A DWT Domain Video Watermarking Algorithm Using Chaotic Mixing Technique

Rogelio Reyes, Clara Cruz, Mariko Nakano, Héctor Pérez

SEPI ESIME Culhuacan, National Polytechnic Institute of México
Av. Santa Ana 1000 Col. San Francisco Culhuacan, CP 04430, México, City. MÉXICO
rogreyes@gmail.com, mariko@calmecac.esimecu.ipn.mx

Abstract. Based on the imperceptibility and robustness requirement for video content protection, a watermarking algorithm for digital video with blind extraction is presented in this paper. In practice, the robustness depends on the watermark embedding energy used, which is limited by the media degradation caused by the watermark. Reliable embedding algorithms must assure watermark persistence up to an extreme quality downgrading. The proposed algorithm embeds binary visually recognizable pattern, such as owner's logotype, in DWT domain of some randomly selected video shots. To increase security, watermark data is disordered by chaotic mixing method before its embedding and to increase watermark imperceptibility, blue channel of RGB color space is used its embedding. The experimental results demonstrate the watermark imperceptibility and robustness against several video degradations and attacks. Also we show that extracted watermark data from watermarked video sequence in blind manner is sufficiently clear after several attacks.

Key words: Video watermarking, Copyright protection, Blind detection, Discrete Wavelet Transform

1 Introduction

With the fast development of multimedia application and communication systems, including digital broadcasting, the growth of the internet and especially popular internet software based on a peer-to-peer architecture has been used to share movies, music and other digital materials. Due to that duplication and modification of digital content are realized in very easy manner using digital editor tools provided for personal computer, illegal copying and distribution of digital data have been serious problems for intellectual property protection. Technical solutions for copyright protection of multimedia data are actively being pursued; two typical technologies are encryption and watermarking. Digital watermarking is the technique which embeds the copyright information into digital content, unlike encryption, watermarking does not restrict access to the data. A watermark is designed to permanently reside in the

© A. Argüelles, J. L. Oropeza, O. Camacho, O. Espinosa (Eds.)
Computer Engineering.
Research in Computing Science 30, 2007, pp. 37-46

host data [1].While encrypted data once is decrypted, intellectual property rights are no longer protected.

A watermarking scheme for digital video should include the capability to support following requirements: the embedded watermark in video data should be imperceptible and difficult to remove without degrading the perceptual quality of video, it means if embedded watermark is removed from video sequence, the video sequence has lost commercial value any more. In addition to above two requirements, watermarking technique used for digital video should extract the watermark information without using original video data (blind detection). The current issue of the watermarking becomes to get robustness to the signal distortion and tampering caused by intentional or unintentional attacks and common signal processing, including frame averaging, frame dropping, frame swapping, etc. [2],[3],[4].

There are three embedding positions for video watermark, i.e. base band video stream, at the same time when video is being compressed and in the compressed video stream. The watermark signal can be a random sequence with one information bit or multiple bit meaningful information, such as logotype. The random sequence watermark is more robust in general; however, embedding meaningful watermark is more important in some application. Therefore in this paper, we propose a video watermarking scheme that embeds a meaningful watermark in a base band video stream based on Discrete Wavelet Transform (DWT) and the blind extraction process extract watermark clearly from watermarked video.

The paper is organized as follows. In Section 2 and 3, the watermark embedding and extraction process of the proposed algorithm are described, respectively. Experimental results are presented in Section 4 and finally in Section 5, some conclusions are drawn.

2 Watermark Embedding

2.1 Watermark Preprocessing

A binary watermark image W (with values -1 or 1) is disordered based on chaotic mixing method [5], this procedure makes a mapping $A_N(k)$ with $L_N \rightarrow L_N$, where L_N is a two-dimensional indexes set, and it is computed iteratively by (1).

$$W^d = W^{(i)} = A_N^i(k)W^{(0)}, \quad i=1,2,\ldots,P-1,$$

$$A_N(k) = L_N \rightarrow L_N, \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\bmod N). \tag{1}$$

where $W^{(i)}$ is an *i-th* disordered watermark image, $W^{(0)}$ is a original watermark image, $(x_n, y_n) \in L_N$, $k \in [1, N] \subset Z$, P is a recurrent time depended on k, and N is the size of $W^{(0)}$. Two keys are required to reconstruct the watermark image: k is a first key and the iterations number i is a second one. An example of watermark image disorder is given by figure 1.

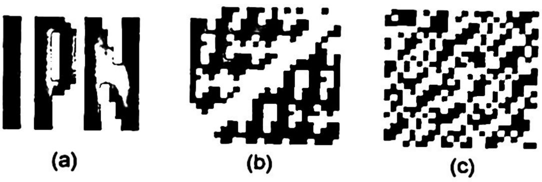


Fig. 1. (a) Original watermark, (b) Watermark processed with Chaotic Mixing using a key $k=5$ and iteration $i=5$ and (c) Watermark preprocessed with Chaotic Mixing using a key $k=5$ and iteration $i=10$.

2.2 Video Watermark Embedding Algorithm

First the host video is segmented into video sequences, and then some of them are selected randomly for watermark embedding. For each selected sequence watermark is embedded. The watermark embedding scheme is shown by figure 2.

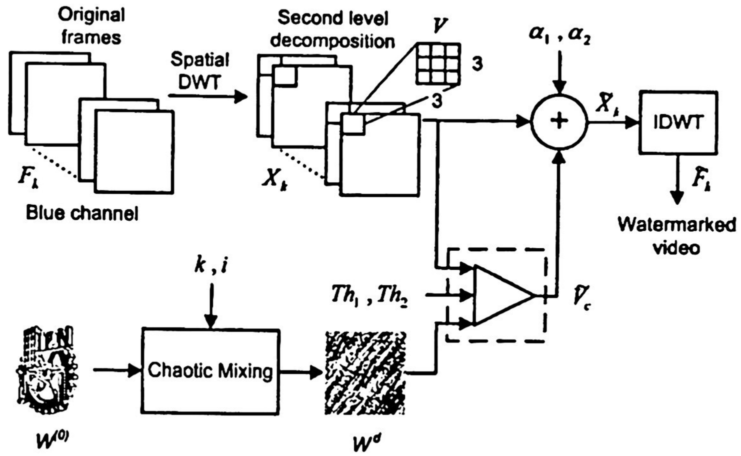


Fig. 2. Flowchart of video watermark embedding scheme.

The following steps are repeated for each frame of the selected video sequence and the process into the broken line frame in the figure 2 is described as follows.

A) Perform a two dimensional DWT based on the Daubechies-wavelet on each frame of the blue color channel, which is denoted by $F_k\ (k=1,2,\ldots,n)$. The multilevel decomposition is processed until the second level. Then the watermark is embedded into the LL_2 subband. Here wavelet coefficient frames of F_k are denoted by $X_k\ (k=1,2,\ldots,n)$.

B) Watermark embedding is based on magnitudes of the wavelet coefficients; disordered watermark image is adaptively spread spectrum and embedded into these coefficients. Wavelet coefficients X_k are divided into blocks with size 3x3 pixels, then a mean of the block V is computed and denoted as M. Watermark bit is embedded by changing the center coefficient value V_c of each block V with the corresponding modified value $\tilde{V}_c$, using the following rules shown below.

i. Assign values to two thresholds Th_1, Th_2, and also to two intensity factors α_1 and α_2.

ii. Calculate difference δ_1 between V_c and M.

$$\delta_1 = |V_c - M| \tag{2}$$

iii. Depending on δ_1 value with respect to Th_1, Th_2 and the corresponding bit of the pixel $W^d(i,j)$, V_c is modified:

1) If $\delta_1 > Th_1$, then watermark is not inserted.
2) If $\delta_1 < Th_1$, then watermark is inserted according to the following cases:

a) If $V_c > M$, $W^d(i,j)=1$ and $\delta_1 < Th_2$, then the center coefficient value V_c of the block is modified using (3).

$$\tilde{V}_c = V_c + \frac{9}{8}(Th_2 - \delta_1) + \alpha_1 \tag{3}$$

b) If $V_c > M$, $W^d(i,j)=-1$ and $\delta_1 > Th_2$, then the center coefficient value V_c of the block is modified using (4).

$$\tilde{V}_c = V_c - \frac{9}{8}(\delta_1 - Th_2) - \alpha_2 \tag{4}$$

c) If $V_c < M$, $W^d(i,j)=1$ and $\delta_1 < Th_2$, then the center coefficient value V_c of the block is modified using (5).

$$\tilde{V}_c = V_c - \frac{9}{8}(Th_2 - \delta_1) - \alpha_1 \tag{5}$$

d) If $V_c < M$, $W^d(i,j) = -1$ and $\delta_1 > Th_2$, the center coefficient value V_c of the block is modified using (6).

$$\tilde{V}_c = V_c + \frac{9}{8}(\delta_1 - Th_2) + \alpha_2 \tag{6}$$

C) The watermarked video is obtained computing the inverse DWT of the modified wavelet coefficient frames in the blue color channel $\tilde{X}_k$ and recombining the color channels.

Watermark image is embedded into a video by adaptive spread spectrum based on the characteristics of video data, in which the watermark was preprocessed with Chaotic Mixing method; so each pixel of the disordered watermark is embedded into a 3x3 block of magnitudes of the wavelet coefficients for the corresponding frame in the blue color channel. As mentioned above each watermark data is related to the static and dynamic composition in the video sequence offering better robustness to malicious attacks.

3 Blind Watermark Extraction

To extract the watermark, the original unmarked video and original watermark data are not required. A watermark can be extracted easily according to scheme shown in figure 3.

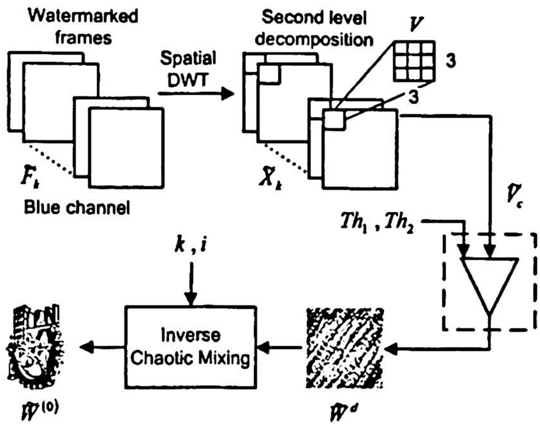


Fig. 3. Flowchart of video watermark blind detection.

The following steps are repeated for each frame of the selected sequence and the detail process into the broken line frame in the figure 3 is describe as follows.

A) Again, the process starts with the two dimensional wavelet decomposition of the blue color channel frames $\tilde{F}_k \ (k = 1,2,\ldots,n)$ of each video sequence selected in embedding scheme. Applying DWT to $\tilde{F}_k$, we can retrieve the LL_2 coefficients, these are denoted by $\tilde{X}_k \ (k = 1,2,\ldots,n)$.

B) Wavelet coefficients $\tilde{X}_k$ are divided in blocks with size 3x3 pixels, and then a mean of the block $\tilde{V}$ is computed and denoted $\tilde{M}$, extract the center coefficient value $\tilde{V}_c$ of each block $\tilde{V}$, and to obtain the corresponding value of the pixel $\tilde{W}_k^d(i,j)$ in these block $\tilde{V}$ following the rules shown below.

   i. Thresholds values Th_1 and Th_2 are known.

   ii. Calculate difference $\tilde{\delta}_1$ between $\tilde{V}_c$ and $\tilde{M}$.

$$\tilde{\delta}_1 = \left|\tilde{V}_c - \tilde{M}\right| \tag{7}$$

   iii. Depending of $\tilde{\delta}_1$ value with respect to Th_1 and Th_2 the corresponding value of the pixel $\tilde{W}_k^d(i,j)$, is obtained according with:

      1) $\tilde{\delta}_1 > Th_1$, then $\tilde{W}_k^d(i,j) = 0$.

      2) $\tilde{\delta}_1 < Th_1$ then a watermark bit is extracted according to the following cases:

         a) $\tilde{\delta}_1 \geq Th_2$, therefore $\tilde{W}_k^d(i,j) = 1$.

         b) $\tilde{\delta}_1 < Th_2$, therefore $\tilde{W}_k^d(i,j) = -1$.

C) Calculate a mean of the disordered watermark embedded in each frame of the selected sequences using (8).

$$\hat{W}^d(i,j) = \frac{1}{k}\sum_{k=1}^{K}\tilde{W}_k^d(i,j) \tag{8}$$

Where K is the total number of frames used in the embedding process, $\tilde{W}_k^d(i,j)$ is the watermark bit in the *k-th* frame of video.

D) Disordered watermark image $\tilde{W}^d$ can be formed using (9).

$$\tilde{W}^d(i,j) = \begin{cases} 1 & \hat{W}^d(i,j) > 0 \\ -1 & \hat{W}^d(i,j) < 0 \end{cases} \tag{9}$$

E) The reconstructed watermark image $\tilde{W}^{(0)}$ starting from $\tilde{W}^{d}$, can be obtained through the two keys used in the watermarking preprocessing section k and i, by calculating the inverse matrix of $A_N(k)$ iteratively until the number of iterations i using (10) where $\tilde{W}^{(i)} = \tilde{W}^{d}$.

$$\tilde{W}^{(0)} = A_N^{-i}(k)\tilde{W}^{(i)} = A_N^{P-i}(k)\tilde{W}^{(i)} \tag{10}$$

4 Experimental Results

The proposed algorithm has been evaluated using well-known video sequences "Foreman", "carphone" and "bus". These sequences are in the YUV color space in terms of one luma and two chrominance components, and their size are 288*352 (CIF format) [6]. The watermark is a binary image with size 24*24.

In the experiments we use 60 frames in these sequences to embed a watermark image and used the following values to the thresholds and intensity factors: $Th_1 = 70$, $Th_2 = \frac{1}{2}Th_1$, $\alpha_1 = \frac{9}{16}(Th_1 - Th_2)$ and $\alpha_2 = \frac{Th_2}{4}$.

We have conducted some experiments to evaluate the robustness of our proposed watermarking algorithm. For this purpose, we have performed some of the classical sequence manipulations including: noise attack, frame dropping, frame averaging, frame swapping. In the experiments, we have tested 10 times each video sequence with different frames (scenes), in which the results are average values of independent experiments.

Figure 4 demonstrates the invisibility of the embedded binary watermark image in the proposed algorithm. Similar results can be obtained with other video sequences.

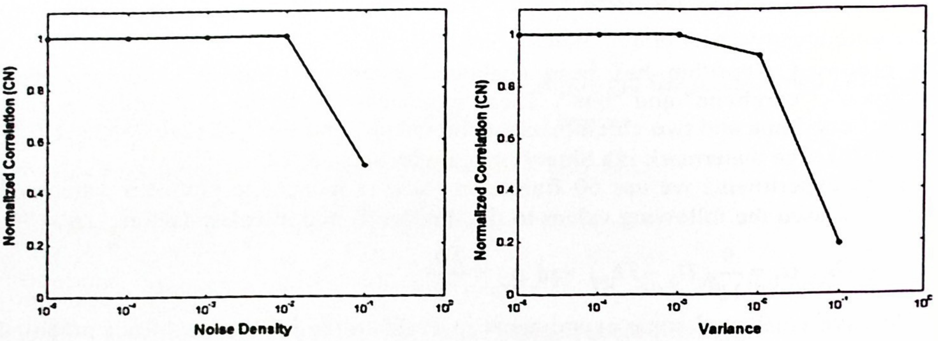
4.1 Noise Contamination

The watermarked video is corrupted by adding impulsive noise and gaussian noise with different intensity. The performance of video watermark approach is calculated in terms of normalized correlation between original watermark and reconstructed watermark defined as (11). Simulation results are shown in figure 5.

$$C\left(\tilde{W}^{(0)}, W^{(0)}\right) = \sum_i \sum_j \left(\tilde{W}^{(0)}(i,j) \cdot W^{(0)}(i,j)\right) \Big/ \sum_i \sum_j W^{(0)}(i,j)^2 \tag{11}$$

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

Fig. 4. Demonstration of invisibility. (a) The original "Foreman" frame, (b) Watermarked "Foreman" frame, (c) The original "bus" frame and (d) Watermarked "bus" frame.



(a) (b)

Fig. 5. Robustness to noise contamination, (a) robustness to impulsive noise with different noise densities, (b) robustness to Gaussian noise with different variances.

The results shown in figure 5 demonstrate the robustness of our video watermarking procedure against several noise contamination when up to 7% of the watermarked frame has been modified with impulsive or Gaussian noise, also video's commercial value will be lost if its contaminated more than or closer to 10% due to lower quality.

4.2 Frame Dropping , Frame Averaging and Frame Swapping Attacks

Based on the existence of temporal redundancy in video data, frame dropping or frame cutting, which removed some frames from the video sequence, this is an effective video watermark attack since it doesn't damage the video signal. Frame Dropping attack is given by (12).

$$V_{attacked} = V_{original} - \{F_{r1}, F_{r2}, \ldots . . F_{rn}\} \tag{12}$$

where $V_{attacked}, V_{original}$ are attacked and original video signals, and $F_{r1,} F_{r2}, \ldots .$ are some video frames.

Frame averaging attack compute the average of the two nearest neighbors' frames to replace the actual frame is calculated as (13).

$$F_k'(i,j) = \frac{1}{3}\left[F_{k-1}(i,j) + F_k(i,j) + F_{k+1}(i,j)\right] \tag{13}$$

Frame swapping attack can destroy some dynamic composition of the video signal and embedded watermark. This attack is formulated as (14), simulation results of the attacks are presented in figure 6.

$$F_k(i,j) \Leftrightarrow F_{k+1}(i,j), \quad k = 1,3,5,\ldots n-1 \tag{14}$$

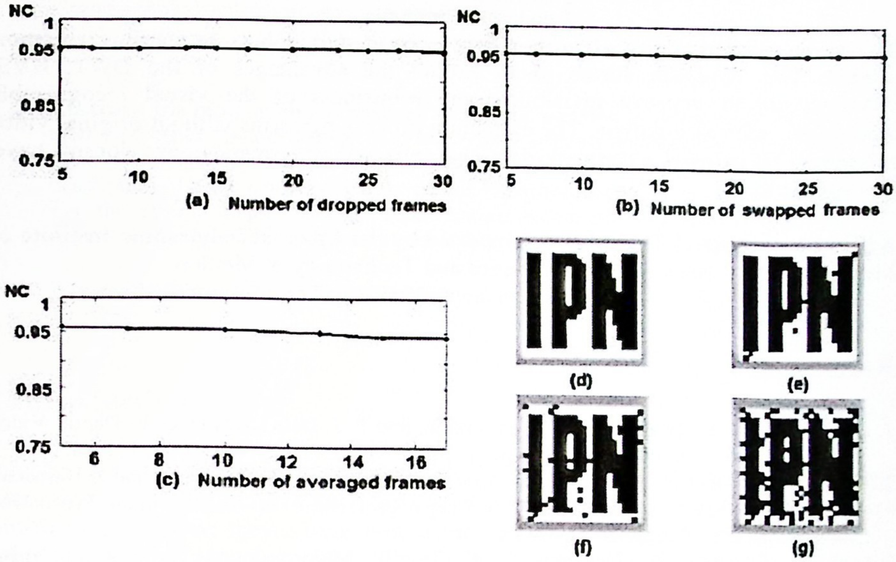


Fig. 6. Robustness to (a) frame dropping, (b) frame swapping, (c) frame averaging and extracted watermark with different normalized correlation respect to the original one: (d) original watermark, (e) extracted watermark with NC=0.9792, (f) extracted watermark with NC=0.9021, (g) extracted watermark with NC=0.7326.

Figure 6 demonstrates that our watermarking method is able to resist Frame Attacks, in all of these cases, the embedded watermark can be recovered with a little or no damage even when up to 50% of the watermarked frames has been modified.

In all analyzed attacks, normalized correlation values between original watermark and extracted one is higher than 0.95, which indicates that the extracted watermark image is very clear after watermarked video sequence is attacked.

We compare the proposed algorithm with different schemes [4], [7] and [8]. The results are shown in Table 1 'O' means that the embedded watermark is robust against attack and 'X' means that embedded watermark can not be recovered correctly.

Table 1. Performance comparison of the proposed scheme.

	Frame Attack			Noise Contamination	
	Averaging	Dropping	Swapping	Impulsive	Gaussian
Our scheme	O	O	O	O	O
Zhuang [4]	O	O	O	O	X
Zhao [7]	O	O	O	X	X
Zhang [8]	X	O	O	O	O

5 Conclusions

The video watermarking algorithm here presented is robust to various common attacks. This approach allows us to exploit the advantages of the DWT, HVS characteristic to improve invisibility and robustness of the visual recognizable watermark, such as logotype. The extraction process performs without original video sequence and original watermark data and extracted watermark image doesn't have any ambiguity.

Acknowledgments. This work is supported by the National Polytechnic Institute of México and National Council for Science and Technology of Mexico.

References

1. E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp.: Advances in Digital Video Content Protection. In: Proceedings of the IEEE, Vol. 93. No. 1, Jan. 2005. 171-183.
2. M. Maes, T. Kalker, J.-P. M. G. Linnartz, J. Talstra, G. F. G. Depovere, and J. Haitsma,: Digital watermarking for DVD video copy protection. In: IEEE Signal Processing Magazine, Vol. 17. Sep. 2000. 47–57.
3. M. D. Swanson, B. Zhu, and A. H. Tewfik. Multiresolution Scene-Based Video Watermarking Using Perceptual Models. In: IEEE Journal on Selected Areas in Communications. Vol. 16. May 1998. 540–550.
4. H. Zhuang, Y. Li and C. Wu.: A Blind Spatial-temporal Algorithm Based on 3D Wavelet for Video Watermarking. In: IEEE International Conference on Multimedia and Expo. (ICME) , vol. 3, 2004. 1727-1730.
5. G. Voyatzis and I. Pitas.: Embedding Robust Watermarks by Chaotic Mixing. In: Proceedings of Conf. Int. Digital Signal Processing, Vol. 1. 1997. 213-216.
6. K. N. Plataniotis and A. N. Venetsanopoulos.: Color Image Processing and Applications. Springer-Verlag Berlin. 2000. 20-39.
7. Z. Zhao, N. Yu and X. Li: A Novel Video Watermarking Scheme in Compressed Domain Based of Fast Motion Estimation. In: IEEE Int. Conf. on Communication Technology (ICCT). 2003. 1878-1882.
8. J. Zhang, J. Li, and L. Zhang.: Video Watermark Technique in Motion Vector. In: XIV Brazilian Symposium on Computer Graphics and Image Processing. 2001.