International Journal of Research in Advent Technology, Vol.3, No.12, December 2015
E-ISSN: 2321-9637
Available online at www.ijrat.org

Efficient Signature Embedding in Video for High Security

Sushmita B. Kashyap [1], Nitin Jain [2]
M-Tech Scholar, Electronic and Telecommunication, Chouksey Engineering college, Chhattisgarh, India [1].
Asst. Professor, Electronic and Telecommunication, Chouksey Engineering college , Chhattisgarh, India [2]
Email: sushmita.kashyap85@gmail.com[1] *, ernitin-jain@rediffmail.com*[2]

Abstract- With increase in growth of internet, users of networks are increasing rapidly. Digital product owners are concerned about illegal repetition of their products. Security and copyright protection are becoming important issues in multimedia applications and services. Methods are needed to protect copyright of the owner and prevent illegal copying. Several intentional attacks are undergone by video, like frame dropping, averaging, cropping and median filtering and inadvertent attacks like addition of noise and compression which can compromise the owner information thereby denying authentication. In this paper, a robust Discrete Wavelet Transform (DWT) has been adopted for the authentication of digital video, which embeds different parts of a single watermark into different scenes of a video. The proposed method has been compared with an existing DWT based watermarking method and is found to exhibit better strength.

Index Terms- Discrete Wavelet Transform (DWT), Video Processing, Digital Watermarking, Video Security, Encryption.

1. INTRODUCTION

Video is three-dimensional array of colored pixels. Two dimensions serve as spatial (horizontal and vertical) directions of the stirring pictures, and one dimension represents the time domain [1]. Digital video offers a number of advantages over analog video, including the ease of sharing and storing, no degradation of data quality when replicated, easy and inexpensive repetition and the ability for multicasting. The use of digital multimedia content is increased large amount of data is transferred and distributed easily. This development will benefit multimedia product owners as sales will increase. Also, it will pose test to their ownership as most of multimedia products are distributed in insecure format. These products can be transmitted and redistributed easily without any authentication as various tools are available at no cost. So there is need for patent protection of multimedia data. Video become an important tool for the educational industry and entertainment industry [2]. Digital video watermarking is new technology used for copyright protection of digital media. [3] It inserts the authentication information in multimedia data which can be used as proof of ownership. Progress in technology has set multimedia users the skill to tamper with, produce copies of, and illegally redistribute digital content. The fastest growing internet can facilitate piracy on a large scale, with users distributing illegal copies via peer-to-peer file distribution. The owner of the digital content, desires to make sure that all access to the information is official under the rules of a license (conditional access), unlawful reproductions cannot be simply made (duplicate protection), and any illicit copies that are created can be identified and found (authentication and content detection). Without rectifying these security issues, digital multimedia products and services cannot take-off in an eCommerce setting [4]. An ideal solution to this problem would be to somehow integrate the security information directly into the content of the multimedia document such that the security information should be inseparable from the document during its constructive lifespan. Also, the additional information should be perceptually invisible as the multimedia papers are finally processed by human spectators or listeners and the contents should not be unnatural. Finally is the flexibility of the scheme. As the manuscript might undergo duplication, it should be able to hold identification of diverse copies of the document. Some of the techniques that can offer this ideal solution and that might be used in this situation are steganography, data embedding, watermarking and data hiding. The main difference between watermarking and steganography is steganograpic methods rely on reality that covert message is a point to point communication between legal parties alone and that is strange to third parties. Thus, steganography methods are naturally not designed to be strong against attempted attacks. In watermarking technique the existence of the embedded data is unknown to illegal parties who have access to the information, and can try unlawful attacks. There exists a composite trade-off between the three parameters in digital video watermarking, robustness, data payload and fidelity. The data payload is the amount of information, i.e. the number of bits that is encoded by the watermark. The fidelity is another property of the watermark: the

distortion that the watermarking process is bound to introduce, should remain imperceptible to a human observer. Finally, the robustness of a watermarking scheme can be seen as the ability of the detector to extract the hidden watermark from some altered watermarked data. The robustness are often evaluated via the survival of the watermark after attacks. These three parameters are conflicting and a tradeoff has to be found, which is often tied to the targeted application.

1.1. *Video Watermarking*

Maximum occurrences of copyright violation and distribution happen for video media content. So Video Watermarking is one of the most accepted techniques between the various Watermarking techniques currently in use. Requirements for video Watermarking are as follows:

(1) Video data are subject to increased attacks than any other media.
(2) Video content is sensitive to distortions and Watermarking may degrade the quality.
(3) Video compression algorithms are computationally rigorous.
(4) Video requires large bandwidth that is why it is mostly carried in compressed domain. So Watermarking algorithms also adaptable for compress area processing.

2. IMPLEMENTATION SCHEME

DWT (Discrete Wavelet Transform) is used in a wide selection of signal processing applications. 2-D DWT (discrete wavelet transforms) decomposes an image or a video frame into sub-images, 3 details and 1 approximation. The 2-D DWT is an relevance of the 1-D DWT in both the horizontal and the vertical components. DWT split the frequency band of an image into a lower resolution approximation sub-band (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail coefficients. A Watermark is set in low frequencies obtained by Wavelet decomposition which increases the toughness. So that resulting watermark video turn to be susceptible to different attacks that have low pass character like filtering, geometric distortions and lossy compression.

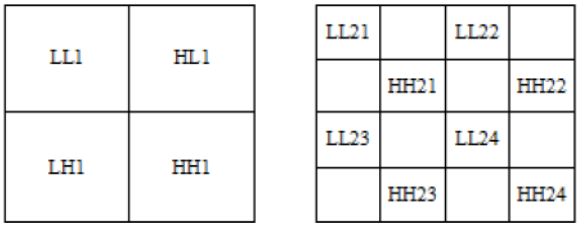

Fig.1: DWT sub-bands in (a) level 1, (b) level 2.

2.1. *Watermark Embedding Process*

The Video preprocessing stage includes 3 parts: frame extraction, application of DWT and image change detection. The video stream of the input in the form of frames is extracted such that the watermarks can be embedded into the video channel. The audio channel in the video is left intact. All frames are transformed to wavelet domain with four levels. DWT transform a signal into coarse and detail signals by "averaging and differencing" on the coefficients. It breaks the signal into a coarse value (DC component) and a hierarchy of detail value (AC components). DWT is chosen as it is more computationally more efficient than other transform methods. The speed is faster than DFT and DCT as sum or difference of the pixel only have to be calculated. Using DWT, one can achieve both spatial and frequency localization, robustness to noise, perceptual invisibility and robustness to compression, image processing techniques, and median filter (which can be considered as a case of pixel permutation), resistance to geometric transforms (lots of existing algorithms do not survive) and resilience to counterfeit attempts. The scheme is robust against format conversions because the watermark is inserted before compression. Otherwise the authentication information will be lost if the video file is converted to a different compression standard. The Watermark embedding process consists of the following steps:

(1) The video is divided into frames RGB frames are converted to YUV frames.

(2) 2-DWT is applied on it.

(3) The RGB watermark image is converted into a vector P= {p1, p2… p_{NxM}}.

(4) This vector P is again divided into n parts. Then each part is embedded into each of the corresponding LL and HH sub bands. The watermark pixels are embedded with strength x into the maximum coefficient Mi of each PC block Yi. The embedding equation is:

$$M_i = M_i + xW \quad \ldots(1)$$

(5) Where, x is the watermark embedding strength.

(6) Inverse DWT is applied to obtain the watermarked luminance component of the frame. Finally watermarked frame is reconstructed and watermarked video is obtained.

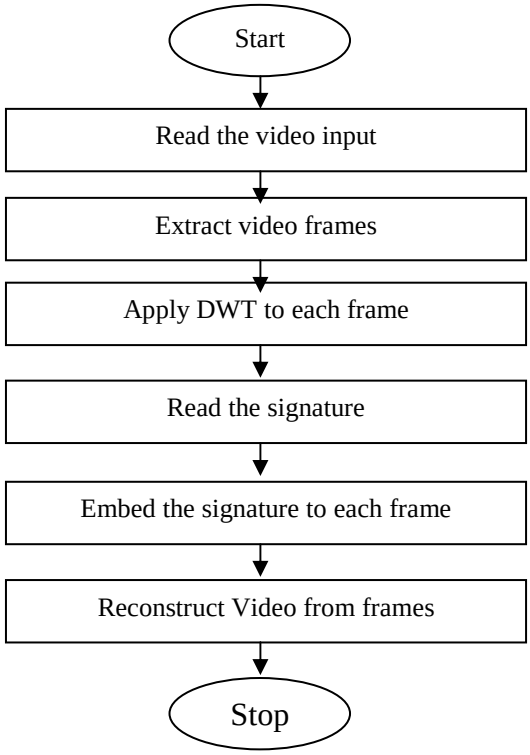

Fig.2: Video Signature Embedding Process.

Fig.3: Original Frame.

Fig.4: Signature Image.

Fig.5: Watermarked Frame.

Fig.6: Original Frame.

3. RESULTS AND DISCUSSION

Above algorithm is applied to the sample video sequence using the colored watermark logo. The watermarked frame and its corresponding original sampled frame are shown in Fig.3, Fig.4, and Fig.5. Watermarked frame emerge visually matching to the original. The performance of proposed algorithm can be measured in terms of its PSNR (Peak Signal to Noise Ratio), MSE (Mean Squared Error), AD (Average Difference) and MD (Maximum differences) which are used as a general measure of the visual quality of the watermarking system.

PSNR: The Peak-Signal-To-Noise Ratio (PSNR) is used to measure the deviation of the watermarked and attacked frames from the original video frames and is defined as:

$$PSNR = 10\log_{10}(255^2/MSE) \quad \text{.....(4)}$$

Where MSE (mean squared error) between the original and distorted frames (size m x n) is defined as:

$$MSE = (1/mn)\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - I'(i,j)] \quad \text{....(5)}$$

Where I and I′ are the pixel values at location (i, j) of the original and the distorted frame respectively. Higher values of PSNR indicate more imperceptibility of watermarking. It is expressed in decibels (dB).

Fig.7: SignatureImage.

Fig.8: Watermarked Frame.

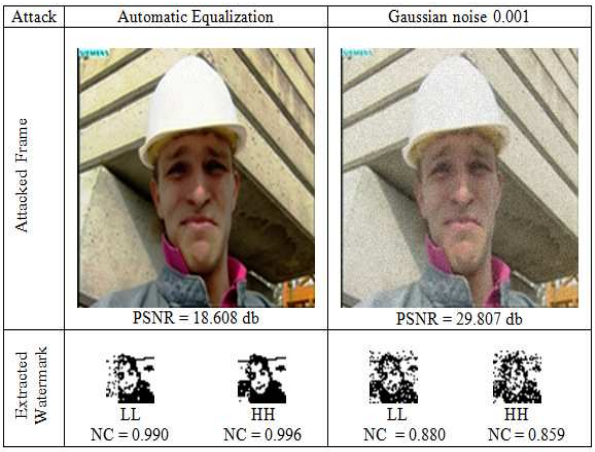

Fig.9: Automatic equalization and adding Gaussian noise attack.

Table-1: Performance Analysis of Video Frames without any Attack

	Image Rotation	PSNR	MSE	AD	MD
Video1	0^o	39.9356	0.0182	0.0167	0.8783
	45^o	29.7721	0.1345	0.1424	0.6161
Video2	0^o	39.0356	0.0201	0.0213	0.2946
	45^o	30.1760	0.0201	0.0213	0.3029

Table-2: PSNR Comparison of Video Frames with Previous Results.

Attack	PSNR (db)	
	Sanjana Sinha et al.	Proposed Method
GAUSSIAN NOISE	31.1564	33.6862
SALT & PEPPER NOISE	24.4592	22.9248
ROTATION	28.8256	28.4862
MEDIAN FILTERING	39.1676	39.6547
CONTRAST ADJUSTMENT	32.4420	33.4582
AUTOMATIC EQUALIZATION	46.4597	29.8072

4. CONCLUSIONS

Here execution of digital video watermarking scheme based upon DWT is shown. Due to its multi resolution characteristics, DWT scheme is robust against various attacks. The Software used to develop the proposed system is MATLAB, version R2012a. There is no noticeable difference between the watermarked video frames and the original frames. As shown in above table the difference is the video frames are not so high and consequently the performance of the developed method is superior and as a future work this method can be implemented on various videos which can be used to prove the performance of the system.

REFERENCES

[1] K. Su. (2001): Digital Video Watermarking Principles for Resistance to Collusion and Interpolation Attacks. Master of Applied Science thesis, University of Toronto.

[2] Hanane H. Mirza, Hien D. Thai, Yasunori Nagata and Zensho Nakao. (2011): Digital Video Watermarking Based on Principal Component Analysis. Department of Electrical and Electronics Engineering, University of the Ryukyus Okinawa.

[3] Nisreen I. Yassin, Nancy M. Salem, and Mohamed I. El Adawy. (2012): Block Based Video Watermarking Scheme Using Wavelet Transform and Principle Component Analysis. International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3.

[4] F. Deguillaume, G. Csurka, J. Ruanaidh, and T. Pun. (1999): Robust 3D DFT video watermarking. Proceedings Electronic Imaging.

Security and Watermarking of Multimedia Contents, Vol. 3657.

[5] Sanjana Sinha, Prajnat Bardhan, Swarnali Pramanick, Ankul Jagatramka, Dipak K. Kole, Aruna Chakraborty. (2011): Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis. International Journal of Wisdom Based Computing, Vol. 1 (2).

[6] Snehal V. Patel, Prof. Arvind R. Yadav. (2011): Invisible Digital Video Watermarking Using 4-level DWT. National Conference on Recent Trends in Engineering & Technology.

[7] Kesavan Gopal, Dr. M. Madhavi Latha. (2010): Watermarking of Digital Video Stream for Source Authentication. International Journal of Computer Science Issues,Vol. 7,Issue 4, No 1.

[8] Keshav S Rawat, Dheerendra S Tomar. (2002): Digital watermarking schemes for authorization against copying or piracy of color images. Indian Journal of Computer Science and Engineering Vol. 1 No. 4 295-300.

[9] Yavuz E., Telatar Z. (2007): Digital Watermarking with PCA Based Reference Images, ACIVS 2007, Springer-Verlag Lecture Notes in Computer Science, 4678, pp.1014- 1023.

[10] Saraju P. Mohanty, Renuka Kumara C, and Sridhara Nayak. (2004): FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder" CIT 2004, LNCS 3356, pp. 344–353.

[11] C. Serdean, M. Ambroze, M. Tomlinson, and G. Wade. (2002): "Combating geometrical attacks in a dwt based blind video watermarking system. Proceedings Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIProm Com, pp. 263- 266.

[12] C. Lu and M. Liao. (2001): Video object-based watermarking: a rotation and flipping resilient scheme. Proceedings 2001 International Conference on Image Processing, Vol. 2, pp.483-486.

[13] Sanjana Sinha, Prajnat Bardhan, Swarnali Pramanick, Ankul Jagatramka, Dipak K. Kole, Aruna Chakraborty. (2011): Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis, International Journal of Wisdom Based Computing, Vol. 1, Issue 2 pp.7-12.

[14] B. Mobasseri. (1998): Direct sequence watermarking of digital video using m-frames. Proceedings International Conference on Image Processing (ICIP-98), Vol. 3, pp. 399- 403.