Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Encrypted Key Mechanism Based Enhanced Video Cryptography

Pawanpuneet Mander
M.Tech(E-Security)
Baba Banda Singh Bahadur Engineering College,India

Balpreet Kaur
Assistant Professor(Computer Science)
Baba Banda Singh Bahadur Engineering College,India

Abstract— With the advent of technology, authors of digital media can easily distribute their works by making them available on web pages or other public forums. This requires a secure way to transmit information. This paper gives a digital video watermarking technique based on sharp edge point detection algorithm and an encrypted key concept for authorization. An experiment result shows that the proposed method is robust in visual quality measured in terms of BER, MSE and PSNR.

Keywords— Digital watermarking, Sharp point detection, Encoding, Decoding, Copyright protection

I. INTRODUCTION

A watermark is a visible embedded overlay on a digital photo consisting of text, a logo or a copyright notice. The purpose of watermark is to identify the work and discourage its unauthorized use. Though a visible watermark cannot prevent unauthorized use, it makes it more difficult for those who may want to claim someone else's photo or art work as their own [18]. Another type of watermark is the digital watermark pioneered by Digimarc Corporation. Digimarc offers a service for embedding digital code into photos and other media that is undetectable during normal use, but enables tracking and identification of the media [24]. A large number of watermarking schemes have been proposed to hide copyright marks and other information in digital images, video, audio and other multimedia objects. Typically the watermark contains information about the origin, ownership, destination, copy control, transaction etc [2][8]. Digital video is a type of digital recording system that works by using a digital rather than an analog video signal. Digital video comprises a series of orthogonal bitmap digital images displayed in rapid succession at a constant rate. In the context of video these images are called frames [4]. Video watermarking is different from image watermarking because additional data is available here that allows information to be more redundantly and reliably embedded [6].

II. COMPONENTS OF WATERMARKING

Video watermarking involves embedding cryptographic information derived from frames of digital video into the video itself. Ideally, a user viewing the video cannot see a difference between the original, watermarked video and unmarked video, but a watermark extraction mechanism can read the watermark and get the embedded information [10].
This watermarking algorithm optimizes for three separate factors:

I. **Robustness** : the ability of the watermark to resist attempts by an attacker to destroy it by modifying the size, rotation, quality or other visual aspects of the video [11].
II. **Security** : the ability of the watermark to resist attempts by a sophisticated attacker to remove it or destroy it via cryptanalysis, without modifying the video itself [3].
III. **Perceptual fidelity** : the perceived visual quality of the marked video compared to the original, unmarked video.

III. TECHNIQUES OF WATERMARKING

A. Principal Component Analysis (Watermarking)

In this method, the watermark is embedded into all the video frames by the decomposition of the frames into DWT sub-bands in accordance with the mechanism of block based PCA on the sub block of the low frequency sub-band. The watermark is embedded into the principal components of the sub-blocks [5][23].

B. Singular Value Decomposition

SVD is used for factorization of a real or complex matrix. SVD of an image M with dimensions m x m is given by: M=USVT where S is a singular matrix of matrix M, U and V are orthogonal matrices. The columns of U, called left singular vector represents the horizontal details and the columns of V, called right singular vector represents the vertical details of the original image [16][19].

C. Discrete Cosine Transform

It is one of the most common linear transformations in digital signal process technology. The 2D-DCT does not only concentrate the important information of original image into the smallest low frequency coefficient, but also it can show the image blocking effect being the smallest, which can realize the good compromise between the information centralizing and the computing complication [1][17][21].

IV. APPLICATIONS OF WATERMARKING

I. *Fingerprinting*

In this technique, the video identified the fingerprint by a software that extract and then compresses various components of a video. Several features that are involved in video fingerprinting analysis are key frame analysis, colour changes, motion changes etc of a video frame. In this technique, watermarks are embedded as fingerprints in the video.

II. *Copy Control*

In this technique, a watermark is used to indicate whether a video content is copyrighted. The watermark used can only be removed with a severe degradation of video sequence by attacks.

III. *Broadcast Monitoring*

In broadcast monitoring, the owner of the content embeds the watermark before transmission. The watermark can only be extracted by the monitoring site that is used within the transmission area.

IV. *Video Authentication*

Through video authentication, the images and the videos are checked for their integrity. The generally used policies are fragile, semi fragile and robust watermarking. The technique is robust to content-preserving manipulations and it is sensitive to content-changing manipulations [7].

V. *Copyright Protection*

This technique is an important topic of discussion in digital video delivery networks. There are several techniques of video watermarking for copyright protection. In one of the technique, a watermark is added to the video signal that contains information about sender and receiver of the delivered video [13].

V. SHARP EDGE POINT DETECTION

This algorithm relies on a central principle: at a corner, the image intensity will change largely in multiple directions. This can alternatively be formulated by examining the changes of intensity due to shifts in a local window. Around a corner point, the image intensity will change greatly when the window is shifted in an arbitrary direction. Now a second moment matrix will be generated on the basis of corner decisions. The matrix A, has also been called the autocorrelation matrix and has values closely related to the derivatives of image intensity.

$$A(\mathbf{x}) = \sum_{p,q} w(p,q) \begin{bmatrix} I_x^2(\mathbf{x}) & I_x I_y(\mathbf{x}) \\ I_x I_y(\mathbf{x}) & I_y^2(\mathbf{x}) \end{bmatrix}$$

where $I_x$and $I_y$are the respective derivatives (of pixel intensity) in the $x$and $y$direction at point $\mathbf{x}$and $p$and $q$are the values of the weighting function. The off-diagonal entries are the product of $I_x$and I_y, while the diagonal entries are squares of the respective derivatives. The weighting function $w(x,y)$can be uniform, but is more typically an isotropic, circular Gaussian,

$$w(x,y) = g(x,y,\sigma) = \frac{1}{2\pi\sigma^2} e^{\left(-\frac{x^2+y^2}{2\sigma^2}\right)}$$

that acts to average in a local region while weighting those values near the center more heavily. As it turns out, this A matrix describes the shape of the autocorrelation measure as due to shifts in window location. Thus, if we let $\lambda_1$and λ_2 be the eigenvalues of A, then these values will provide a quantitative description of how the autocorrelation measure changes in space: its principal curvatures. Then a threshold is set and according to its value points are selected and rejected.

Features of sharp edge detection

a. It uniquely identifies the author of copyrighted work.

b. It is easy to embed the watermark.

c. It results in the video that contain a hidden encrypted key and a watermark of high visual quality.

VI. RELATED WORK

The two watermarking techniques are proposed [13] and compared for compressed and uncompressed video to show the possibilities and weaknesses in the schemes working in the frequency and spatial domain for colour video sequences. The algorithm embeds data in HL and LH bands by using motion estimation approach and random Gaussian distribution in video sequences. The experimental results show that the performance parameters (quality measure and similarity) in frequency domain especially the similarity measure before and after different attacks(frame dropping, adaptive quantization, frame filtering) is very close to each other in comparison to the spatial domain.

An FPGA based implementation of an invisible watermark encoder is proposed [20]. This is robust and secure watermarking system for authentication of video. For implementation, discrete wavelet transform (DWT) and principal component analysis (PCA) is used. The 2-level DWT is applied on video frames and split them into sub-bands. Divide each sub-band with N/2 X N/2 dimension into n x n non-overlapping parts then apply PCA to each part. The results of the embedding and extraction process shows watermarking video frames having PSNR 46.06 db and Normalize Coefficient of 0.5.

In this proposed watermarking method [21] , the original image is rearranged using zigzag sequence and DWT is applied to it. Then DCT and SVD are applied on all high bands LH, HL, HH that gives more robust mechanism against different kinds of filtering noises and geometric noises. A robust and blind watermarking method is proposed [22] based on edge insertion. The wavelet transform used that change the coefficients of the HH band by adding edges. The robustness of this technique was evaluated by attacking the watermarked image with filtering, addition of Gaussian noise and salt-pepper, JPEG compression, GIF colour reducing and rotation and results were evaluated on basis of BER. The calculated value of PSNR is 26 db.

In the proposed technique [26], first a survey is performed on available video watermarking techniques, feasibility study on watermarking techniques meeting application specific criteria for H.264/AVC then the comparative analysis is performed based on robustness and computational complexity of different watermarking algorithms.

VII. PROBLEM FORMULATION

A. The survey has shown that in existing techniques the watermark is showing effects on video frames that make its properties changed and quality degraded. The systems that works in frequency domain will change the frequency of video frames and these video frames are used for watermarking.

B. The proposed system is based on Sharp Edge Point Detection algorithm. Edge detection is the name for a set of mathematical methods which aim at identifying points in a digital image at which the image brightness changes sharply or, more formally, has discontinuities. The points at which image brightness changes sharply are typically organized into a set of curved line segments termed edges. In this proposed work an algorithm is developed which will give the points on basis of sharp point detection algorithm and the watermark is placed on that detected points in the video frames so that it cannot be detected easily by unauthorized users. A security key is inserted which is embedded inside the video and is useful to hide secret information, as it cannot be detected by anyone without been authorized to the video.

VIII. PROCESS OF WATERMARKING

The watermarking system is divided into two sections: encoding process in which watermark is embedded into the video and decoding process is used to extract the watermark from video.

Encode

1) Fetch a video for watermarking and security key hiding.
2) Divide the video onto equal frames.
3) Detect the required points for embedding watermark on the basis of sharp point algorithm.
4) Take an image which is to be embedded as watermark and resize this image.
5) Encode secret image and key into the selected number of frames of the video.
6) The secret key which is inserted is provided by the user, which is first encoded and then inserted in the frames of the video.
7) At last, watermarked video is obtained.

Decode

1) The encoded video is taken and the extraction process is made of the key which is inserted in it at the time of encoding.
2) While extraction, take the secret key for extraction and there comes two case
3) Case 1 , if the key matched then start the extraction of watermark image inside the video.
4) Case 2 , if the key didn't match then a dialog box will appear, displaying a message as you are not an authorized user. Then it will stop
5) If case 1 occurs then the watermark is extracted and compared with the original video and results are shown on the basis of MSE, BER, and PSNR.

IX. RESULTS

Sharp point detection is used to find finest point of watermark insertion. A key is also inserted as for reason of security so as no one can hack the information unless and until he knows the key. NC is the normalized correlation. NC value is 1 when the watermark and the extracted watermark are identical and zero if the two are different from each other. The Figure 2 shows extracted watermark image having Normalized correlation of 0.8.

The Results of embedding and extraction process are as shown in figures below. It shows watermarked video frame having PSNR 45.07 db. Here watermarked frame appears exactly same as original video frame. The following figures show respectively the original video, the inserted mark (Figure 1), the watermarked video and the extracted watermark (Figure 2):

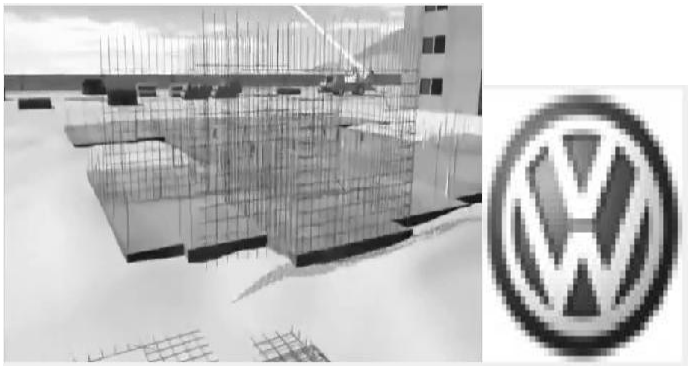
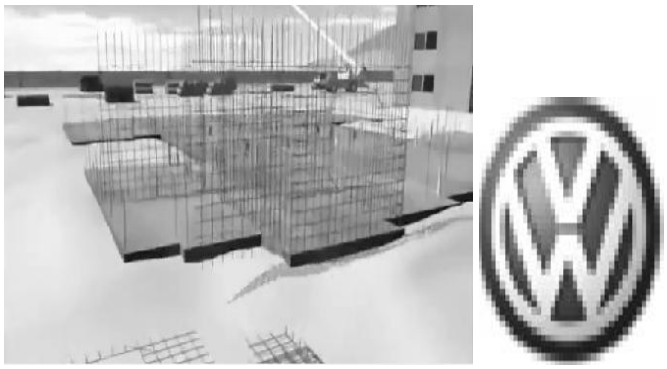


Figure 1 original video and inserted mark



NC=[0.8]

[PSNR=45.07] Figure 2 watermarked video and extracted mark

After that the watermark image and the extracted watermark image compared on the basis of BER, MSE and PSNR. The following figure shows the MSE and BER value comparison respectively. The values are depicting the errors between the original and distorted frames. The values of these two parameters make it clear that there is zero comparative error rate in the proposed algorithm as the videos are identical.

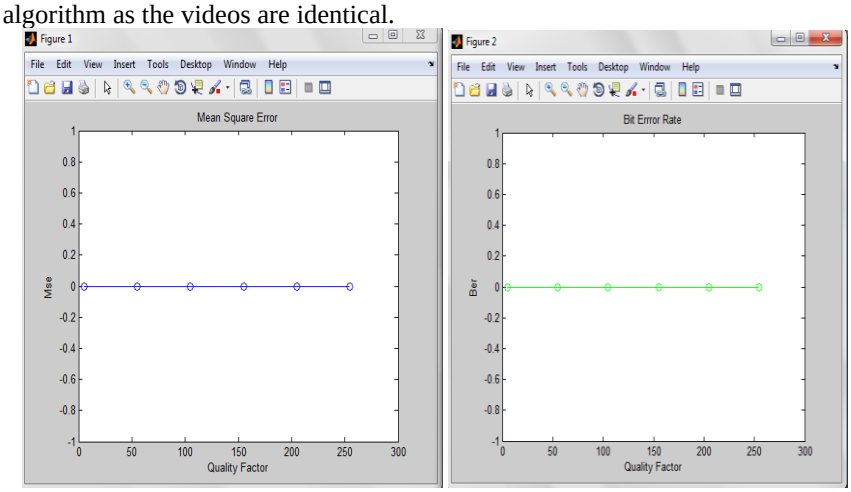


Figure 3 MSE and BER values on basis of quality factor

X. CONCLUSIONS

In this paper, an algorithm is shown which give the points on basis of sharp point detection algorithm and watermark is placed on that detected points so that it cannot be easily detected by hackers. As this system works on edges which mix the watermark on pixel basis. In this system the watermark puts on little effect and show better visuality within video which almost shows no effect on video. A security key is inserted which is embedded inside the video and is useful to hide important and secret information, as it cannot be hacked by anyone without been authorized to it. Edge detection is a fundamental tool in image processing, machine vision and computer vision, particularly in the areas of feature detection and feature extracton.

REFERENCES

[1] Agarwal.A. ; Bhadana.R. ; Chavan.S. ; "A Robust Video Watermarking Scheme using DWT and DCT". (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011,1711-1716.

[2] Averkiou.M.; "Digital Watermarking"

[3] Bhatnagar.G. ; Balasubrmanian.R. ; "Wavelet packet transform-based robust video watermarking technique", Indian Academy of Sciences, pp. 371-388, 2012.

[4] Bhattacharya. S, Chattopadhyay.T. and Pal.A.; "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC", 1-4244-0216-6/06/$20.00 ©2006 IEEE

[5] Chimanna.M.A. ; Khot.S.R. ; "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 2, March -April 2013, pp.839-844

[6] Cox.J.I. et.al," A Secure Robust Watermark for Multimedia, Information Hiding in Computer Science", Vol. 1174, pp.183-206, 1996.

[7] Deshpande.N. ; Rajurkar.A. ; Manthalkar.R. ; "Review of Robust Video Watermarking Algorithms", International Journal of Computer Science and Information Security, 2010, pp. 237-246, 2010.

[8] Fridrich.J. ; Goljan.M. ;" Comparing robustness of watermarking techniques"

[9] Gopal.K. ; Latha.M. ; "Watermarking of Digital Video Stream for Source Authentication", International Journal of Computer Science Issues, Vol. 7, pp. 18-25, 2010.

[10] Gupta.P. ; "Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518.

[11] Hartung.F. ; Girod.B. ; "Watermarking of Uncompressed and Compressed Video", Vol. 63, No. 3, pp. 283-301, 1998.

[12] H. Choi, H. Kim, and T. Kim, "Robust Watermarks for Images in the Subband Domain", Proc. of The 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems (ISPACS'98), Melbourne, Australia, pp. 168–172, 19

[13] Hussein.J. ; Mohammed.A. ; "Robust Video Watermarking using Multi-Band Wavelet Transform", International Journal of Computer Science Issues, vol. 6 pp. 44-49,2009.

[14] Kang.X. ; Huang.J. ;" A DWT-DFT Composite Watermarking Scheme Robust to both Affine Transform and JPEG Compression". IEEE in CirSys Video, Vol. 13, No. 8, pp.776-786, 2003.

[15] Kaur.G. ; Kaur.K. ; " Image Watermarking Using LSB (Least Significant Bit), International Journal of Advanced Research in Computer Science and Software Engineering", Volume 3, Issue 4, April 2013.

[16] Khatib.A.T. et al," A Robust Video Watermarking Algorithm", Journal of Computer Science, Nov, 2008, pp.910-915.

[17] Mane.G.V. ; Chiddarwar.G.G. ; **"**Review Paper on Video Watermarking Techniques", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153

[18] Miller.L.M. ; Cox.J.I. ; "A Review of watermarking principles and practices". Published in Digital Signal Processing in Multimedia Systems, Ed. K. K. Parhi and T. Nishitani, Marcell Dekker Inc., 461-485, (1999).

[19] Powar.P.V. ; Agrawal.S.S. ; "Design of digital video watermarking scheme using matlab simulink", ISSN: 2319 – 1163, Volume: 2, Issue: 5, 826 – 830, IJRET, MAY 2013.

[20] Powar.P.V. ; "Implementation of digital video watermarking scheme based on FPGA", International Journal of Electrical, Electronics and Computer Systems, vol.1 , pp. 99-104,2013.

[21] Rahman.M.; "A DWT, DCT and SVD based watermarking technique to protect the image piracy", Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, Bangladesh.

[22] Razafindradina.H.R. ; Karim.A.M. ; "Blind and robust images watermarking based on wavelet and edge insertion", International Journal on Cryptography and Information Security(IJCIS), Vol.3, No. 3, September 2013.

[23] Sinha.S. ; Bardhan.P. ; et.al ; "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis", International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011

[24] Thapa.M. ; Sood.S.K. ;" On Secure Digital Image Watermarking Techniques", Journal of Information Security, 2011, 2, 169-184 doi:10.4236/jis.2011.24017, Published Online October 2011

[25] Wan Adnan, W.A. ; Ahmad, S.M.S. ; Saripan, M.I. ; "Analysis of watermarking techniques in video", Published In Hybrid Intelligent Systems (HIS), 2011 11th International Conference on 5-8 Dec. 2011, 486 – 492, IEEE

[26] Yen.S.H. ; Wang.C.J. ; "SVM Based Watermarking Technique", Tamkang Journal of Science and Engineering, Vol. 9, No 2, pp. 141_150 (2006)

