that our scheme achieves better performance than the DWT-based scheme without scene-based watermarks.

3.2 Experiment with Frame Averaging and Statistical Analysis

Frame averaging and statistical analysis is another common attack 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 [17,18]. The scenario is shown in Fig. 10.

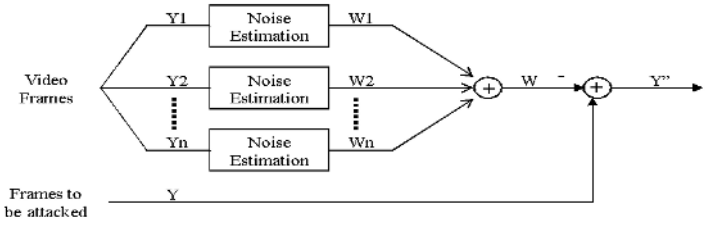


Fig. 10. Scenario of statistical averaging attack.

Our proposed scheme performs better because our scheme crops a watermark into pieces and embeds them into different frames, it making the watermarks resistant to attacks by frame averaging for the watermark extraction. 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 [19]. Independent watermarks used for successive, but different scenes can prevent attackers from colluding with frames from completely different scenes to extract the watermark.

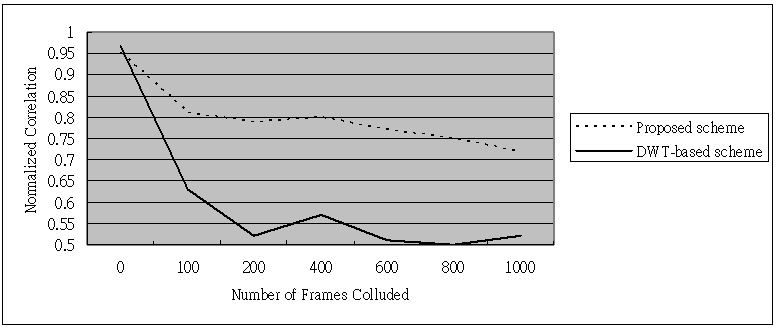


Fig. 11. NC values under statistical averaging. After this attack is applied to the watermarked video with different numbers of video frame colluded, watermarks are extracted and NC values are obtained. It is found that the proposed scheme can resist to statistical averaging quite well.

3.3 Experiment with Lossy Compression

This experiment is aimed at testing the robustness of the scheme under attack by lossy compression. Fig. 12 shows the NC values of the extracted watermarks with different quality factors of MPEG.

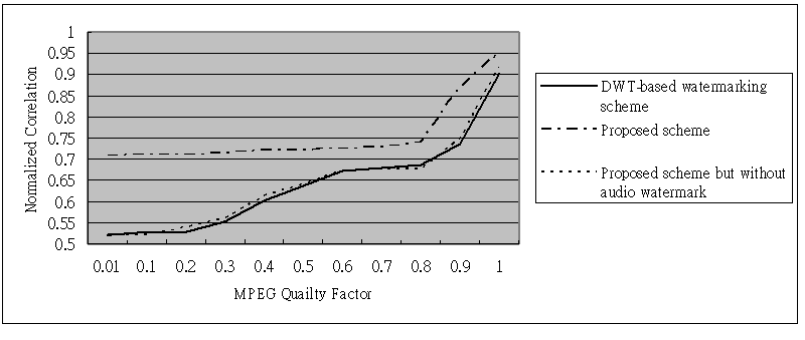


Fig. 12. NC values under lossy compression. From the experiment, we found that the proposed scheme improves the robustness for watermark protection.

The performance of the scheme is significantly improved by combining with audio watermark, especially when the quality factor of MPEG is low. This is because 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. The proposed scheme without audio watermark has similar performance with other DWT-based scheme because both of them satisfy the following condition. Higher frequency DWT coefficients of the watermark are embedded to higher frequency part of the video frame and high frequency sub-band DWT coefficients (HH) of video frame are not watermarked. This approach makes

the watermark survive MPEG lossy compression, as lossy compression removes the details of the image [20].

3.4 Experiment with Attacks on Watermarked Frame

DWT inherits many advantages in resisting the attacks on the watermarked frames. It achieves both spatial and frequency localization, perceptual invisibility and attacks by image processing techniques [15]. Cropping is one of the attacks applied to video frequently. Fig. 13 shows the result of the watermarked video under different ratio of cropping. It is also found that the proposed scheme gives the best result.

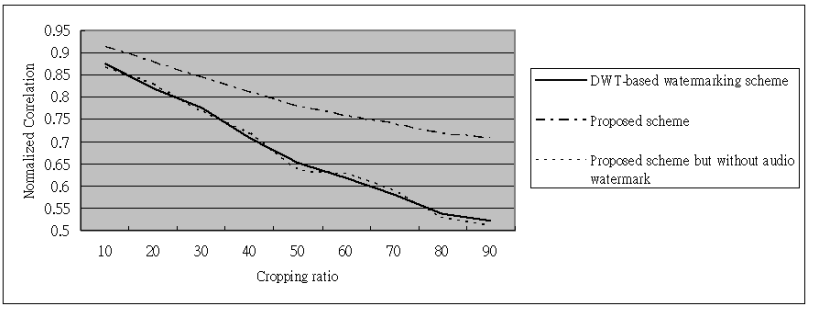


Fig. 13. NC values under cropping

4 Conclusion and Future Work

This paper proposes an innovative blind video watermarking scheme with scrambled watermarks and error correcting code. The process of this video watermarking scheme, including watermark preprocessing, video preprocessing, watermark embedding, and watermark detection, is described in detail. Experiments are performed to demonstrate that our scheme is robust against attacks by frame dropping, frame averaging, and statistical analysis. Robustness of the scheme is enhanced by combining with audio watermarks. The scheme can be improved by making use of the information from the video, such as time information, to increase the robustness of the watermark. We will conduct this improvement in the future.

References

1. A. Piva, F. Bartolini, and M. Barni: Managing copyright in open networks. *IEEE Internet Computing*, Volume 6, Issue: 3, pp: 18–26, May-June 2002
2. Chun-Shien Lu, Hong-Yuan, and Mark Liao: Multipurpose Watermarking for Image Authentication and Protection. *IEEE Transactions on Image Processing*, Volume: 10 Issue: 10, Oct 2001 Page(s): 1579–1592
3. C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. M. Liao: Cocktail watermarking for digital image protection. *IEEE Transactions Multimedia*, Volume 2, pp. 209–224, Dec. 2000.

4. Joo Lee and Sung-Hwan Jung: A survey of watermarking techniques applied to multimedia. *Proceedings 2001 IEEE International Symposium on Industrial Electronics (ISIE2001)*, Volume. 1, pp: 272–277, 2001.
5. M. Barni, F. Bartolini, R. Caldelli, A. De Rosa, and A. Piva: A Robust Watermarking Approach for Raw Video. *Proceedings 10th International Packet Video Workshop PV2000*, Cagliari, Italy, 1–2 May 2000.
6. M. Eskicioglu and J. Delp: An overview of multimedia content protection in consumer electronics devices. *Signal Processing Image Communication 16 (2001)*, pp: 681–699, 2001.
7. N. Checcacci, M. Barni, F. Bartolini, and S. Basagni: Robust video watermarking for wireless multimedia communications. *Proceedings 2000 IEEE Wireless Communications and Networking Conference (WCNC 2000)*, Volume 3, pp: 1530–1535.
8. Bijan G. Mobasseri: Direct sequence watermarking of digital video using m-frames. *Proceedings International Conference on Image Processing (ICIP-98)*, Chicago, Illinois, Volume 3, pp: 399–403, October 4–7 1998.
9. Mitchell D. Swanson, Bin Zhu, and Ahmed H. Tewfik*:* Multiresolution Video Watermarking using Perceptual Models and Scene Segmentation. *Proceedings International Conference on Image Processing (ICIP '97),* 3-Volume S*e*t-Volume *2*, Washington, DC October 26–29, 1997.
10. P. P. Dang and P. M. Chau: Image encryption for secure Internet multimedia applications. *IEEE Transactions on Consumer Electronics*, Volume: 46 Issue: 3, pp: 395–403, Aug. 2000.
11. Lijun Zhang, Zhigang Cao and Chunyan Gao: Application of RS-coded MPSK modulation scenarios to compressed image communication in mobile fading channel. *Proceedings 2000 52nd IEEE Vehicular Technology Conference, VTS-Fall VTC.2000*, Volume: 3, 2000 pp: 1198–1203.
12. A Ambroze, G. Wade, C. Serdean, M. Tomlinson, J. Stander, and M. Borda: Turbo code protection of video watermark channel. *IEE Proceedings-Vision, Image and Signal Processing*, Volume: 148, Issue: 1, Feb 2001 pp: 54–58.
13. F.Y. Duan, I. King, L. Xu, and L.W. Chan: Intra-block algorithm for digital watermarking. *Proceedings IEEE 14th International Conference on Pattern Recognition (ICPR'98)*, volume II, pp: 1589–1591, 17–20 August 1998.
14. Chiou-Tung Hzu and Ja-Ling Wu: Digital watermarking for video. *Proceedings 1997 13th International Conference on Digital Signal Processing, DSP 97*, Volume: 1, pp: 217–220, 2–4 Jul 1997.
15. Xiamu Niu and Shenghe Sun: A New Wavelet-Based Digital Watermarking for Video. *9th IEEE Digital Signal Processing Workshop*, Texas, USA, Oct. 2000.
16. D. Kirovski, and H. Malvar: Robust spread-spectrum audio watermarking. *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing, 2001*, Volume 3, pp: 1345–1348.
17. K. Su, D. Kundur and D. Hatzinakos: A Novel Approach to Collusion-Resistant Video Watermarking. *Security and Watermarking of Multimedia Contents IV, E. J. Delp and P. W. Wong, eds., Proc. SPIE*, Volume 4675, pp:12, San Jose, California, January 2002.
18. K. Su, D. Kundur and D. Hatzinakos: A Content-Dependent Spatially Localized Video Watermarked for Resistance to Collusion and Interpolation Attacks. *Proceedings IEEE International Conference on Image Processing*, October 2001.
19. Yiwei Wang, John F. Doherty, and Robert E. Van Dyck: A wavelet-based watermarking algorithm for ownership verification of digital image. *IEEE Transactions on Image Processing*, Volume 11, No 2, Feb 2002.
20. Eugene T. Lin, Christine I. Podilchuk, Ton Kalker, and Edward J. Delp: Streaming Video and Rate Scalable Compression: What Are the Challenges for Watermarking? *Proceedings SPIE International Conference on Security and Watermarking of Multimedia Contents III*, Volume 4314, January 22–25, 2001, San Jose, CA.