Digital watermark algorithm based on Key-frames Detection

Assistant Lecturer
Nadia Moqbel Hasan
E-mail: nadiamoh_2007@yahoo.com

Abstract

In this paper a new digital video watermarking scheme based on detection of video key-frames using histogram color techniques. The watermark is embedded in the DWT of the blue band of all key-frames using LSB algorithm, (as blue color is less sensitive to human visual). Stream cipher is included in the proposed scheme for encryption of the watermark for better security. The watermark is recovered by averaging the watermark from all the key-frames. Results show that the proposed method is robust against different type of attacks like lossy compression, frames dropping, frames swapping, sharpening, lightening, darken, noising, and distortion.

Keywords: discrete wavelet transform (DWT), least significant bit (LSB), key-frame, and histogram color techniques.

خوارزمية العلامة المائية الرقمية المعتمدة على كشف الاطر الرئيسة

الخلاصة:

في هذا البحث تم اقتراح طريقة جديد لادخال علامة مائية في فلم فديوي، تتلخص هذه الطريقة بايجاد الاطر الرئيسية (key-frames) *داخل الفلم الفديوي باستخدام تقنية المنحني التكراري للالوان ثم ادخال العلامة المائية في جميع هذه الاطر بعد عمل تحويلة (DWT) للحزمة الزرقاء التي تتميز بانها الاقل حساسية للعين البشرية، ولزيادة امنية الخوارزمية تم تشفير العلامة المائية باستخدام مولد للارقام العشوائية . ان العلامة المائية المستعادة هي معدل جميع العلامات في الاطر الرئيسية. اظهرت النتائج لهذه الخوارزمية بانها ذات كفاءة عالية ضد ضغط الفلم الفديوي، حذف بعض الاطر، تبديل الاطر، زيادة الحدة، التغميق، التفتيح، والضوضاء.*

I. Introduction

As digital video-based application technologies grow, such as Internet video, wireless video, and video conferencing, the problem of unauthorized copying and distribution of digital video rises more and more, thus creating copyright dilemma for the multimedia industry in general, and to the audio-video industry in particular. Many researches and technologies were proposed to provide methods to solve the problem of illegal copying and manipulations of digital video. An attractive method that has been proposed a decade ago to implement copyright information in multimedia documents is digital watermarking [1,2,3].

Effective watermarking has many requirements, the most important of which are imperceptibility and robustness. Imperceptibility refers to perceptual transparency and it requires that the watermarking algorithm to embed the watermark in such a way that the quality of the underlying video frames is not affected. As for the robustness requirement, the watermark must always remain in the watermarked video frames, even if the quality of the frames is degraded intentionally or unintentionally [4,5,6].

II. Literature Survey:

Video watermarking approaches can be classified into two main categories based on the method of hiding watermark information bits in the host video. The two categories are: Spatial domain watermarking, and transform-domain watermarking. In spatial-domain watermarking techniques, embedding and detection are performed on spatial pixels values (luminance, chrominance, and color space) or on the overall video frame. Spatial-domain techniques are easy to implement, however they are not robust against common digital signal processing operations such as video compression. [7,8]

Transform-domain techniques, on the other hand, alter spatial pixel values of the host video according to a pre-determined transform. Commonly used transforms are the Discrete Cosine Transform (DCT), the Fast Fourier Transform (FFT), the Discrete Wavelet Transform (DWT), and the Singular Value Decomposition (SVD). Transform-domain watermarking techniques proved to be more robust and imperceptible compared to spatial domain techniques since disperse the watermark in the special domain of video frame, making it very difficult to remove the embedded watermark [9,10,11].

Many watermarking methods have been proposed in the literature. Schyndel, Tirkel, and Osborne [12] generated a watermark using a m-sequence generator. The watermark was either embedded or added to the least significant bit of the original image to produce the watermarked image. The watermark was extracted from a suspected image by taking the least significant bits at the proper locations. Detection was performed by a cross-correlation of the original and extracted watermark. Schyndel *et al*. showed that the resulting image contained an invisible watermark with simple extraction procedures. The watermark, however, was not robust to additive noise.

Cox et al. [13] noted that in order for a watermark to be robust to attack, it must be placed in perceptually significant areas of the image. The watermark was based on 1000 random samples of a N(0,1) distribution. These samples were added to the 1000 largest DCT coefficients of the original image, and the inverse DCT was taken to retrieve the watermarked image. For detection, the watermark was extracted from the DCT of a suspected image. Extraction was based on knowledge of the original signal and the exact frequency locations of the watermark. The correlation coefficient was computed and set to a threshold. If the correlation was large enough, the watermark was detected. Their method was robust to image scaling, JPEG coding, dithering, cropping, and rescanning.

Xia, Boncelet, and Arce [14] proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT). The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire, extracted watermark was correlated with the entire, original watermark. This technique proved to be more robust than the DCT method [13] when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images.

Improvements on the above schemes were possible by utilizing properties of the Human Visual System. Bartolini et al. [15] first generated a watermarked image from DCT coefficients. Then spatial masking was performed on the new image to hide the watermark. Kundur and Hatzinakos [16] embedded the watermark in the wavelet domain. The strength of the watermark was determined by the contrast sensitivity of the original image. Both techniques showed resistance to common signal processing operations.

Delaigle et al. [17] proposed a unique watermarking scheme based on the Human Visual System. Binary m-sequences were generated and then modulated on a random carrier. This image served as the watermark, and then it was masked based upon the contrast between the original signal and the modulated image. The masked watermark was added to the original image to form the watermarked image. Their technique was robust to additive noise, JPEG coding, and rescanning.

Craver et al [18] noted that certain watermarking techniques were susceptible to counterfeit attacks. They showed that the method proposed by Cox et al. can be attacked by creating a fake original image and fake watermark that is indistinguishable from the true original image and watermark. To prevent this scenario, they modified the Cox et al. algorithm by making the watermark dependent on the original image. This new scheme was less susceptible to counterfeiting and still maintained robustness.

Bas, Chassery, and Davoine [19] introduced a watermarking system using fractal codes. A collage map was composed from 8x8 blocks of the original image and from the image's DCT. The watermark was added to the collage map to produce a marked image. Results showed that fractal coding in the DCT domain performed better than coding in the spatial domain. The DCT-based watermarking technique was robust to JPEG compression, while spatial fractal coding produced block artifacts after compression.

III. Key-frame detection

There are many algorithms to Key-frames detection (scene detection) into pixel domain included pixel differences [5], statistical differences [5], histogram comparison [6], edge detection [6], motion vectors etc. The color histogram of an image can be computed by dividing a color space into discrete image colors called bins and counting the number of pixels that fall into each bin. The algorithm that is used in our works, called consecutive histogram compare two frames based on their color histograms. A key-frame is detected if the distance between two consecutive frames is greater than a pre-defined threshold Θ and the equation is given below:[3]

$$d\,(fi,\ fj)\quad \frac{\sum_{k=0}^{k=n} (\,H(f_i,k) - H(f_j,k)\,)^2}{\max\,(\,H(f_i,k)\ ,\ H(f_j,k)} \;>\Theta \quad \ldots \quad (1)$$

Where $H(f_i,k)$ and $H(f_j,k)$ denote the histograms of kth color of the histograms of kth color of the frames f_i and f_j respectively and N is the total number of bins.

IV. The watermark embedding process:

Step 1: Using key-frame detection algorithm EQ. (1) to detect the key-frames (N) in the input video (Avi format) as shown in figure (1).

Step 2: Each key-frame (blue band) is transformed using DWT (discrete Wavelet Transform).

Step 3: The watermark is cipher using pseudo random key generation and xor function. The seed number of pseudo random key generation is given to a certified authority, and is used in case of dispute later.

Step4: Embedded the ciphered watermark in each transformed key-frame (blue band) using least significant bit algorithm. (as blue color is less sensitive to human visual, modifying blue colors of pixels as watermarking embedding is common approach)

Step5: Implement the Inverse of (DWT). The block diagram for watermarking embedding process is shown in figure (2)

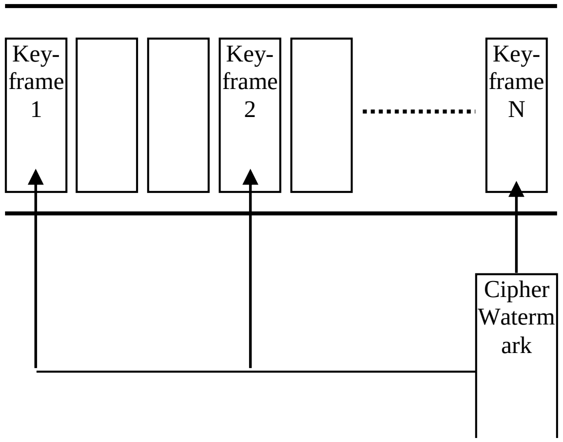

Figure (1) Detection of key-frames using equation (1)

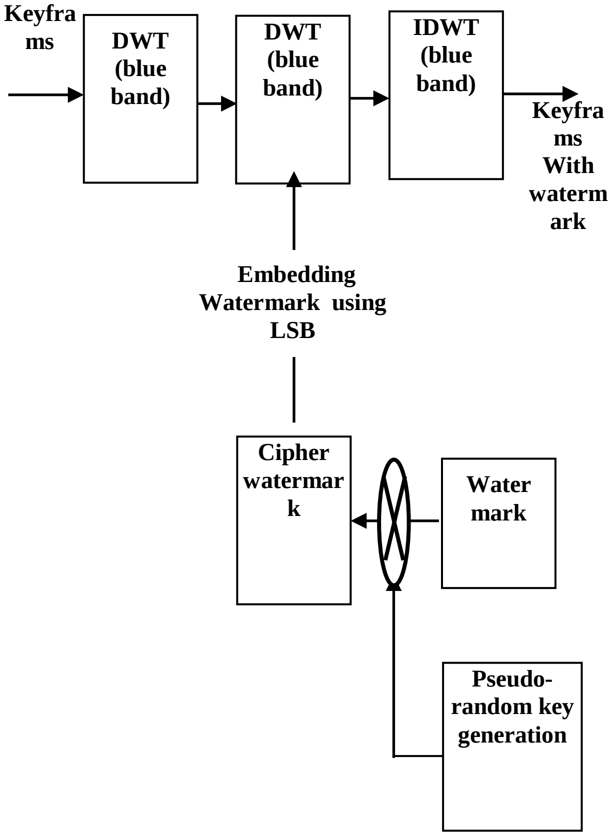

Figure (2) Block diagram of the watermark embedding process.

V. The watermark recover process:

Step 1: Using Scene detection algorithm EQ. (1) to detect the key-frames (N) in the input video.

Step2: Each key-frame (blue band) is transformed using DWT (discrete Wavelet Transform).

Step3: Extract the cipher watermark in each transformed key-frame (using least significant bit algorithm.

Step4: Decipher the watermark using (seed number, random-key, xor function) from each key-frame.

Step5: find the average of the extract watermarks

The block diagram for watermarking recover process is shown in figure (3)

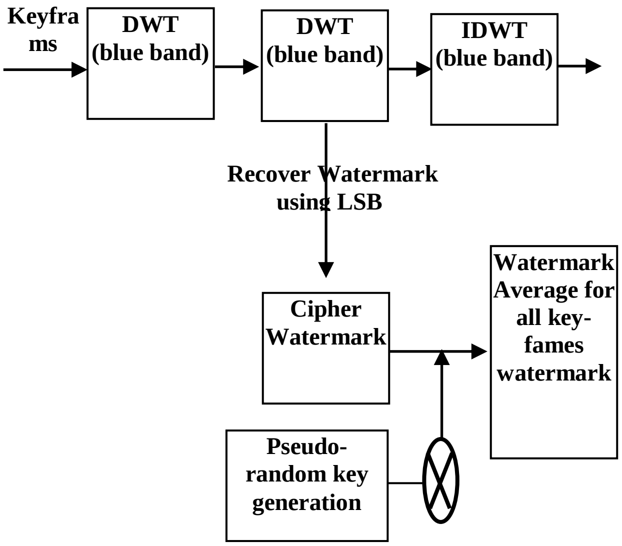
Keyframs
DWT (blue band)
DWT (blue band)
IDWT (blue band)
Recover Watermark using LSB
Cipher Watermark
Watermark Average for all key-fames watermark
Pseudo-random key generation

Figure (3) Block diagram of the watermark recover process.

VI. Video Quality Measurement

PSNR (Peak Signal-To-Noise Ratio) is a widely used method for measuring objective quality produced by image and video manipulating algorithms [11]. PSNR is expressed in terms of the logarithmic decibel scale. The typical values of the PSNR are between 30 and 50 dB, where higher means better quality. It is calculated using (2):

$$PSNR = 10 \cdot \log_{10}\left(\frac{255^{2}}{MSE}\right) \quad \ldots \quad (2)$$

Where *MSE* is the value of the Mean Square Error between the original and the modified frame. It is calculated using (3):

$$MSE = \frac{1}{MN}\sum_{i-1}^{M}\sum_{j-1}^{N}\left[x(i,j) - y(i,j)\right]^{2} \quad \ldots (3)$$

VI. Results

Simulation is performed to test the performance of algorithm. The video sequence which is used in our proposed system consisting of 160 frames and the size of frame is (240 x 320) pixels. The list of representative key-frames using (Ɵ = 15000) are shown in figure (4).

Figure (4) Tour in Iraqi National Museum (AVI format)
Detect of nine key-frames using equation 1 and (Ɵ = 15000)

The watermark was ciphered using random key generation (MATLAB language) and XOR function as shown in figure (5).

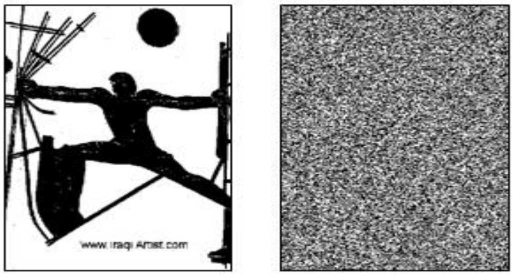

Figure (5) freedom statue Baghdad
Watermark ciphering using stream cipher (seed number, random key, xor function)

The proposed algorithm was tested for its robustness against frame dropping, frame swapping and interpolation, Jpeg compression, lightening, darkening, and noising, blurring, sharpening, cropping and resizing figure (6) shows the recovered watermark after some type of attacks.

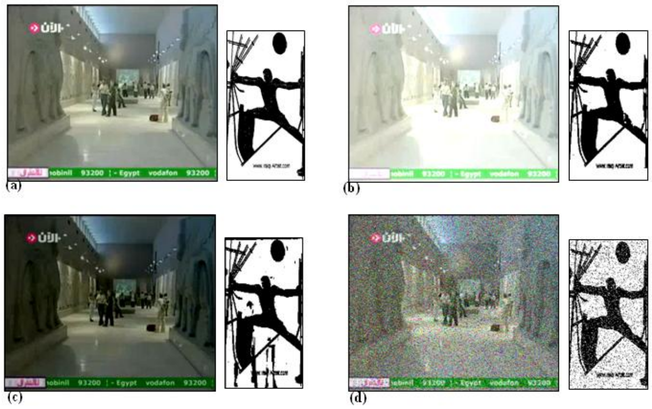

Figure (6) some type of attacks
a) Original watermark and key-frame
b) Lightened frame and retrieved watermark.
c) Darken frame and retrieved watermark
d) Noise frame and retrieved watermark.

Peak-signal-to-noise-ratio (PSNR) and Normalize correlation are used to evaluate the similarity of the original watermarked frame and the attacked watermarked frames table (1) shows the results.

	Type of Attaccks						
	compression	lightening	darkening	noising	blurring	sharpening	cropping
NC%	30.52	15.7	17.7	35.67	25.57	36.78	15.4
PSNR	55.78	90.65	89.76	66.13	67.63	87.56	94.67

VII. Conclusion

In this paper video watermarking algorithm is presented. Watermark embedded is made in the wavelet transform of the key-frames of the video using LSB. The watermark is recovered by averaging the watermark from all the key-frames. Results show that the proposed method is robust against different type of attacks like lossy compression, frames dropping, frames swapping, sharpening, lightening, darken, noising, and distortion.

Reference

[1] Langelaar, G., I. Setyawan, and R. Lagendijk, 2000. “Watermarking Digital Image and Video Data: A State-of-Art Overview”, IEEE Signal Processing Magazine 17, pp. 20-46.

[2] V. Potdar, S. Han, and E. Chang, 2005. "A Survey of Digital Image Watermarking Techniques", in Proceedings of the 2005 IEEE International Conference on Industrial Informatics, pp. 709-716.

[3] M. Ramkumar and A. Akansu, 2004. "A Robust Protocol for Proving Ownership of Multimedia Content”, IEEE Trans. Multimedia 6, pp. 496-478.

[4] Doerr, G., and J. Dugelay, 2003. “A Guided Tour to Video Watermarking”, Signal Processing: Image Communication 18, pp. 263-282.

[5] Hartung, H., and B. Girod, 1998. “Watermarking of Compressed and Un-Compressed Video”, Signal Processing 66, pp. 283-301.

[6] P. Chan and M. Lyu, 2003. "A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code", in Proceedings of the 5th International Conference on Information and Communications Security, Springer Berlin/Heidelberg 2836, pp. 202-213.

[7] D. Mukherjee, S. Maitra, and S. Acton, 2004. "Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication", IEEE Trans. Multimedia 6, pp. 1-15.

[8] R. Shah, A. Argawal, and S. Ganesan, 2005.
"Frequency Domain Real Time Digital
Watermarking", in Proc. of the IEEE 2005 Int.

Conf. on Elector Info. Tech, pp. 1-6.

[9] S. Mitra, 1998. “Digital Signal Processing”, McGraw–Hill, USA.

[10] M. Herandez, M. Miyatake, and H. Meana, 2005. "Analysis of a DFT-based watermarking algorithm", in Proc. of the IEEE 2nd Int. Conf. on Electrical and Electronics Eng., pp. 44-47.

[11] Mallat, S, 1989. “A theory for multi-resolution signal decomposition: The wavelet representation”, IEEE Trans. Pattern Anal. And Machine Intell. 11, pp. 674-693.

[12]. R. Schyndel, A. Tirkel, and C. Osborne, “A Digital Watermark,” Proc. IEEE Int. Conf. on Image Processing, Nov. 1994, vol. II, pp. 86-90.

[13]. I. Cox, J. Kilian, F. Leighton, and T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[14]. X. Xia, C. Boncelet, and G. Arce, “A Multiresolution Watermark for Digital Images,” Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551.

[15]. F. Bartolini, M. Barni, V. Cappellini, and A. Piva, “Mask Building for Perceptually Hiding Frequency Embedded Watermarks,” Proc. Int. Conf. on Image Processing, Oct. 1998, vol. I, pp. 450-454.

[16]. D. Kundur and D. Hatzinakos, “A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion,” Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 544-547.

[17]. J. Delaigle, C. De Vleeschouwer, and B. Macq, “Psychovisual Approach to Digital Picture Watermarking,” Journal of Electronic Imaging, vol. 7, no. 3, pp. 628-640, July 1998.

[18]. S. Craver, N. Memon, B. Yeo, and M. Yeung, “Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications,” IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 573-586, May 1998.

[19]. P. Bas, J. Chassery, and F. Davoine, “Using the Fractal Code to Watermark Images,” Proc. IEEE Int. Conf. on Image Processing, vol. I, Oct. 1998, pp. 469-473