

A Scene Based Video Watermarking in Discrete Multiwavelet Domain

N. Leelavathy¹, E. V. Prasad² and S. Srinivas Kumar³

^{1,2}Department of Computer Science & Engineering, J.N.T. University, Kakinada, A.P. India

³Department of Electronics & Communication Engineering, J.N.T. University, Kakinada, A.P. India

¹nleelavathy@gmail.com, ²drevprasad@yahoo.co.in, ³samay_ssk2@yahoo.com

Abstract— The rapid increase in internet usage has resulted in the media ownership and attention towards intellectual property rights among internet users. In this paper, a Discrete Multiwavelet Transform (DMWT) and Quantization Index Modulation (QIM) based video watermarking is proposed. A logo watermark is inserted in the uncompressed domain of a video. Using QIM, the watermark is embedded into the selected multiwavelet coefficients by quantizing the coefficients. Scrambled watermarks are generated using a set of secret keys, and each watermark is embedded in each motionless scene of the video. The watermark extraction does not require the original video. Experimental results demonstrate that the proposed method is robust against the frame dropping, averaging, swapping, and statistical analysis attacks. It is also robust against some intentional and unintentional attacks.

Keywords— Discrete Multiwavelet Transform, Quantization Index Modulation, Quantization Step, Scene-Change and S-Transform

I. INTRODUCTION

There is a wide use of Internet facility for digital media transfer. It has increased the interest in multimedia security and multimedia copyright protection for the data owners. In this paper, an approach for protecting a video copyright with watermarking technique is introduced. Video watermarking is a technique used for protecting the intellectual property rights of a digital media by embedding a logo or watermark into the video.

Video watermarking schemes can be roughly divided into two categories: spatial domain watermarking and frequency domain watermarking. The watermarking schemes in spatial domain are less robust than that of frequency domain and can be used for proving the integrity of the data. The frequency domain watermarking using Fast Fourier Transform (FFT), Discrete Wavelet Transform (DWT), S-Transform (a modified Haar wavelet), Walsh Transform (WT), Contourlet Transform (CT), Discrete Multiwavelet Transform, etc., are more robust than spatial domain techniques.

Lot of research is undertaken in the transform domain. As video watermarking is associated with many sophisticated technologies, it needs further research in transform domain and is application specific. The oblivious video watermarking still remains a challenging problem since the original video is often unavailable due to the size of the videos. The video watermarking schemes are based on the techniques of the

image watermarking and are applied to raw video in the uncompressed domain or the compressed video which are domain specific [1]-[4]. As the coded video streams can be easily converted using public domain converters, the watermarking strategy in uncompressed video offers better robustness than compared to compressed domain techniques.

Chen and Wornell [5], [6] proposed Quantization Index Modulation (QIM) watermarking which protects against fully informed attacks than compared to time consuming spread spectrum computations. QIM implementation of embedding/detection is a low complexity method which relies on uniform scalar quantization called Dither Modulation (DM). There is always a trade of between quantization step and the quality of the video. Higher is the quantization step better is the sustainability against attacks. But with the increase in the quantization step, the quality of the video is reduced.

Hui-Yu Huang, et al. [7] method has used modified 3D-DCT and QIM in the frequency domain of a sequence of video which is effectively resistant to compressions, noises, and filtering attacks but not robust to geometric attacks. Hefei Ling, et al. [8] method is suitable for DCT based compressed videos. The method is based on Harris-Affine detector and is resistant to rotation, scaling attacks, cropping, etc. Po-Chyi Su, et al. [9] method is used for authentication of digital video in H.264/AVC. This algorithm uses a scene change for calculating the hash which in turn determines the watermark sequence.

This paper proposes a multiwavelet transform domain video watermarking scheme based on the scene change analysis. The proposed video watermarking algorithm is robust and transparent against the attacks of frame averaging, dropping and statistical analysis.

This paper is organized as follows: Introduction to discrete multiwavelet transform is given in Section II. The embedding and extraction algorithms are proposed in Section III. The experimental results and analysis are drawn in Section IV. Finally, the conclusions are given in Section V.

II. DISCRETE MULTIWAVELET TRANSFORM

Discrete Multiwavelet transforms divide the image or a video frame into a lower resolution approximation. The process can be repeated to compute multiple scale wavelet decomposition. Discrete Wavelet Transform has a good

property of localization in time and frequency. But multiwavelets have some more advantages over DWT. There is only one scaling function in DWT, where as in multiwavelet transform there are more than one scaling functions. Hence, DWT are called scalar wavelets. In multiwavelet, useful properties like symmetry, orthogonality, short support, and a higher number of vanishing moments are achieved simultaneously.

The multiwavelet scaling function vector is:

$$\Phi(t) = [\Phi_1(t), \Phi_2(t), \dots, \Phi_r(t)]^T \quad (1)$$

which satisfies a matrix dilation equation

$$\Phi(t) = \sum_k C[k] \Phi(2t - k) \quad (2)$$

The coefficients $C[k]$ are $r \times r$ matrices instead of scalars. Associated with these scaling functions are r wavelets i.e., $w_1(t), w_2(t), \dots, w_r(t)$, satisfying the matrix wavelet equation as in Eq. (3)

$$w(t) = \sum_k D[k] \Phi(2t - k) \quad (3)$$

where,

$$w(t) = [w_1(t), w_2(t), \dots, w_r(t)]^T \quad (4)$$

$w(t)$ is a vector and the $D[k]$ are $r \times r$ matrices.

One of the important multiwavelets was constructed by GHM (Geronimo, Hardin and Massopust) system [10, 11]. Similar to scalar wavelets and for the case where $r = 2$, GHM multiwavelets function satisfies the following two-scale equations as shown in Eq. (5) and Eq. (6)

$$\Phi(t) = \sqrt{2} \sum_{k=-\infty}^{\infty} H_k \Phi(2t - k) \quad (5)$$

$$\Psi(t) = \sqrt{2} \sum_{k=-\infty}^{\infty} G_k \Phi(2t - k) \quad (6)$$

The histogram difference method [12] is used for scene change detection. Scene-change is detected from the raw frames of the investigated video before the watermark embedding. Independent watermarks $\{m_1, m_2, m_3, \dots, m_k\}$ produced from the logo watermark selected are embedded in the frames of different video scenes. Within a motionless scene, an identical watermark is used in each frame. Watermark m_1 is used for the first scene. When there is a scene change, another watermark m_2 is used for the next scene. 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. Experiments have shown that the sensitivity of the human visual system drops significantly after a scene change in a video sequence. It takes up to 100 ms for the visual system to adapt to the new stimuli. During this interval, the images of the video sequence can suffer considerable quality degradation without a perceptual loss of quality [13].

III. PROPOSED WATERMARKING SCHEME

A. Preprocess of Watermark

The visually recognizable watermark is better than a correlation value, and also improves the proof of ownership even for non-technical arbiters. In this paper a watermark logo is chosen. The watermark logo is scrambled with a predefined set of secret keys $\{k_1, k_2, k_3, \dots, k_n\}$ generated from a secret key. Each key k_n generates a scrambled watermark logo for embedding into each scene.

The following are the reasons for scrambling the watermark logo:

- Scrambling is to protect against an attacker because attacker may be able to detect the logo but attacker gets the scrambled image and, is not useful.
- Applying independent watermarks to each frame presents a problem of maintaining statistical and perceptual invisibility. If the regions of each video frame remain little or motionless then, regions may be statistically compared or averaged to remove the watermarks. Hence, algorithm uses an identical watermark within each motionless scene and a different watermark for every scene change. Hence, the proposed method is robust against the attacks of frame dropping, averaging, swapping, and statistical analysis.

B. The Video Preprocess

Scene changes are detected from the raw video by applying the histogram difference method on the video. That is, the histograms of adjacent frames is calculated as given by Eq. (7)

$$Z_m = \sum_{b=1}^{N_{bins}} |H_m(b) - H_{m-1}(b)| \quad (7)$$

where N_{bins} is the total number of bins in the frame luminance and H_m is the histogram associated with the frame, F_m . If Z_m is larger than a threshold, T_c a scene change has taken in the frame, F_m .

C. The Watermark Embedding Algorithm

The following steps of watermark embedding algorithm for each scene k of the video are as follows:

1. Each frame of a video of size $N_k \times M_k$ is divided into blocks of $r_k \times s_k$.
2. The scrambled watermark logo from a set of $\{m_k\}$ generated is used as per the secret key. It is impossible to obtain the original watermark logo without the secret key.
3. Each block $r_k \times s_k$ is pre-filtered to produce two input streams.
4. GHM multiwavelet transform is applied to the block after pre-filtering. A 2nd level decomposition is performed on each block. The 'low-low-pass' sub-bands

of 2nd level are selected for watermark embedding where it concentrates most of the energy of the frame.

5. The bits of watermark logo mk , w_i will be embedded into the multiwavelet coefficients of selected blocks using QIM method described below:
 - i) A coefficient, c_n from the selected sub-band is chosen,
 - ii) A frame based threshold, t is calculated. Then, one coefficient from each block is quantized with respect to watermark bit $w_i(i, j)$.

$$d = (c_n - t) \bmod Q,$$

if $w_i(i, j) = 0$

$$c_n' = c_n - d + (Q/4),$$

else if $w_i(i, j) = 1$

$$c_n' = c_n - d + (3Q/4)$$

end.

6. The inverse GHM multiwavelet is applied to the modified sub-block.
7. The post-filtering is performed in each block and the final watermarked blocks of the frame are reassembled.

D. The Watermark Extraction Procedure

The steps of watermark extraction algorithm for each scene k of the video are as follows:

1. Each frame of a video of size $N_k \times M_k$ is divided into blocks of $r_k \times s_k$.
2. Each block $r_k \times s_k$ is pre-filtered to produce two input streams.
3. GHM multiwavelet transform is applied to the block after pre-filtering. A k 2nd level decomposition is performed on each block. The 'low-low-pass' sub-bands of 2nd level are selected for watermark embedding where it concentrates most of the energy of the frame.
4. The bits of w_i' extracted are as follows-
 - i) A coefficient from the selected sub-band is chosen, c_n .
 - ii) A frame based threshold, t is used.

$$d' = (c_n' - t) \bmod Q,$$

if $d' \leq Q/2$,

$$w_i'(i, j) = 0$$

else

$$w_i'(i, j) = 1$$

end.

5. The scrambled watermark is descrambled with the same secret key to obtain the original watermark.

IV. EXPERIMENTAL RESULTS

The proposed system does not require the original video for detecting the watermark logo. This system needs to communicate the quantization step, video dependent threshold th and a secret key to the watermark logo retrieving end. In this system, one scrambled watermark logo mk is embedded into one motionless scene of a video. The Peak Signal to Noise Ratio (PSNR) values are computed for the test videos (stennis and foreman). The proposed algorithm is tested using multiwavelet transform, DWT, and S-Transform and the results are illustrated in Fig. 1(a) and Fig. 1(b). The Quantization vs PSNR is calculated and is as shown in Fig. 2. It is obvious that, multiwavelet transform is superior to other two transforms viz., DWT and S-Transform.

As one scrambled watermark logo mk is embedded into each and every frame of a video hence, frame dropping attack does not arise. Then, three consecutive frames are averaged and tested against frame averaging attack. Bit Error Ratio (BER) of the retrieved watermark is 0.1182 with a new frame of PSNR value is 28.0584 dB. An identical watermark is used within each motionless scene and consequently, this method is robust against the attacks of frame dropping, averaging, swapping, and statistical analysis.

Various intentional and unintentional attacks, such as noise attacks ("Salt & pepper" noise, Gaussian noise, Speckle noise), JPEG compression, rotational attacks, filtering attacks, cropping, etc., are performed to demonstrate the robustness of the proposed system. The BER of the retrieved watermark logo is shown in Table II and Table III.

On the other hand, selection of video dependent threshold t and choice of multiwavelet transform coefficients from each block plays an important role. The threshold t for stennis video and for foreman video is chosen as 96 and 218 respectively.

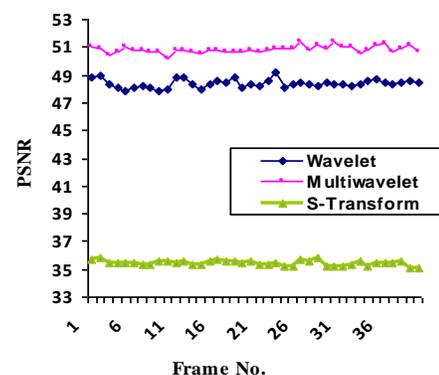


Fig. 1 (a): PSNR in dB for each frame of watermarked stennis video with $Q=40$

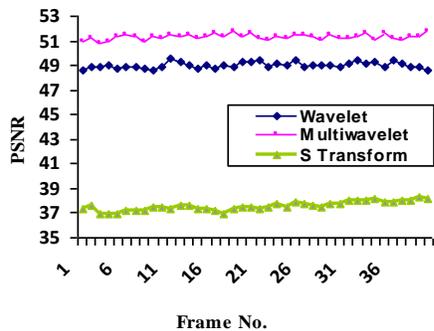


Fig. 1(b): PSNR in dB for each frame of watermarked foreman video

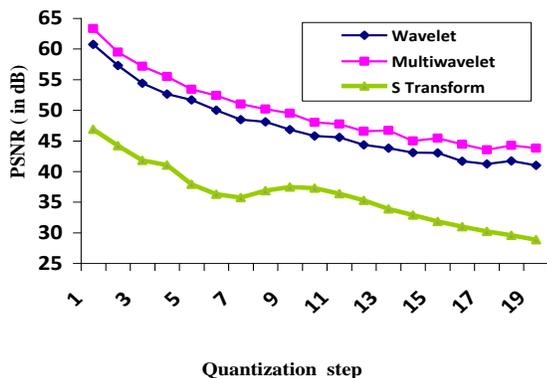


Fig. 2: PSNR in dB vs quantization step of watermarked video frame

TABLE I:
Original watermark logo and watermarked video frames with wavelet and multiwavelet transform

Comparison	Proposed method	Proposed method
Transform Domain	Wavelet (Haar)	Multiwavelet (GHM)
Decomposition Level	Level : 2	Level : 2
PSNR in dB		
		
logo (15×22)	48.03242	50.64191

TABLE II:

BER of retrieved logo after applying various attacks to the frame

S. No.	Type of Attack	Parameter	BER
1	Salt & Pepper Noise	0.001 0.010	0.0030 0.0242
2	Gaussian Noise	0.001 0.010	0.0061 0.0879
3	Speckle Noise	0.001 0.010	0.0061 0.0152
4	Poisson's Noise	-	0.0121
5	Wiener filter (R,G,B planes)	(3×3)	0.1515
6	Cropping	20%	0.0333
7	Bit Plane zero	2nd	0.0061

V. CONCLUSIONS

In this paper, the proposed system is an effective scene based video watermarking technique based on QIM to achieve copyright protection in discrete multiwavelet transform domain. It is easy and less complex to derive the embedded bits as QIM method is used. The detection process does not require the whole original video which is very important in video watermarking. As previously presented, it is obvious that the proposed method can effectively sustain JPEG compression, rotation of the frame, cropping, noises, and filtering attacks and can maintain a good performance in robustness and transparency. Improvement in scene change analysis for gradual changes in the scenes of a video will be the future work.

REFERENCES

- [1] Frank Hartung, and Bernd Girod, "Watermarking of uncompressed and compressed video," Telecommunications Institute I, University of Erlangen-Nuremberg, Cauerstrasse 7, 91058 Erlangen, Germany, Signal Processing 66 (1998) 283-301.
- [2] C. Cruz-Ramos, R. Reyes-Reyes, M.Nakano-Miyatake, and H. Perez-Meana, "A blind video watermarking scheme robust to frame attacks combined with MPEG2 compression," Journal of applied research and Technology, vol. 8, No. 3, Dec., 2010.
- [3] Ersin Esen, and A. Aydin Alatan, "Robust video data hiding using forbidden zone data hiding and selective embedding," IEEE Transactions on circuits and systems for video technology, vol. 21, No. 8, Aug., 2011.
- [4] Gaobo Yang, Junjie Li, Yingliang He, and Zhiwei Kang, "An information hiding algorithm based on intra-prediction modes and matrix coding for H.264/AVC video stream," International Journal of Electronics and Communication, 2011, pp. 331-337.
- [5] Chen B, and Wornell G.W, "Quantization Index Modulation: A class of provable good methods for digital watermarking and information embedding," IEEE Transaction on Information Theory, vol. 47, pp. 1423-1443, 2001.
- [6] Chen B, and Wornell G.W, "Quantization Index Modulation methods for digital watermarking and information embedding of multimedia," Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology, Special issue on Multimedia Signal Processing, vol. 27, pp. 7-33, 2001.

[7] Hui-Yu Huang, Cheng-Han Yang, and Wen-Hsing Hsu, "A video watermarking technique based on pseudo-3D DCT and quantization Index Modulation," IEEE transaction on information forensics and security, vol. 5, No. 4, Dec., 2010.

[8] Hefei Ling, Liyun Wang, Fuhao Zou, Zhengding Lu, and Ping Li, "Robust video watermarking based on affine invariant regions in the compressed domain," Signal Processing, Elsevier, 2011, pp. 1863-1875.

[9] Po-Chyi Su, Chin-Song Wu, Ing-Fan Chen, Ching-Yu Wu, and Ying-Chang Wu, "A practical design of digital video watermarking in H.264/AVC for content authentication," Signal Processing: Image Communication, 2011, pp. 413-426.

[10] Keinert F, "Wavelets and multiwavelets": Chapman and Hall / CRC, 2004, ISBN, 1-58488-304-9.

[11] Geronimo J, Hardin D, and Massopust P, "Fractal Functions and Wavelet Expansions Based on Several Functions," Journal of Approximation Theory, vol. 78, pp. 373-401, 1994.

[12] Xiaoquan Yi, and Nam Ling, "Fast Pixel-Based Video Scene Change Detection," IEEE, Circuits and Systems, 2005.

[13] Steven Schimmel, "Motion Sensitive Video Watermarking: preliminary study," Notlab, Philips, Tech. Rep, Citeseer, April 2001



N. Leelavathy is currently working as Professor and HOD, Computer Science and Engineering Department, Sri Prakash College of Technology, Rajahmundry, A.P., India. She is working towards her Ph.D. at Jawaharlal Nehru Technological University, Kakinada, A.P., India. She received her M.Tech. in Computer Science and Engineering from Jawaharlal

Nehru Technological University, Hyderabad, India in 2003. She did her B.E. in Electronics & Communication Engineering from Vasavi College of Engineering, Hyderabad, India in 1992. She has thirteen years experience of teaching undergraduate students and post graduate students. Her research interests are in the areas of Digital Image Processing, Image Watermarking, and Cryptography and Network Security.



E. V. Prasad is working as Registrar, Jawaharlal Nehru Technological University, Kakinada, India. He received his Ph.D. in Computer Science & Engineering from University of Roorkee in 1990. He did his M.E. in Control Systems from Madras University in 1978. He received his B.E. in Electronics & Communication Engineering from S V University in 1975. He has thirty three years of experience in teaching undergraduate students and post graduate students. He has taught over 15 courses in CSE and supervised 4 Ph.D students. He held different positions in his carrier like Head of the Department, Vice Principal, Principal and BOS Chairman. He is the Co author of four books and published more than twenty papers in National and International journals and 53 in various Conferences. His research interests include Parallel Computing, Data Mining, and Information Security.



S. Srinivas Kumar is currently working as Professor and Director, Sponsored Research, Jawaharlal Nehru Technological University, Kakinada, India. He received his Ph.D. from E&ECE Department IIT, Kharagpur. He received his M.Tech. from Jawaharlal Nehru Technological University, Hyderabad, India. He

has twenty one years experience of teaching undergraduate and post-graduate students and guided number of post-graduate thesis. He has published 30 research papers in National and International journals. Presently he is guiding ten Ph.D. students in the area of Image processing. His research interests are in the areas of digital image processing, computer vision, and application of artificial neural networks and fuzzy logic to engineering problems.

TABLE III:
BER after attacked by JPEG compression with various quality factors (QF) and Rotational attacks for stennis video

QF/ BER	50 / 0.1121	60 / 0.0636	70 / 0.0152	80 / 0.0061	90 / 0.0061	100 / 0
Rotation (in Degree) / BER	0□ 0	1□ 0.0424	5□ 0.0515	15□ 0.1061	30□ 0.1485	45□ 0.1879