Wavelet Domain Quantization Based Video Watermarking

Afshin Shaabany[1] and Fatemeh Jamshidi[2]
[1,2]Science and Research Branch, Islamic Azad University, Fars, Iran

Abstract— **in this Article, We present a robust watermarking technique based on singular value disintegration and PREDA extracted watermark to initiate a digital watermarking technique for working in the Discrete Wavelet Transform domain. The plan practice binary images as watermarks. The maximum capacity is not essential in most implementation; thereby we have diminished it to increase the robustness of the plan. Every bit of the watermark is extending over a number of wavelet coefficients with the use of a secret key. We use error correction codes to increase in quality the resilience of the algorithm. we choose the quantization step q is a tradeoff between the intuitive qualities of the watermarked video Inverse Discrete Wavelet Transform is computed to acquire the watermarked video the q should be small so we try the plan with q=8.The results The experimental results show that the proposed scheme is robust against a variety of attacks including frame dropping and have very good intuitive quality with mean PSNR values of the watermarked videos frame.**

Keywords— Digital Watermarking, Domain Quantization and Resilience to Assault

I. INTRODUCTION

Digital watermarking is a process by which a user-specified signal is hidden or embedded into another signal , for example digital content such as electronic documents, images, sounds and video [2]. The use of digital video applications such as video-conferencing, digital television, digital cinema, distance learning, videophone, and video-on-demand has grown very rapidly over the last few years. Today it is much easier for the digital data owners to transfer multimedia data over the internet, and hence the data could be perfectly duplicated and rapidly redistributed on a large scale. Thus, the importance of copyright protection for multimedia data has become more critical. Digital watermarking is an effective way to protect the copyright of multimedia data even after its transmission there is urgent demand for techniques to protect the original digital data and to prevent unauthorized duplication or tampering. [1]

A variety of watermarking techniques have been proposed to embed a robust watermark into digital images. These techniques can be divided into two main categories according to the inserting domain of the cover image: the spatial domain methods and the transform domain methods.

The spatial domain methods are the earliest and simplest watermarking techniques but they have a low information hiding capacity, and the watermark can be easily erased by image compression. On the other hand, the transform domain approaches insert the watermark into the transform coefficients of the original image "cover", yielding more information inserting and more robustness against watermarking attacks.

The most important issues in video watermarking are the invisibility of the watermark and the resilience of watermarking to assault. A lot of watermarking methods have been examined to increase in quality both of these aspects. Extensive surveys dealing with video watermarking implementation, assault and methodologies can be found in [1], [2].

The DWT is computed by continuous low-pass and high-pass filtering of the discrete time-domain signal. Its consequence is in the manner it connects the continuous-time multi resolution to discrete-time filters. At each level, the high pass filter cultivates detailed information, while the low pass filter collaborated with scaling function cultivate abrasive estimate. We use a 2D version of the analysis and synthesis filter banks by applying a 1D analysis filter bank to the columns of the image and then to the rows. If the image has m rows and n columns, then after applying the 2D analysis filter bank we acquire four sub-band images (LL, LH, HL, and HH), each having $m/2$ rows and $n/2$ columns.[3,6]

Most transform domain techniques use the Discrete Cosine Transform [3] - [5] and the Discrete Fourier Transform [6]. Lately the methods in the Wavelet domain are gaining more popularity due to their excellent localization, frequency extend, and multi-resolution characteristics [7] - [9]. Watermarking plans performed in the compressed domain include those for MPEG 1-4 [10] - [12] and H.26x [13] compressed videos. Such methods usually embed the watermark directly into the VLC code by modifying the transform domain coefficients [10], [11], [13] or the motion vector information [12, 15].

The early video watermarking techniques add a visible signature or a logo to the video frames [1]. These watermarks do not usually cover significant areas of the video frames, making them easy to remove by a cropping attack.

In this paper, we propose a public digital watermarking technique for video copyright protection working in the Discrete Wavelet Transform domain, robust to a series of, temporal and compression assault [1].

II. WATERMARK EXTRACTION

In this Section the examined watermarking plan according to [2].is described. Fig. 1 shows the block diagram of the watermark encoder.

The watermark is embedded in the wavelet coefficients of the LH, HL and HH sub-bands of the second Wavelet disintegration level. The choice of the second [2, 15]

Disintegration level is a tradeoff between the invisibility of the watermark and the resilience to assault.

The intuitive quality of the video will be significantly altered. For these reasons, the best choice for watermark inserting is the second wavelet disintegration level. Fig. 2 shows the sub-bands chosen for watermark inserting and extraction. The number of selected wavelet coefficients of a frame is: [2]

$$d = 3\frac{MN}{2^{2(L-1)}} \qquad (1)$$

The first step of the algorithm is the conversion of the RGB color space into the YUV color space. Y represents the luminance component for example the brightness; U and V represent the chrominance components for example color.

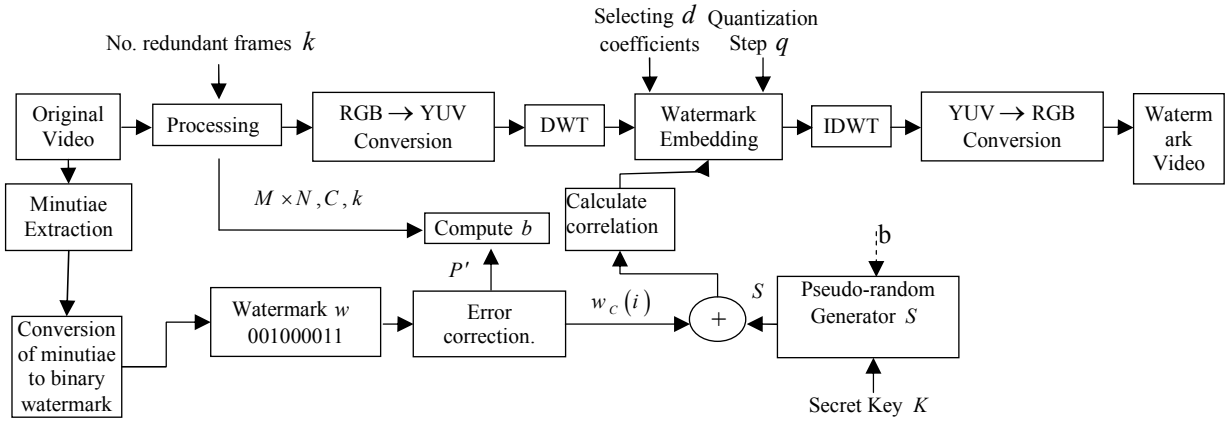

Fig 1. Block Diagram of the examined watermark encoder

Where $M \times N$ is the resolution of the video. The maximum capacity of the watermarking plan is $d' = Fd$ where F the number of video frames is and can be achieved by inserting a watermark bit in every selected wavelet coefficient. For example, for CIF videos of resolution 352x288 and 30 frames/s, the maximum capacity is 556 kb/s. This maximum capacity is not essential in most implementation, thus we have diminished it to increase in quality the robustness of the plan. The watermark used by the encoder is a binary image of resolution $A \times B$ depending on the size of the original video, the error correction code used and the number of redundant frames. The steps of the watermark inserting process are described in the following: [2]

1) The original video is partitioned into groups of k frames.

2) Convert the I-frames from RGB to YUV

3) Apply Discrete Wavelet Transform to the converted luminance layers (Y) of the I-frames to acquire 4 sub-bands of each frame. For each set of I-frames, divide the sub-bands into four chunks (groups). The first group is created from LL sub-bands, the second one from LH sub-bands, the third one from HL sub-bands, and the fourth one from HH sub-bands.

4) Extract Minutiae points such as end points and divided into two parts points are recognized by calculating Crossing number. Crossing Number method squeeze the ridge endings and divided into two parts points from the framework image by examining the local area of each ridge pixel using a 3×3 window.

5) The binary image is transformed into a binary row vector w of size $P = A \times B$.

6) To protect the watermark against bit errors, a Hamming error correction code with codeword length of m bits and data-word length of n bits is applied on the vector$w$. The size of the resulting watermark vector w_C is:

$$P' = P\frac{m}{n} \qquad (2)$$

LL	LH
HL	HH

Fig 2. Wavelet detail coefficients selected for inserting and extraction

7) The binary sequence w_C is partitioned into a number of $\frac{C}{k}$ sequences $w_C(j)$ of size $P'\frac{k}{C}$, $j = 1, \overline{\frac{C}{k}}$, where C is the number of video frames. The same sequence $w_C(j)$ will be embedded into every frame of the group j of frames.

8) The number b of wavelet coefficients in computed

9) An extend-spectrum technique is used to extend the power spectrum of the watermark data, thus, increasing its robustness against assault. First a binary pseudorandom code sequence $S = \{s_r \mid S_r \in \{0,1\}, r = 0,1,\cdots,b\}$ with equal number of zeros and ones is generated using the Mersenne-Twister algorithm by Nishimura and Matsumoto [14] with the use of a 64 bit secret key K as seed for the generator.

10) Calculate the correlation between the selected Watermarked sub-band and the generated pseudorandom Sequence.

11)Number b depends on the number d of the selected wavelet coefficients of every frame, the number of frames C of the original video, the size P of the watermark and the number k of redundant frames:

$$b = \left\lfloor \frac{dC}{P'k} \right\rfloor \quad (3)$$

12) Every sequence S (representing one bit of the original watermark) is embedded into a number b of wavelet coefficients, every bit of S in a wavelet coefficient A bit of the binary sequence S is embedded in the selected wavelet coefficient by rounding its value to an even or odd quantization level. Rounding to an even quantization level embeds a "0", while rounding to an odd quantization level embeds a "1" of the sequence S , as shown in Equation (4):

$$c^w = \left\lfloor \frac{c}{2q} \right\rfloor 2q + qw_C \, sign\left(d - \left\lfloor \frac{c}{2q} \right\rfloor 2q \right) \quad (4)$$

Where c is the original wavelet coefficient, c^w is the watermarked wavelet coefficient, q is the quantization step and $sign(.)$ is defined as:

$$sign(x) = \begin{cases} -1, if \ x \le 0 \\ +1, if \ x > 0 \end{cases} \quad (5)$$

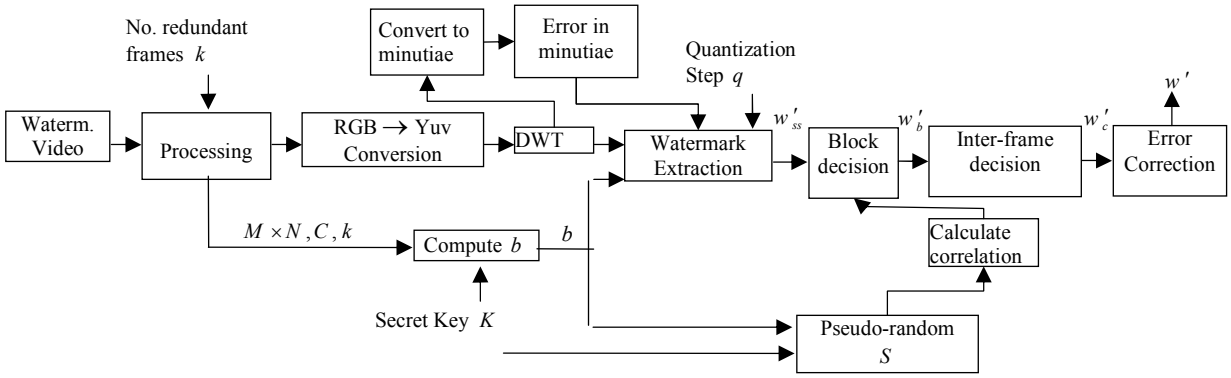

Fig 3. Block diagram of the examined watermark decoder

Watermark bit	Binary pseudorandom sequence S	Extend spectrum watermark	Quantization step size	Original Wavelet coefficient	Watermarked wavelet coefficient
w=0		□0 0 0 1□			[50 4 68 82]
w=1	□0 1 0 0□	□1 11 0□	q=8	[52 6 72 84]	[54 8 72 88]

TABLE I
EXAMPLE OF INSERTING A WATERMARK BIT IN 8 WAVELET COEFFICIENTS

13) Finally use the modified I-frames to produce the watermarked video sequence.

. An example of inserting a watermark bit in a group of 8 wavelet coefficients is given in Table 1.The choice of the quantization step q is a tradeoff between the intuitive qualities of the watermarked video (q should have a small value) and the resilience of the watermarking plan to assault (q should have a big value).[2]

The watermark extraction process, shown in Fig. 3, implies the following steps: [2]

1) The watermarked video is partitioned into groups of k frames.

2) Convert the I-frames from RGB to YUV

3) Use Discrete Wavelet Transform to the converted luminance layers (Y) of the I-frames to acquire 4 sub-bands of each frame

4) The watermarked wavelet coefficients are selected according to the model in Fig. 2.

5) Select the sub-band into which the watermark was embedded

6) From every selected wavelet coefficient a watermark bit is extracted using Equation (6), resulting in a sequence w'_s of b bits from every group of b coefficients:

$$w' = \mathrm{mod}\, 2\left(round\left(\frac{c^w}{q} \right) \right) \quad (6)$$

Where c^w is the watermarked wavelet coefficient.

7) Using the 64 bit seed from the secret key K the binary sequence S of b bits is locally generated.

8) The watermark bit w'_b corresponding to the group of b wavelet coefficients is determined using Equation (7):

$$w'_b = \begin{cases} 0, dec\tilde{a}\sum_{r=1}^{b}\left|w'_{ss.r} - s_r\right| \le \frac{b}{2} \\ 1, dec\tilde{a}\sum_{r=1}^{b}\left|w'_{ss.r} - s_r\right| > \frac{b}{2} \end{cases} \quad (7)$$

9) From every frame of a group of k frames a binary sequence, $w'_{c,i}(j)$ is extracted, where $i = \overline{1,k}$. The watermark sequence corresponding to the group j of frames is acquired using Equation (8):

$$w'_c(j) = \begin{cases} 0, dec\tilde{a}\sum_{r=1}^{k} w'_{c,i}(j) \le \frac{k}{2} \\ 1, dec\tilde{a}\sum_{r=1}^{k} w'_{c,i}(j) > \frac{k}{2} \end{cases}, j \in \{1, 2, \cdots, P'\} \quad (8)$$

10) The resulting watermark bit stream w'_c of size P' is error corrected resulting in the watermark w' of size P.

11) The extracted binary image is acquired by reshaping the vector w' to a matrix of size $A \times B$. [2]

III. RESULTS

The binary images used as watermarks are shown in Table 2. We applied a 2D Wavelet disintegration using 4 resolution levels on the luminance component Y of every frame of the video.

TABLE II
BINARY IMAGES USED AS WATERMARKS

Code error	Red frames	Resolution
No	No	201 x 58
	K=4	110 x 31
	k=16	68 x 16
Cyclic	No	148 x 44
	K=4	88 x 28
	K=16	62 x 14

Every watermark bit of the binary image is extend over a number b of wavelet coefficients from the,LL, LH, HL and HH sub-bands of Wavelet disintegration level (see Fig. 2) using the secret key K known only by the owner of the video. The key K contains the size of the watermark (16 bits) and the seed used by the random binary number generator (64 bits).

We embedded the watermark with no temporal redundancy and with temporal redundancy in $k = 4$ and $k = 16$ frames. The error correction code used was a cyclic code (7, 4) with codeword length of 7 bits and data-word length of 4 bits. It is a simple code, can correct one error and is useful when the decoding Bit Error Rate (BER) is low (below 13, 58%).

First we have determined the objective intuitive quality of the watermarked videos using the quantization step size2, 4 and 8. The results are illustrated in Fig. 4, where PSNR is the mean Peak Signal to Noise Ratio of all frames of the video:

$$PSNR = \frac{\sum_{i=1}^{nr\_frames} PSNR(i)}{nr\_frames} \quad (9)$$

The resulting $PSNR$ has values between 39.6 and 49.2 dB and the watermarked videos appear visually identical to the original ones.

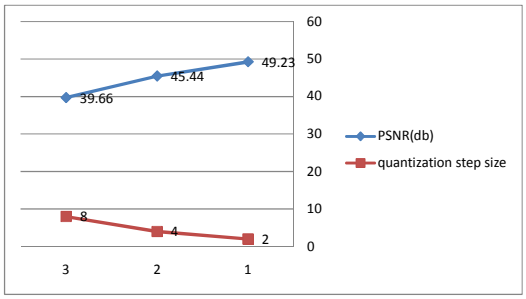

Fig. 4. Mean PSNR values of the watermarked videos

Another important property of the watermarking plan is the robustness. In order to evaluate this performance of the watermarking algorithm objectively, we have calculated the mean decoding BER for the watermarked videos after they were attacked. The decoding BER after every attack is illustrated in Fig. 5 and Fig. 6 for the quantization step size $q = 8$ and the cyclic (7, 4) error correction code.[2]

$$BER = \frac{1}{P}\sum_{j=1}^{P}\left|w_{out}(j) - w_{in}(j)\right| \quad (10)$$

In equation (11) w_{out} is the extracted watermark, w_{in} is the original watermark and P is the size of the watermark.

The following eight assaults were used to test the robustness of the watermarking plan:

- Blurring using blocks of 2x2 pixels
- Brightening by adding Y_0=5 to the luminance of every pixel
- Adding Gaussian noise of mean 0 and variance 0, 05%
- Median filtering using a 3x3 pixel local area
- Adding "salt and pepper" noise with density $d = 0{,}05\%$
- Frame averaging, where the current frame

$$f(i) = \frac{f(i-1) + f(i) + f(i+1)}{3} \quad (11)$$

- JPEG compression of every frame with quality factor $Q = 70$
- MPEG-2 compression at 4 and 2 Mbps

The experimental result illustrated in Fig. 5 and Fig. 6 shows that the watermarking plan is robust to almost all assault. Increasing the quantization step size q the resilience

of the plan against all assault is increase in quality, but the intuitive quality of the watermarked video is decreased.

For $q = 8$ the video watermarking method is immune to blurring, brightening, and addition of Gaussian and "saltandpepper" noise, frame averaging, JPEG compression and MPEG-2 compression at 4 Mbps. The examined plan has some detection problems after median filtering and MPEG-2 compression at 2 Mbps. Any video sequence may contain a large number of redundancies between the frames. So, the frame dropping attack is very common and effective on video watermarking. The watermark is embedded into the frames of a scene, and due to the large amount of redundancies between frames will not change significantly by frame dropping up to 60% of the highly correlated frames. The proposed method achieves better performance as compared to other methods.

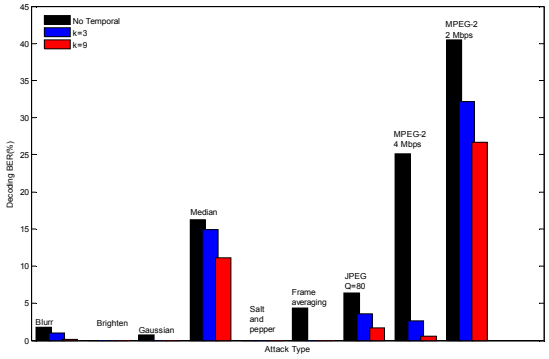

Fig 5. Decoding BER for all attack for q=8 using a cyclic error correction code (7, 4)

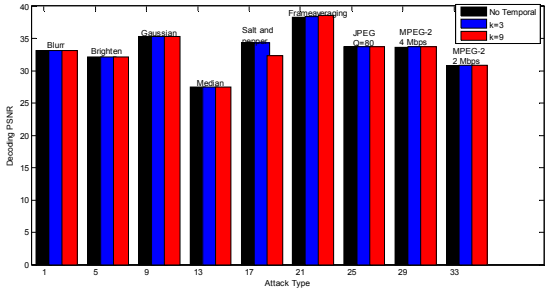

Fig 6. Decoding PSNR for all assault for q=8 using a cyclic error correction code (7, 4)

IV. CONCLUSION

In this paper, we introduced a simple and inexpensive watermarking method for inserting a watermark in the transform domain of an MPEG video.

We examined a video watermarking based on the quantization of the wavelet coefficients from the LL, LH, HL and HH sub-bands of the Wavelet disintegration level. We introduced a simple and computationally inexpensive watermarking methodology for inserting a watermark in the Discrete Wavelet transform domain of video.

The performance of the algorithm is increase in quality by using error correction codes and by redundantly inserting the same watermark in different frames of the video. The algorithm can be increased in quality for a better protection against the implemented types of assault.

REFERENCES

[1] Emad E. Abdullah · A. Ben Hamza Video watermarking using wavelet transform and tensor algebra, Springer-Verlag London Limited 2009,SIViP (2010) 4:233–245

[2] R.O Preda ,Nicolae D.Vizireanue. Quantization-based video watermarking in the wavelet domain with and temporal redundancy, international journal of electronics, vol, 98.march 2011, 393-405.

[3] J. J. O Rauanaaidh, W. J. Dowling, and F. M. Boland,Watermarking Digital Images for Copyright Protection," IEE Proceeding of Vision, Image, Signal Processing, Vol. 143, no. 4, pp.250-256, Aug., 199

[4] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-ofthe- art overview," *IEEE Signal Process. Magazine,* vol. 17, no. 5, pp. 20–46, Sep. 2000.

[5] Lian-Shan Liu, Ren-Hou Li, Qi GAO. "A robust video watermarking plan based on DCT," *In Proc. IEEE Conf. Machine Learning and Cybernetics,* China, Aug, 2005, vol. 8, pp. 5176- 5180.

[6] J. R. Hernandez, M. Amador, F. Perez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure," *IEEE Trans. Image Processing*, vol. 9, pp. 55-68, Jan. 2000.

[7] M.A. Suhail, M.S. Obaidat, "Digital Watermarking- Based DCT and JPEG Model," *IEEE Trans. Instrumentation & Measurement,* vol. 52, no. 5, pp. 1640-1647, Oct. 2003.

[8] Xiangui Kang, Jiwu Huang, Yun Q Shi, Yan Lin. "A DWT-DFT composite watermarking plan robust to both affine transform and JPEG compression," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 13, no. 8, pp.776-786, Aug. 2003.

[9] M. Tsai, C. Lin, J. Liu, "A wavelet-based watermarking plan using double wavelet tree energy modulation," in *Proc. 15th IEEE Int. Conf. Image Processing*, San Diego, USA, Oct. 2008, pp. 417–420.

[10] R. O. Preda, N. Vizireanu, C. C Oprea, R. M. Udrea, "Highly scalable image watermarking in the wavelet domain," *European Conf. Visual Perception,* Olanda, Aug. 2008, pp. 122.

[11] R. O. Preda, N. Vizireanu, "Blind Watermarking Capacity Analysis of MPEG2 Coded Video," in *Proc. Conf. Telecommunications in Modern Satellite, Cable and Broadcasting Services,* Serbia, Sept. 2007, pp. 465- 468.

[12] S. Biswas, S.R. Das, E.M. Petriu, "An adaptive compressed MPEG-2 video watermarking plan," *IEEE Trans. Instrumentation and Measurement,* vol. 54, no. 5, pp. 1853-1861, 2005.

[13] Zina Liu, Huaqing Liang, Xinxin Niu et al. "A Robust Video Watermarking in Motion Vectors," in *Proc. 7th Int. Conf. Signal Processing,* China, Sept. 2004, vol. 3, pp. 2358-2361.

[14] J. Zhang, A. Ho, G. Qiu, and P. Marziliano, "Robust video watermarking of H.264/AVC", *IEEE Trans. Circuits and System-II: Express Briefs,* vol. 54, pp. 205–209, Feb. 2007.

[15] Matsumoto, M. and Nishimura, T., "Mersenne Twister: A 623-Dimensionally Equidistributed Uniform Pseudorandom Number Generator", *ACM Trans. Modeling and Computer Simulation*, vol. 8, no. 1, pp. 3-30, 19

Email: afshinshy@yahoo.com

Afshin Shaabany was born in Marvdasht, Iran, in 1975. He received the Bs degree in Electrical Engineering from Tehran University, Tehran, Iran in 1999 and the Ms degree in Electrical Engineering from Polytechnic University, Tehran, Iran 2008. His research interests include IT, telecommunication, switching systems; Intelligent systems.

Email: fjamshidi59@yahoo.com

Fatemeh Jamshidi was born in Shiraz, Iran, in 1980. She received the Bs degree in Biomedical Engineering from the Jondi Shapthe University, Ahvaz, Iran in 2002 and the Ms and PhD degree in Electrical Engineering from Shiraz University and Tarbiat Modares University, respectively. Her research interests include switching systems; Intelligent systems, Robust control, IT, telecommunication