The 5th Student Conference on Research and Development –SCOReD 2007
11-12 December 2007, Malaysia

Improving Invisibility of Blind Video Watermarking Scheme

Ahmed A. Baha'a Al-Deen, Abdul Rahman Ramli, Mohammad Hamiruce Marhaban, and Syamsiah Mashohor

Abstract-- **A video watermarking algorithm is developed here to embed a binary image inside the uncoded video stream acting as a logo. A mid-band discrete wavelet transform coefficients of the selected frames are chosen to be the hosted region in the frequency domain. An inverse transformation should be taken in order to get the desired watermarked video shot. In extraction process the watermark is extracted from the marked video directly without access to the original video. The experiment results showed that the proposed scheme provides better quality watermarked videos in term of watermark invisibility to human eyes. In conclusion, modifying the wavelet coefficients depending only on the logo object's pixels will highly improve the invisibility and at the same time providing a good robustness level.**

Index Terms—**BER, Copyright protection, PSNR, Video watermarking, Wavelet transform.**

I. Introduction

Digital Television offers many potential benefits in picture quality which able to store and copy material without loss of quality or fidelity resulting superior quality compared with analog form due to noise free transmission. At the same time, there has been tremendous growth in computer networks and increasing of the computer performance create considerable challenges for copyright enforcement. Thus, there is a great desire for copyright systems that can preserve the economic value of digital data and protect the rights of the owners. [1,2,3,4].

Until recently, the primary tool available to protect content owners' rights has been encryption. Encryption protects content during the transmission of the video stream from the sender to receiver, by encrypting the video using a secret key. However, this technique has one significant disadvantage: encryption does not offer any protection once the encrypted video has been decrypted. This is a significant limitation and encryption alone may not be sufficient for copyright protection. In fact, it is mainly concerned with secure communication but not copyright protection [5].

Digital watermarks have been proposed as a way to handle this tough issue. A watermark could act as invisible signature to discourage copyright violation. This may help to determine the authenticity and ownership of the copyrighted video even after data has been decrypted.

Watermark embedding techniques apply minor modifications to the host video in a perceptually invisible manner, where the modifications are related to the watermark information. The watermark information can be retrieved afterwards from the watermarked video by detecting the presence of these modifications. A wide range of modifications in any domain can be used for watermarking techniques. Prior to embedding or extracting a watermark, the host video can be converted, for instance, to the spatial, the Fourier, the wavelet, the discrete cosine transform or even the fractal domain, where the properties of the specific transform domains can be exploited [6].

A large variety of watermarking techniques is currently available in the literature. The proposed schemes have shown that digital watermarks can be fairly successful in achieving the desired properties such as imperceptibility and resistant to wide range of attacks. These watermarks, however, are not perfect, and more could be done to improve a watermark's robustness or accuracy in detection.

The wavelet domain proved to be highly resistant to both compression and noise, with minimal amounts of visual degradation. The wavelet domain may be one of the most promising domains for digital watermarking yet found [7].

On the other hand, the schemes of embedding digital watermark into still image have been researched and developed greatly. Whereas the researches of embedding watermark into video are not sufficient enough. Because the video is dominant in the practice, it is significant to research it in more deep way [8].

In order to be robust against format conversions and to prevent the watermark data from being vanished the watermark has to be inserted before compression i.e. in the non-compressed raw video [2,9].

Ahmed A. Baha'a Al-Deen, Faculty of Engineering, Universiti Putra Malaysia, (e-mail: gs15542@mutiara.upm.edu.my).
Abdul Rahman Ramli, Institute of Advanced Technology ITMA, Universiti Putra Malaysia, (e-mail: arr@eng.upm.edu.my).
Mohammad Hamiruce Marhaban, Faculty of Engineering, Universiti Putra Malaysia, (e-mail: hamiruce@eng.upm.edu.my).
Syamsiah Mashohor, Faculty of Engineering, Universiti Putra Malaysia, (e-mail: syamsiah@eng.upm.edu.my).

The watermark detection can be carried out in two ways: blind and non-blind detections. Non-blind detection needs the help of the original video during the process of video watermarking detection. However, this method is not suitable in this massive digital video era. The blind detection mode is chosen for designing the video watermarking scheme [9].

II. THE PROPOSED SCHEME

A. *Watermark Embedding Process*

Let $f(m,n)$ be the original frame to be watermarked with the binary image $w(m_1,n_1)$, and Fe is a generalized formula of the embedded function which takes the original image $f(m,n)$ and watermark $w(m_1,n_1)$ and then generate a new frame called a watermarked frame $f'(m,n)$ such that there is no perceptually significant degradation in the watermarked frame as compared to the original frame. The relation can be expressed as:

$$f' = F_e(f,w) \tag{1}$$

Note that in the case of video, the embedded frame must not only satisfy the invisibility as each frame which is viewed as a static image (denotes as static invisibility), but also satisfy the invisibility as frames which are playing at a certain frame rate (denotes as dynamic invisibility).

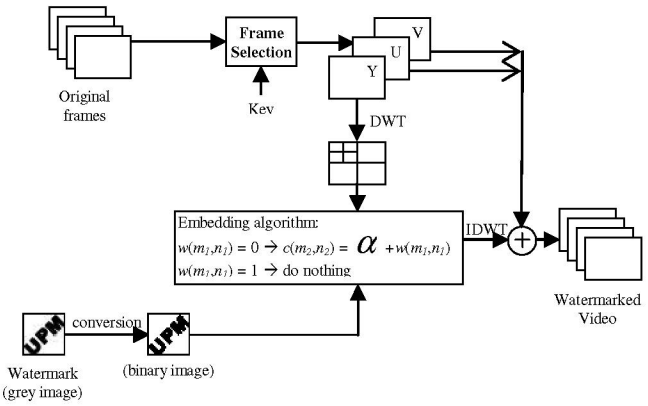


Figure 1: Proposed video watermarking (embedding process)

A block diagram of the proposed video watermarking algorithm is shown in Figure 1. The embedding process is composed of the following steps:

Step one: Load video and watermark

Load the original video signal and the original watermark image $w(m_1,n_1)$. The video files have a certain aspect ratio and frame rate with a fixed total number of frames and the resolution $M \times N$ pixels for each video frame. The watermark used could be a grey-scale or a binary image with the size of $M_1 \times N_1$ pixels. To simplify the presentation of the pre-processing steps, the binary image is assumed as the watermark.

Step two: Select a frame

To make the meaningful watermark to be more randomized and secretive, a random number matrix with each element different and its values denote the frame number is used as the key. It is the exclusive key to pick the frames that are to be watermarked. Without the valid key, it will be difficult for any attacker to break the hidden data even when the embedding method is known.

Step three: Colour component selection

The video frame consists of Y, U and V colour components. Both the U and V components are decimated because the human visual system (HVS) is dull for the change of these components. Hence, if the watermark is embedded into these components, it may be vanished. For this reason, the Y component is chosen to carry the watermark information and considered to be a grey-scale image.

Step four: DWT decomposition

Apply 3 levels 2 dimension wavelet transform to the selected frame $f(m,n)$ to decompose it to ten sub-bands of frequencies: LL_3, LH_3, HL_3, HH_3, LH_3, LH_2, HL_2, HH_2, LH_1, HL_1, and HH_1. The filter used in this transformation can be determined by the owner of the video data and hence, used as part of the security key. Here, the wavelet Haar filter [10] is used because of to its simplicity.

Step five: Sub-band selection

The mid frequency sub-bands LH_2, HL_2, and HH_2 are the candidates for watermark insertion. Among these sub-bands, the one which has the minimum energy e_s is chosen. The energy of a sub-band is defined by the following equation:

$$e_s = \frac{1}{M_2 \cdot N_2} \sum_{m_2=0}^{M_2-1} \sum_{n_2=0}^{N_2-1} c(m_2,n_2) \tag{2}$$

Where $M_2 \times N_2$ denotes the size of the sub-band, the $c(m_2,n_2)$ is the coefficients of the sub-band. In the other words, the min $e_s\{LH_2, HL_2, HH_2\}$ are the sub-bands in which the watermark is embedded.

Step six: Embed the watermark in the selected sub-band

In the embedding step, only the object's pixels of the binary logo watermark with zero values are embedded into the centre of the selected sub-band $c(m,n)$ by using the following formula:

$$c(m_2,n_2) = \begin{cases} w^*(m_1,n_1) & if \quad \frac{M_2-M_1}{2} < m_2 < \frac{M_2+M_1}{2} \\ & and \quad \frac{N_2-N_1}{2} < n_2 < \frac{N_2+N_1}{2} \\ c(m_2,n_2) & otherwise \end{cases} \tag{3}$$

Where $w^*(m_1,n_1) = \alpha + w(m_1,n_1)$ in case of object, $M_2 \times N_2$ is the size of the selected sub-band, and $M_1 \times N_1$ is the size of the watermark, $0 \le m_1 < M_1$, $0 \le n_1 < N_1$, and $0 \le m_2 < M_2$, $0 \le n_2 < N_2$, α : scaling factor.

Step seven: IDWT

The watermarked luminance colour component (Y) is obtained by applying the inverse discrete wavelet transform (IDWT) to the watermarked DWT coefficients.

Step eight: Re-mixture the colour components

The watermarked frame is obtained by remixing or concatenating the watermarked luminance Y with the other chrominance U and V colour components.

Step nine: Store and display the watermarked video

In this step, the procedure used to read and store the video file could be summarized as the followings

- Read the first video frame and check if whether the number is included in the key or otherwise.
- If the number is included, apply the watermarking subroutine on it and save it in a new video file.
- If the number is not included, skip the subroutine and save the frame in the new video file.
- Continue this loop until the last frame is reached.

After this step, the watermarked video is released (distributed) to the public.

B. Blind Detecting Video Watermark

The extraction process requires the key used for selecting the frames, the wavelet transform filter, and the channel in which the watermark is inserted. Due to the act of requantizing, a threshold region T should be defined in order to detect the existence of the video watermark. Figure 2 shows the overall process of watermark extraction process.

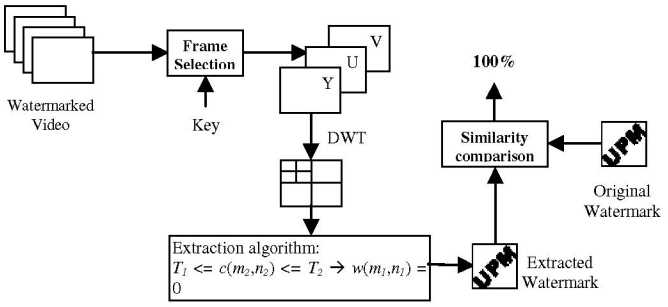


Figure 2: Proposed video watermarking (extraction process)

The generalized formula of the above extraction function is as below:

$$w^* = F_x(f') \tag{4}$$

The watermark is extracted from the watermarked video by the following steps:

Step one: load the watermarked video and original watermark

Step two: select a frame depending on the key used in the embedding process, and search for the watermarked frames.

Step three: apply 3 levels 2 dimension wavelet which is transformed to the Y components of the watermarked frame using the same Haar filter that is used in the embedding process.

Step four: go to the selected sub-band in which the watermark was embedded.

Step five: the watermark is extracted from the selected sub-band according to the following condition:

$$w(m_1,n_1) = \begin{cases} 0 & T1 <= c(m_2,n_2) <= T2 \\ 1 & \text{otherwise} \end{cases} \tag{5}$$

Then, the extracted bits are normalized to be either ones or zeros. A reshape should be taken in order to finalize the extracted watermark $M \times N$ and reconstruct the watermark image.

Step six: The similarity between the original and the extracted watermark is computed.

III. EXPERIMENTAL RESULTS

Computer simulations were carried out to demonstrate the performance of the proposed algorithm. The following video sequences are used in the experiments. These sequences are all in the CIF and QCIF format which represent different video scenarios, widely used in the video research community. The sequences for CIF and QCIF have frame size of 352×288 and 176×144 pixels respectively for luminance resolution with 4:2:0 chrominance subsampling. The aspect ratio is 4:3. The Y, U and V components are then concatenated together for each frame. In the experiments, the watermark is a 32×32 pixels binary image. The average Peak signal to noise ratio (PSNR) was used as an objective measure of invisibility, while the Bit error rate (BER) was used to measure robustness. To evaluate the robustness, various attacks were used, such as filtering, noise addition, and MPEG coding.

A. Watermark Embedding and Invisibility Measures

The first original frame and first watermarked frame of the mobile video sequences are shown in Figure 3. The proposed algorithm produced an almost invisible subjective difference between the original and the watermarked frame.

Figure 3: The first frame from original mobile video (left) vs. watermarked version (right)

The invisibility is measured by calculating the average Mean Square Error (MSE) and average Peak Signal to Noise Ratio (PSNR). To evaluate the invisibility, the proposed method is compared with the direct embedding. Table 1 show that the proposed algorithm produced a lower average MSE and higher average PSNR than conventional methods. The higher the PSNR, the better the quality of video is.

Table 1: Invisibility results of the test clips

Video sequence	Direct embedding		Proposed method	
	MSE	PSNR	MSE	PSNR
Mobile	13.9076	36.7060	5.2758	40.9506
Tempete	7.7492	39.2808	3.5351	42.6823
Salesman	10.5930	37.8837	5.2654	40.9209
Suzie	5.3750	40.9154	2.7703	43.7799

The above results show that the proposed watermarking scheme can keep good quality of the host video. This invisibility of the watermark guarantees that an unauthorized person does not know the existence or location of the watermark. Note that in general for digital images, noise with PSNR higher than 30 dB is hardly noticeable. It can be seen that the proposed method does not cause perceptual artifacts.

B. Watermark Extraction and Robustness Measures

To investigate the robustness of the watermark, the watermarked video is attacked by some common possible attacks that the marked video could suffers such as MPEG compression, low pass filtering, and noise addition. Then, the extraction process can proceed. The frame key, wavelet filter, watermark strength and the wavelet subband in which the watermark is inserted, are needed to extract the watermark from the attacked video. The similarity between the original and extracted watermark is measured by Bit Error Rate (BER). Table 2 and shows the BER results.

Table 2: Similarity measures in case of no attacks

Video sequence	*Direct Embedding BER%*	**Proposed method BER%**
Mobile	0	1.3672
Tempete	0	1.1719
Salesman	0	2.2461
Suzie	0	0.6836

Original watermark Extracted watermark

Figure 4: Original vs. extracted watermark in case of no attacks

From the above table, the small error value occurred in the proposed method is caused due to some of the neighbors pixels of the logo's object that could be in the threshold region i.e. they may have a same or near values of the embedded pixels as shown in Figure 4. This tiny distortion is acceptable comparing with the invisibility improvement and robustness enhancement obtained by the proposed method against attacks.

B.1 MPEG Compression

The MPEG coding is one of the most basic attacks to video watermark. The video watermarking scheme should be robust against it. The test here is run as encode and decode the watermarked video frames with MPEG format at frame rate 30frames/sec. and video bitrate at 2.3Mbps. The scheme for this test is as shown in Figure 5.

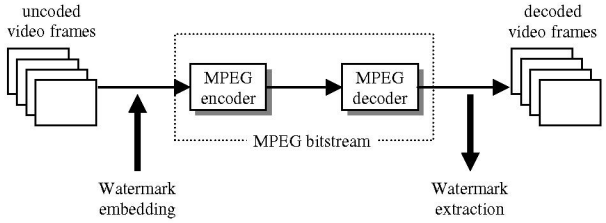


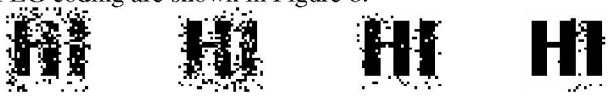
Figure 5: The video watermarking system in the uncoded and decoded domain

The algorithm is robust for MPEG compression and the highest error was 13.6% for the proposed embedding. Table 3 shows the BER values for direct and proposed method.

Table 3: Similarity measures in case of MPEG

Video sequence	*Direct Embedding BER%*	**Proposed method BER%**
Mobile	17.5781	13.6719
Tempete	15.6250	13.3789
Salesman	7.9632	5.6641
Suzie	4.8828	2.6367

The watermark images extracted from the test clips after MPEG coding are shown in Figure 6.



Mobile Tempete Salesman Suzie

Figure 6: Extracted watermark for the proposed method after MPEG coding

The reason behind the better quality of the extracted watermark in case of suzie rather than mobile is depends on the large number of details in mobile comparing to suzie, this details could be removed during the MPEG compression.
From the above, the results show that the quality of the extracted watermark images was good enough to claim copyright and ownership of the digital media.

Figure 7: The effect of MPEG compression

B.2 Filtering

It is possible that the attackers may try to destroy the embedded watermark by filtering using different filters. Therefore, the watermark should be resilient to such possible filtering techniques. For this purpose, the watermarked frames are transformed to frequency domain using Fast Fourier Transformation (FFT), and frequencies above the cutoff point will be removed. Figure 8 illustrates the effect of such process.

Figure 8: The effect of low pass filter

The extraction results in Table 4 and Figure 9 demonstrate that the proposed method acts well under this test.

Table 4: Similarity measures in case of LPF

Video sequence	Direct Embedding BER%	Proposed method BER%
Mobile	13.8672	9.2773
Tempete	13.1836	10.8398
Salesman	14.0625	10.0586
Suzie	15.2344	9.0820

Mobile Tempete Salesman Suzie

IV. Figure 9: Extracted watermark for the proposed method after LPF

B.3 Noise Addition

Noise addition is another method to estimate robustness of the watermark. In many cases the degradation and distortion of the media come from noise addition. The watermark information is also degraded by noise addition and resulted in difficulty in watermark extraction. A salt & pepper noise with density 0.02 is used to investigate the robustness of the watermark. Table 5 and Figure 10 are shown the BER results and the extracted watermarks respectively.

Table 5: Similarity measures in case of noise addition

Video sequence	Direct Embedding BER%	Proposed method BER%
Mobile	13.6291	12.5977
Tempete	13.9924	13.1836
Salesman	15.2720	14.8438
Suzie	12.2070	11.6211

Mobile Tempete Salesman Suzie

Figure 10: Extracted watermark for the proposed method after noise addition

It can be concluded from the results above, that the watermark can be detected even when the noise is added to the watermarked frame. Obviously from the data above, the proposed watermarking system have the ability to embed a watermark in the video with higher degree of invisibility, and enhances the robustness of the watermark against many attacks.

V. CONCLUSIONS AND FUTURE WORK

The method proposed in this paper focuses on reducing the degradation of the watermarked video, i.e. the invisibility of watermark, in which this requirement is considered as one of the most important, ruling the visual quality of the resulted watermarked video. The proposed idea is summarized by embedding only the object's pixels of the logo and the background is estimated. Hence, this reduces the number of the modified coefficients.

The result indicates a positive outcome, whereby it is found that the watermarked video has a better visual quality with an average PSNR equivalent to 41.59dB as compared to 38.48dB in the case of direct embedding. At the same time, the watermark is still be able to resist a variety of attacks, including the MPEG coding and re-encoding, filtering and noise addition. In all cases, the watermark is successfully recovered, and this supports the robustness of the video watermarking scheme.

Open paths still remain in video watermarking. This technology is indeed in its infancy and at the same time, far from being as mature as for still images. Many limitations and challenges have yet to be overcome.

The following are some suggested paths: more attacks and watermarks are required on the proposed scheme. Real-time processing of the proposed watermark method is considered as made possible by using the DWT hardware device proposed in [11] because both the DWT and the inverse DWT occupy most of the processing time of the proposed embedding and extracting algorithms.

VI. REFERENCES

[1] F. Hartung, B. Girod, "Watermarking of uncompressed and compressed video" Signal Processing, vol. 66, no. 3 (Special issue on Watermarking), pp. 283-301, May 1998.

[2] Z. Huai-yu, L. Ying, and W. Cheng-ke, "A blind spatial-temporal algorithm based on 3D wavelet for video watermarking", IEEE International Conference on Multimedia and Expo (ICME), 2004.

[3] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol.35(3/4), pp.313-336, 1996.

[4] I.J. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Transaction Image Processing, vol.6, no.12, pp.1673-1687, 1997.
[5] Lin, E.T., Eskicioglu, A.M., Langendijk, R.L., and Delp, E.J., "Advances in Digital Video Content Protection", in Proceedings of the IEEE, Vol. 93, No. 1, pp. 171-183, Jan. 2005.
[6] Langelaar, G.C., Setyawan, I., and Lagendijk, R.L., "Watermarking Digital Image and Video Data", in Proceedings of the IEEE Signal Processing Magazine, pp. 20-46, Sep. 2000.
[7] C. Shoemaker, "Hidden Bits: A Survey of Techniques for Digital Watermarking", Independent Study, 2002.
[8] L.S. Liu, R.H. Li, and Q. Gao, "A robust video watermarking scheme based on DCT", In Proceedings International Conference on Machine Learning and Cybernetics IEEE, pp. 5176- 5180, Vol. 8, 2005.
[9] M. Ejima, A. Miyazaki, "A wavelet-based watermarking for digital image and video", in Proceedings in International Conference on Image Processing IEEE, pp.678-681, vol.3, 2000.
[10] Weackerhouser, M.V., "Adaptive Wavelet Analysis from Theory to Software", A.K. Peters, Ltd., 1993.
[11] Omaki, R.Y., Fujita, G., Onoye, T., and Shirakawa, I., "Implementation of DWT and EZW cores for a bitrate scalable video coder", Proc. International Technical Conference on Circuits/Systems, Computers and Communications, ITC-CSCC'98, vol.1, pp.221-224, Sokcho, Korea, July, 1998.