DWT-Based Watermarking Technique for Video Authentication

Farhan Alenizi, Fadi Kurdahi, Ahmed Eltawil
Center for Embedded and Cyber-Physical Systems
University of California, Irvine (UCI)
Irvine, California
falenizi@uci.edu, kurdahi@uci.edu, aeltawil@uci.edu

Abdullah Aljumah
College of Computer Engineering and Sciences
Prince Sattam bin Abdulaziz University
Alkharj, Saudi Arabia
Aljumah88@hotmail.com

***Abstract*—This paper proposes a wavelet watermarking scheme for video authentication. The discrete wavelet transform (DWT) has been used extensively in recent years in watermarking systems. It provides the necessary perceptual invisibility and robustness. In this paper, a DWT process is implemented using orthonormal filters, where the Y-components of the video frames are decomposed using DWT, and a watermark is inserted in one or more of the resulting subbands. Then, the watermarked video is reconstructed. The filters used for the DWT decompositions are randomly generated to increase the security of the algorithm. This scheme is integrated into the high efficiency video coding (HEVC) technique to examine the whole performance. The simulation results show that the proposed algorithm achieves well in terms of visual and metric tests. The average normalized correlation achieved is 85%, while the mean peak signal-to-noise ratio is 45 dB.**

Keywords—watermarking; filter banks; video coding.

I. INTRODUCTION

With the growth and advances in digital communication technologies, multimedia have become easy to be delivered and exchanged. These forms of digital information can be easily copied and distributed through digital media. These concerns motivated significant research in image and video watermarking fields [1]. Watermarking is used primarily for authentication and ownership protection. New progress in digital technologies, such as compression techniques, has brought new challenges to watermarking. On the other hand, High efficiency video coding (HEVC) or H.265 standard was introduced officially in 2013, it needs on average only half the bit rate of its predecessor, ITU-T H.264 | MPEG-4 Part 10 'Advanced Video Coding' (AVC), which was considered the most deployed video compression standard worldwide [2]. The new standard is designed to take into consideration advancing screen resolutions and is expected to be phased in as high-end products and services outgrow the limits of current network and display technology [2].

Various watermarking schemes that use different techniques have been proposed over the years [3-8]. To be effective, a watermark must be imperceptible within its host, easily extracted by the owner, and robust to intentional and unintentional distortions [6]. In specific, DWT has wide applications in the area of images and videos watermarking; this is because it has many characteristics and specifications that make the watermarking process robust. Some of these specifications are [4]: Space-frequency localization, Multi-resolution representation, Superior Human Visual system (HVS) modeling, and its adaptivity to the original image. A wavelet-based watermarking technique for ownership verification was presented by Y. Wang [9]. It uses orthonormal filter banks that are generated randomly to decompose the host image and embed the watermark in it.

In this paper, our target is to develop a watermarking technique using discrete wavelet decompositions, and integrate it into the high efficiency video coding (HEVC) process. The technique will be used for data hiding in encoded videos to meet the requirements of imperceptibility, robustness, storage requirements, security, and complexity.

II. PROPOSED WATERMARKING TECHNIQUE

In this section, we introduce our digital video watermarking technique for the purpose of authentication. The proposed technique is aimed at achieving robustness, imperceptibility and security. The hiding technique consists of two stages: the first stage is the decomposition process and the second stage is the hiding process. The watermark can be a logo image of size $n \times m$ pixels. The encoded videos are primarily in the YUV color space. The watermarking process can take place in any of the three components Y, U or V. The proposed algorithm will use the luminance Y frames as host images for the wavelet watermarking process; that is, the watermark will be inserted or distributed in one or more of the subbands that result from the wavelet decomposition process. A method for wavelet image watermarking is proposed in [9]. It uses finite impulse response (FIR), real-coefficients, randomly generated orthonormal filter banks. The watermark itself is processed and added to the coefficients of one or more of the higher subbands; then, the watermarked image will be reconstructed. This watermarking process is blind one; in other words, the original watermark is not required for the extraction process.

The orthonormal analysis and synthesis filters can be constructed in such a way that they have large sidelobes. This makes it possible to embed more watermarks' portions in the medium bands to avoid the effect of the different images processing techniques. These filter banks can be generated randomly depending on the generating polynomials; hence, by generating random numbers for the polynomial coefficients, it's possible to build multiple filter banks that are used for the DWT decomposition and reconstruction processes.

Depending on the number of the decomposition levels, each filter bank can be used for one level of DWT decomposition and reconstruction; furthermore, we will have full control on both the structure and the number of levels of the decomposition process for security reasons. The bands in the middle frequencies will be used for hiding in general; this in turn would avoid the use of the lower frequency bands, where most of the energy is in, and the higher frequency bands which are susceptible to compression and other image processing attacks. The watermark might be distributed in many subbands. This scenario is helpful in counteracting the Non-linear Collusion Attack.

A method to embed the watermark using pseudo-random sequence is proposed in [10]; this method establishes the watermarking embedding process by converting the watermark image to a binary sequence (*S*) of length *M* where the data pixels are valued as +1 and the background pixels are valued as -1. Moreover, a pseudo-random sequence (*P*) that has the same length *M* as the watermark sequence is generated using a secret key and, similarly, represented as binary bits that are valued either +1 or -1. One way to generate robust random keys for both the random sequence and the filter banks of the DWT process is to use the physical unclonable functions (PUF's) [11]; where these functions can generate volatile secret keys for cryptographic operations. The DWT coefficients of the subbands that are used for the embedding process are represented as a vector *T* of length *M*. The watermark is embedded into the vector *T*, to obtain a new vector *T′* according to the following rule:

$$t_i' = t_i + \propto . p_i . s_i \ , \ i=1, 2 .... M. \quad (1)$$

Where α is a magnitude factor which is a weighting constant that controls the strength of the processed watermark. The value is selected to offer a trade-off between robustness and unobtrusiveness [10]. Furthermore, choosing the weighting factor should take into account many issues such as the compression ratio, the smoothness of the image, and the detection process. One way to get the magnitude factor is to compare the original coefficients of the host DWT subband and that of the enhanced watermark image *Q* where *Q*=*S***P*, according to this rule [9]:

$$\propto = \frac{\frac{Max(T)}{Max(Q)}}{2} + \frac{\frac{Norm(T)}{Norm(Q)}}{2} \quad (2)$$

Where *Max(T)* denotes the maximum value of the vector *T*, while *Norm(T)* denotes the Norm of vector *T*.

The extraction process is the reverse of the hiding process. The original watermark image is not required, but still, the knowledge of the synthesis filter banks and the pseudorandom sequence is required. To extract the watermark, a prediction of the original value of the pixels is needed [10]. The watermarked image may be considered to be the original image that is disturbed by the pseudorandom noise. A noise-elimination technique can be used to determine the original pixels; to achieve that, a spatial convolution mask of size 5x5 can be used to smoothen the extracted coefficients. Experimental results showed that the 5x5 mask gave superior performance compared to the 3x3 mask in terms of the normalized correlation under different circumstances such as noise addition and compression processes. The overall watermarking process for a Y-frame is shown in Fig. 1.

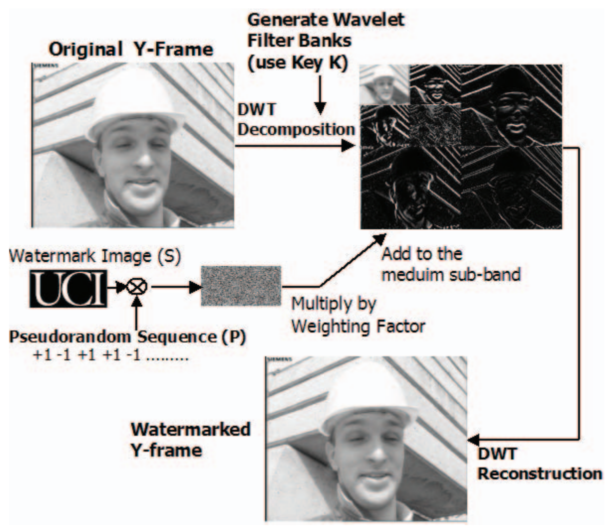

Fig.1. The block diagram of the proposed watermarking method.

The watermark, which is primarily a binary image, could be embedded in any frames of the host video; the frames may be chosen selectively in such a way that is fully controlled by the owner. However, the I-frames of the HEVC process are preferred for watermarking; the dominant intraprediction process maintains more energy in the coefficients. On the other hand, The Y components were selected because they provide higher resolution and hence higher watermarking capacity, but this shouldn't eliminate the fact that the U and V components could be used. Fig. 2 shows the proposed watermarking technique when the HEVC process is applied.

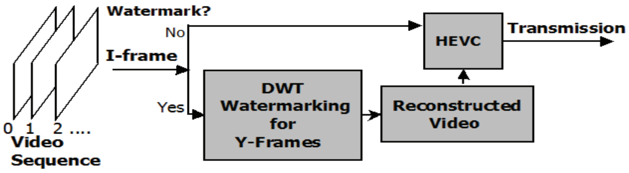

Fig. 2. The block diagram of the watermarking process with the application of HEVC process.

III. EXPERIMENTAL RESULTS

In this section we demonstrate the performance of our algorithm using our proposed method on different standard videos with and without HEVC process, and compare it with method of [12]. Unwatermarked and Watermarked images of the first frame of football video without applying HEVC are shown in Fig. 3. The embedded and extracted watermarks of size 9x11 are shown in Fig. 4.

(a) (b)

Fig. 3. The first frame of: (a) original Football video, (b) reconstructed watermarked Football video.

(a) (b)

Fig.4. (a) Original watermark, (b) Recovered watermark.

Our algorithm performance will be evaluated in terms of peak signal-to-noise-ratio (PSNR) between the original and the watermarked videos, and the normalized correlation (NC) between the original and the extracted watermarks for the standard videos: Foreman, Akiyo, Football, BasketballDrill and BasketballDrive. In these tests, 100 frames were watermarked. Fig. 5 shows the normalized correlation (NC) of the extraction process; moreover, Fig.6 shows the PSNR's of the reconstructed frames.

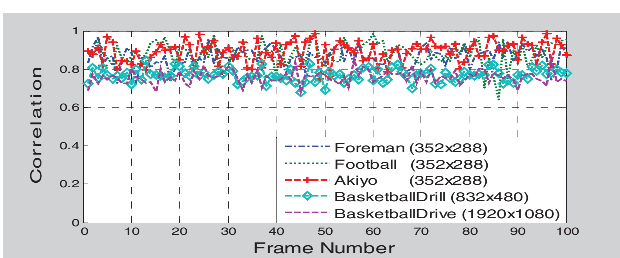

Fig. 5. Normalized Correlation of the proposed watermarking process.

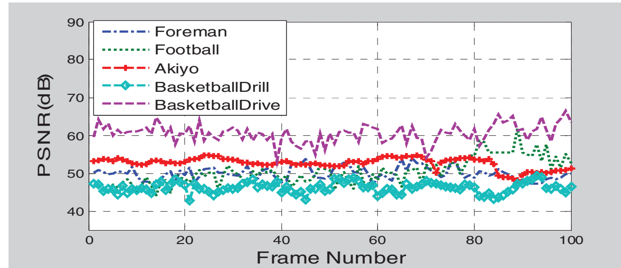

Fig. 6. PSNR of the test videos after the watermarking process.

Method of [12] gives maximum PSNR of 37 dB for the Football video, while our method gives an average of 44 dB. TABLE I shows the PSNR for the proposed watermarking method and the watermarking method of [12]; moreover, TABLE II shows the performance in terms of average NC for the Football video stream using the proposed method and the method in [12].

TABLE I. PSNR's OF PROPOSED METHOD AND METHOD OF [12]

Video Sequence	Number of Frames	Proposed method	Method Of [12]
		PSNR	PSNR
Football	20	44.37	28.53
	40	44.69	30.51
	60	44.78	34.09
	80	45.03	26.24
	100	45.35	29.66

TABLE II. NORMALIZED CORRELATION OF PROPOSED METHOD AND METHOD OF [12]

Video sequence	Proposed method	Method of [12]
	NC	*NC*
Football	0.85	0.728

The proposed scheme was tested under some common video processing attacks, such as salt-and-pepper noise and Gaussian noise. 100 frames of the test videos were subjected to salt-and-pepper noise with 0.01 density value, and to white Gaussian noise with zero mean and 0.01 variance. Fig. 7 and Fig. 8 respectively show the correlation performance under these attacks. The two figures show that the technique was robust against these types of attacks.

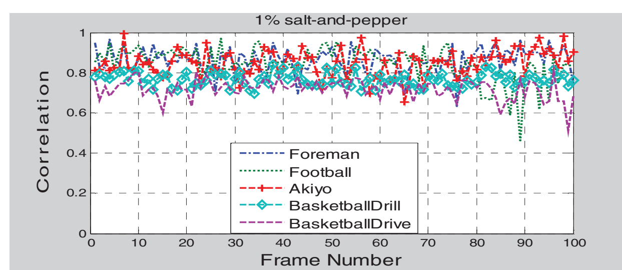

Fig. 7. Normalized correlation of the proposed method with the application of 1% salt-and-pepper noise.

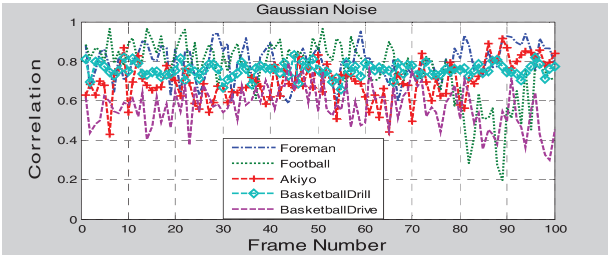

Fig. 8. Normalized correlation of the proposed method with the application of Gaussian noise with zero mean and 0.01 variance.

The algorithm was tested with the application of HEVC. 100 frames of the watermarked video streams were subjected to HEVC process at a quantization parameter (QP) of 20. This quantization factor value is typical one and would result in different compression ratios depending on the input video. The PSNR's are shown in Fig.9 and the NC's at the watermarked frames are shown in Fig. 10.

The videos with more details and motions such as Football and Forman have higher correlation values; on the other hand, the videos with smoother nature and fewer motions such as in the case of Akiyo have lower correlation values. This can be attributed to the fact that the DWT coefficients of the videos in the first case have higher energy and hence the magnitude factor would be greater according to (2). Increasing the magnitude factor for certain smooth videos over a certain limit can cause undesired artifacts. On the other hand, higher compression ratios result in smoother videos due to the use of the deblocking and smoothing filters; this can give more flexibility to increase the magnitude factor over the normal limits since the artifacts could be eliminated.

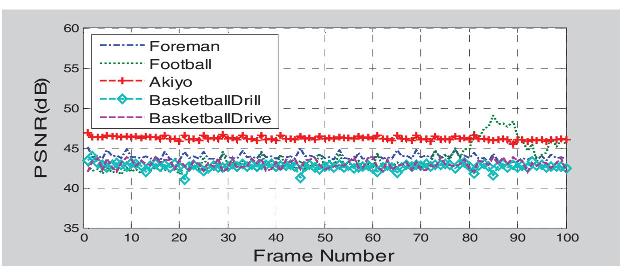

Fig. 9. PSNR of the proposed watermarking method when HEVC process is applied.

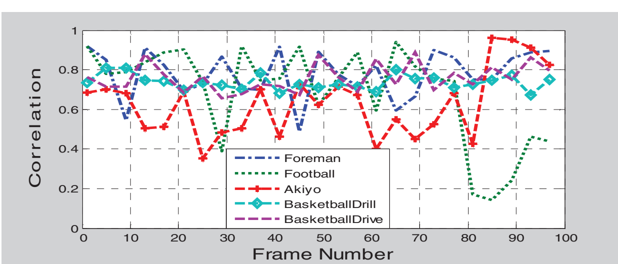

Fig. 10. Normalized correlation of the proposed watermarking method when HEVC process is applied.

IV. CONCLUSIONS AND FUTURE WORK

This paper proposes a DWT-based watermarking process using randomly generated orthonormal filter banks. It can be shown that the proposed technique performs well with and without HEVC. The compression ratio that was used is typical; however, the results under higher compression ratios were encouraging; further investigation of the efficacy of the watermarking process under aggressive HEVC compression is left to future work. Furthermore, it's obvious that the technique performs well under common attacks such as salt-and-pepper noise and Gaussian noise. The performance is better when the videos have more motions. However, Football video gives lower performance in terms of correlation in the blurred frames of the video; these frames, in fact, are a result of fast camera panning process; hence, no significant details are there; this in turn would result in lower energy in the wavelet coefficients, so that the hiding process is not optimal in this case. This, however, can be solved by the avoidance of hiding the watermarks in some portions of the video to be watermarked. Future work will investigate the performance under other common video processing attacks.

REFERENCES

[1] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Processing Magazine,* vol. 17, pp. 20 – 46, Sept. 2000.

[2] *High efficiency video coding*, ITU-T Rec. H.265, ISO/IEC 23008-2, Apr. 2013.

[3] Jantana Panyavaraporn, "Multiple video watermarking algorithm based on wavelet transform," in *Proc. IEEE ISCIT*, pp. 397-401, Sep 2013.

[4] P. Meerwald and A. Uhl, , "A survey of wavelet-domain watermarking algorithms," in *Proc. SPIE*, vol. 4314, pp. 505-516, 2001.

[5] L. Mong-Shu, "image compression and watermarking by wavelet localization," *Intern. J. Computer Math.,* vol. 80(4), pp. 401-412, 2003.

[6] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," in *Proc. IEEE ICASSP*, vol. 5, pp. 2969 – 2972, May 1998.

[7] V. H. Guzman, M. N. Miyatake, and H. M. P. Meana, "Analysis of a wavelet-based watermarking algorithm," in *Proc. IEEE CONIELECOMP,* pp. 283-287, 2004.

[8] S-H. Wang and Y-P. Lin, "Wavelet tree quantization for copyright protection watermarking," *IEEE Transactions on Image Processing*, vol. 13, pp. 154 – 165, Feb. 2004.

[9] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Trans. Image Processing*, vol. 11, pp. 77-88, 2002.

[10] Jantana Panyavarapom, "Wavelet based video watermarking scheme for H.264/AVC, " in *proc. ISPACS*, pp.1-5, Dec. 2011.

[11] G. Edward Suh, " Physical unclonable functions for device authentication and secret key generation," in *Proc. DAC'07*, pp. 9-14, 2007.

[12] M. Sundararajan, G.Yamuna, "DWT based scheme for video watermarking," in *Proc. ICCSP*, pp. 460-466, 3-5 Apr. 2013.