International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-9)

Research Article | **September 2015**

Study and Comparison Analysis of a Video Watermarking Scheme for Different Attacks

Himanshu Sharma*, Ashok Kumar, H. L. Mandoria
Department of Information technology, GBPUAT,
Pantnagar, Uttarakhand, India

Abstract—

Now a days Internet is offering a great convenience in transmitting large amount of data in different parts of the world. However, the security and safety of long distance communication remains a matter of concern. Recording, editing and replication of multimedia contents may be the consequence of transmission of such data over the internet. In order to tackle this problem the need of copyright protection was identified. The interest of research, related to digital watermarking is certainly due to the increase in the need of copyright protection of digital content. The appliance of video watermarking in copyright protection, video authentication, copy control, legacy enhancement, broadcast monitoring, annotation etc. is rising immensely. The main objectives of video watermarking are capacity, unobtrusive and robustness. Capacity is the amount of information or data that is to be concealed. The skill to identify the information in security and robustness refers to the resistance to modification of the cover content before secret information is destroyed. Most of the Video Watermarking Algorithms emphasize on robustness. In this paper a video Watermarking scheme using SVD-DWT has been proposed and is tested against various attacks.

Keywords— SVD, DWT, Video Watermarking Attacks, Video shot, Scene change detection

I. INTRODUCTION

Exploitation of Video and other media content has become an increasing problem particularly with the increase of media sharing through the expansion of Internet services and various storage technologies. Video content ownership has become a major concern for movie producers and studios . As a result of which, copyright protection mechanisms came into the field of research. One of the copyright protection mechanism that is the subject of our study is digital watermarking ,has been receiving an increasing attention from researchers especially in designing a seamless algorithm for effective implementation. Digital video watermarking involves embedding secret symbols known as watermarks within video data which can be used later for copyright detection purposes . There are three factors (robustness, security, perceptual fidelity) which are necessary for video watermarking system . The watermark can be visible or invisible. In visible watermarking, the information is visible in the video while in invisible watermarking, information is not visible. It can be detected only by the owner. Another classification of is based on domain which the watermark is applied i.e., the spatial or the frequency domain. The easiest way to watermark a video is to change directly the values of the pixels, in the spatial domain. A more advanced way to do it is to insert the watermark in the frequency domain.

A video is composed of a sequence of images ,which in terms of our stud, are called as frames. So, this gives an illusion of watermarking technique for video and image to be more or less the same. But practically it is not this way right. Video watermarking is different from image watermarking, because a lot more kind of data are available in case of video that may cause information to be more reliably and redundantly embedded.

Large volume of the inherently repeated sequence of data between frames is merely the cause for which video water marking technique has to face the challenges as compared to image Watermarking. Various other factors such as large volume of data, video coding technologies, the unbalance between motion and motionless region, various attacks like frame swapping , frame averaging and statistical analysis makes it different from image watermarking scheme.

II. PROPOSED WATERMARKING SCHEME

In this section, our proposed Video Watermarking Scheme is discussed. The emphasis is on developing an invisible and robust watermark which can withstand both intentional and unintentional attacks. The mark must be recoverable, not only in the complete work, but also in truncated, filtered, dilated, and otherwise processed clips, in a concatenation of unrelated content, and in the presence of noise. To make our embedded watermark imperceptible to human visual system, we have inserted the watermark directly into the frequency domain of our cover video. For this purpose we have used 3-level DWT followed by SVD.

Discrete Wavelet Transform

DWT decomposes a frame into frequency channel of constant bandwidth.. Implementation of DWT is performed as multistage transformation, which constitutes level wise decomposition. At level 1: Image is decomposed into four sub bands: LL, LH, HL, and HH where LL denotes the coarse level coefficient which is the low frequency part of the image. LH, HL, and HH denote the finest scale wavelet coefficient[1,3]. The LL sub band can be decomposed further to obtain higher level of decomposition.

Fig. 1 DWT decomposition.

This decomposition can continues until the desired level of decomposition is achieved for the application. The watermark can also be embedded in the remaining three sub bands to maintain the quality of image as the LL sub band is more sensitive to human eye.

In the wavelet transform domain, high frequency parts represent detailed information of image's edge, contour and texture and so on. It's not easy to detect the watermark in these places as people are not easily able to recognize it. But after processing or attacking, it doesn't have good stability. Most energy of image is centralized in low frequency. Low frequency coefficients are nearly not changed by common attacks so that watermarking information embedded in low frequency coefficients has better robustness.

SVD

Singular value decomposition is a topic covered in linear algebra that decomposes a real or complex matrix. In signal processing, Singular value decomposition has many applications . SVD factorises a matrix M of size *mxn* in the form of

$$M=U \sum V^*$$

where U is an m × m real or complex unitary matrix, Σ is an m × n rectangular diagonal matrix with non-negative real numbers on the diagonal, and V^* (the conjugate transpose of V, or simply the transpose of V if V is real) is an n × n real or complex unitary matrix. The diagonal entries $\Sigma_{i,i}$ of Σ are known as the singular values of M. The m columns of U and the n columns of V are called the left-singular vectors and right-singular vectors of M, respectively.

Reducing the amount of data required to represent a digital image is termed as image compression. Removal of three basic redundancies viz. interpixel redundancy, which results from correlations between the pixels; coding redundancy, which is present when less than optimal; psychovisual redundancies, which is due to data that is ignored by the human visual ,are responsible for achieving compression of digital media

When an image is SVD transformed, it is not compressed, but the data take a form in which the first singular value has a great amount of the image information. With this, we can use only a few singular values to represent the image with little differences from the original.

The proposed video watermarking scheme comprises of different modules such as watermark preprocess, watermark embedding, Attacks on watermarked video and watermark extraction and detection.

WATERMARK PREPROCESS : Watermark is processed before it is embedded in the video. The watermark is cropped into small images, which are used as different independent watermarks. In the detection stage, the watermark is reconstructed with these images. The watermark must be a256-grey-level image, with 8 bits representing each pixel. It is first scaled to a particular size with the following equation. $2^n \leq m$,$n>0$, Such that $p+q=n$, $p,q>0$, where m is the number of frames in a particular scene and n, p, q are integers. Hence the size of the watermark should be $32*2^p \times 32*2^q$ Then the watermark is divided into 2^nsmall images with size 32 X 32.

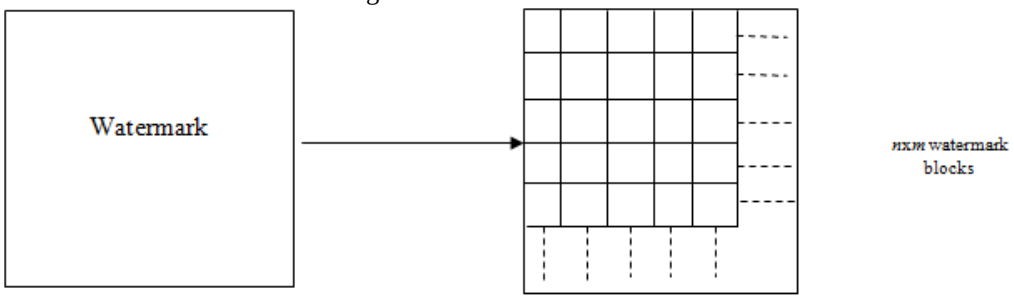


Fig 2. Watermark blocking

Embedding of cropped watermarks into different frames can make the watermarks resistant to attacks by frame averaging. As the watermark is scrambled, it is hard for the attackers to reconstruct the watermark without the knowledge of the cropped watermarks distribution. In the next step, each small image is decomposed into 8 bit-planes, and a large image m_n can be obtained by placing the bit-planes side by side only consisting of 0's and 1's. These processed images are used as watermarks, and totally 2^n independent watermarks are obtained.

WATERMARK EMBEDDING: Watermark is embedded in the wavelet coefficients of low frequency sub-band. Fig.5.3 shows the block diagram of proposed video watermark embedding process. In the present work we consider the host video of size M×N and the watermark W of size n × n. This module is further broken into to 2 sub modules

Scene change detection

This is the video preprocess phase in which different video shots from the input video are identified and taken one by one for watermark embedding process. Scene change detection is done by first calculating the histogram of the red component of all the frames of the supplied video.After this difference of histograms of the consecutive frames are calculated by using the formula:

$$D(x,x+1)= \sum_{x=1}^{n} |A_x(y) - A_{x+1}(y)|$$

where $A_x(y)$ is the histogram value for the red component y in the xth frame.

Now scene change is detected : If D(x,x+1)>threshold(T)

Maximum of D(x,x+1)divided by 3 is considered as threshold value so that adaptive frames for embedding the watermark can be achieved.

Watermark Embedding Algorithm

In the embedding process each video shot is taken one by one to insert watermark individually. This redundancy of watermark will be helpful to sustain a number of attacks like frame averaging, frame dropping. For embedding watermark to a video shot, it is decomposed into m watermark images such as W1, W2, W3….Wm, where the corresponding watermark image is used to modify the frames of corresponding scene. Now SVD is applied on each watermark image to obtain the singular values Sw(j) of jth watermark image as .

$$[Uw(j)\ Sw(j)\ Vw(j)] = svd(W(j))$$

where j=1,2,3……m. For each frame(j = 1, 2 …, m) of the selected video shot , 3 level DWT using HAAR filter on the blue component of every frame of the selected scene to obtain the LL3 sub-band coefficients,is applied. After that SVD is applied on LL3 sub-band coefficients to obtain the singular values $S_i(j)$ as:

$$[U(j)\ S(j)\ V(j)] = svd(LL3(j))$$

where i denotes the sequence of the frames in jth scene. Then, Sw(j) is embedded into $S_i(j)$ using the formula given by

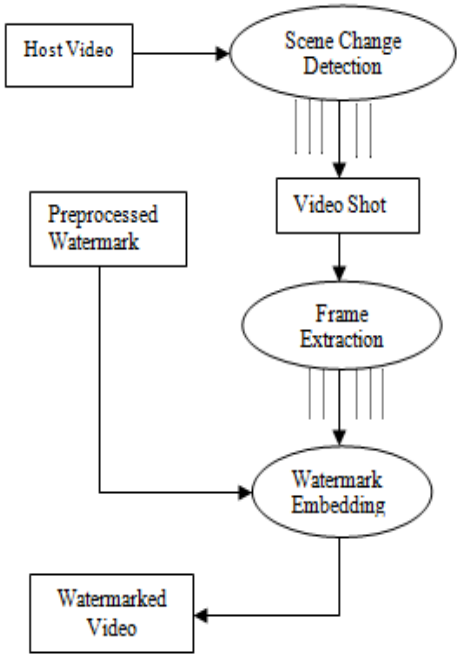
$$D(j)=S(j) + K*Sw(j)$$

where K is the scaling factor or watermarking strength. In the present work, we take K = 50.

Later the watermarked LL3 sub-band coefficients is computed ,using the formula :

$$LL3'(j)=U(j)*D(j)*V^T(j)$$

Finaly inverse 3-level DWT to the modified LL3' sub-band coefficients is applied, to obtain the watermarked blue component of the frame then the original blue component in RGB frame is replaced by the watermarked blue component to obtain the watermarked video.



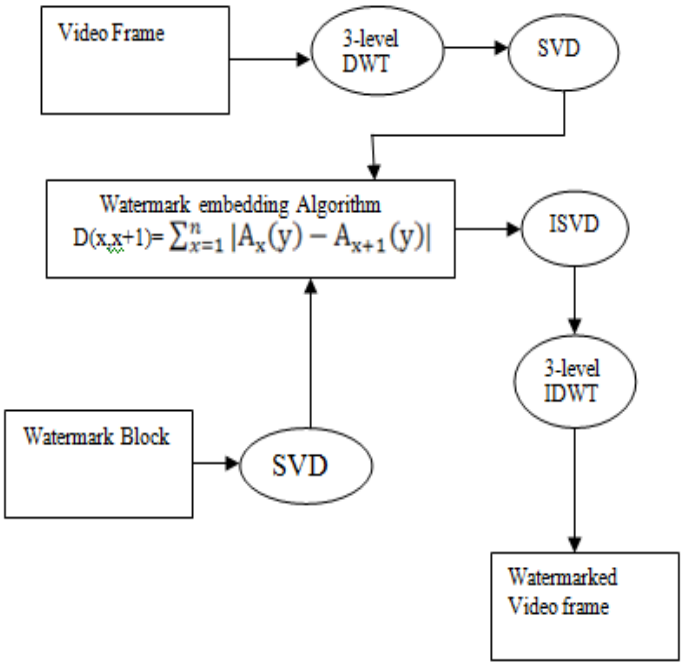


Fig 3. (a). Embedding process (b). Watermark Embedding

ATTACKS ON WATERMARKED VIDEO:

Watermarked video is tested against following attacks to check the robustness and effectiveness of the proposed embedding algorithm.

1. Salt and pepper attack:It is a kind of noise attack in which distortions are added uniformally to frames of video.
2. Cropping and scalling attack: A frame extracted from the video is Cropped, which may result in removal of watermark from the frame.

3. Gaussian Noise attack: Uniformly distributed noise with different intensity is added, to corrupt the Watermarked video.
4. Frame swapping attack: Dynamic composition of the video watermark and video signal can be destroyed by frame swapping.
5. Frame averaging attack: Another significant video watermarking attack is frame averaging.In this attack dynamic composition of the watermark get changed by taking the average of multiple frames.
6. Frame Dropping attack: There is a very little change between the frames in a shot for the existence of the inherent redundancy in video. So, removing frames from the video shot is oftenly used as an effective attack for video watermark.

WATERMARK EXTRACTION

In the extraction process watermark from each video shot is extracted and compared with the original one. Most similar extracted watermark will be considered and rest will be ignored.

For doing so Scene change detection algorithm is applied on the attacked watermarked video. Each scene is considered one by one and extraction process is applied as: Firstly 3 level DWT using HAAR filter on the blue component is applied on each frame of the watermarked video and original video shots to obtain the LL3' and LL3 sub-band coefficients respectively. Secondly SVD is applied on LL3'and LL3 sub-band coefficients to obtain the singular values $S_i^*(j)$ and $S_i(j)$ respectively

$[U(j)\ S(j)\ V(j)]=svd(LL3(j))$

$[U^*(j)\ S^*(j)\ V^*(j)] = svd(LL3'(j))$

where j denotes the sequence of the frames in corresponding scene.

Thirdly, Watermarked singular values are calculated using the formula:

$Sw^*(j)=(S^*(j) - S(j))/K$

Now ,Compute the extracted watermark image $W^*(j)$ for jth frame using the formula given by

$W^*(j) = Uw^*(j)\ Sw^*(j)Vw^*T(j)$

Lastly, Construct the extracted watermark W^* from the computed extracted watermark image to obtain the single watermark image W^*.

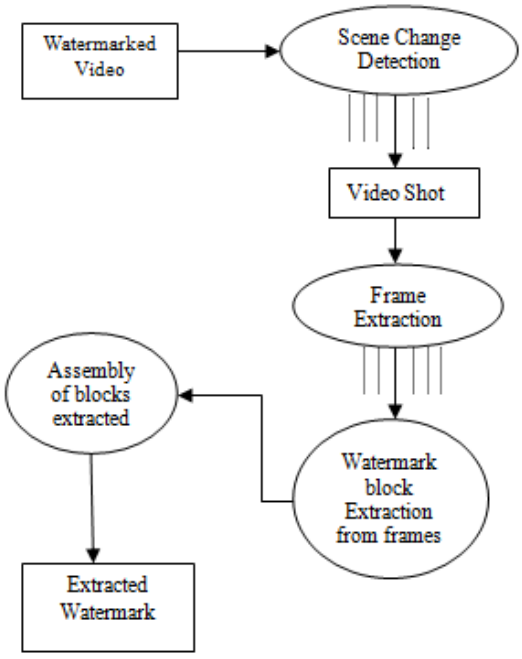
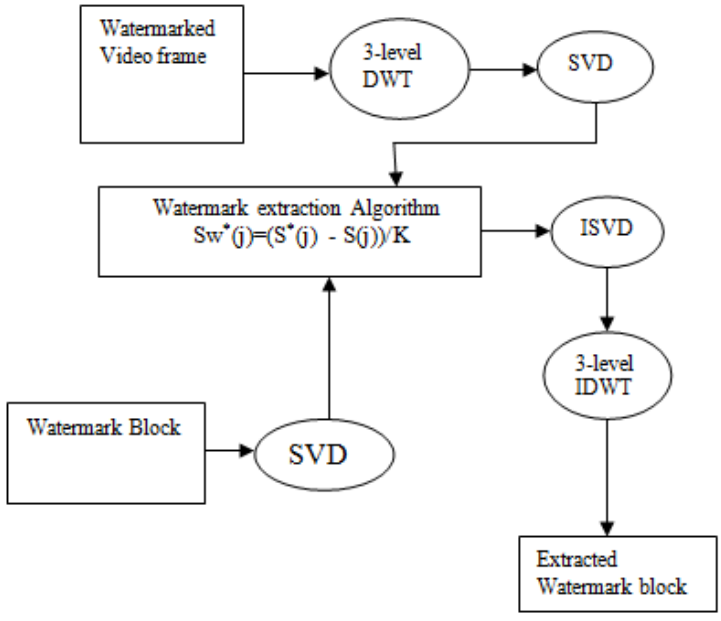


Fig 4 a).Extraction process



b). Watermark Extraction from each shot

WATERMARK DETECTION

1. The imperceptibility of watermarked frame is measured by computing a full-reference metric known as the peak signal-to-noise ratio(PSNR),which is defined by formula

$$PSNR=10*log_{10}\ \frac{(255)^2}{MSE}$$

$$MSE=\frac{1}{m*n}\sum_{i=1}^{m}\ \sum_{j=1}^{n}[X(i,j)-Y(i,j)]^{\ 2}$$

Where m and n are the dimensions of the images X and Y. PSNR is measured in db values of PSNR indicate better watermark concealment.

2. After watermark extraction normalized correlation and bit error rate (BER) is computed between extracted watermark and original watermark by using the formula given by

$$NC=\frac{\sum_i \sum_j W(i,j)W^*(i,j)}{\sum_i \sum_j [W(i,j)^2]}$$

$$BER=\frac{1}{nxn}\sum_{j=1}^{nxn} |W^*(j) - W(j)|$$

here W* is the extracted watermark and W is the original watermark.

3. Most similar watermark is considered and displayed as the Extracted Watermark.

III. CONCLUSION

In our proposed work, an effective and robust DWT-SVD based video watermarking algorithm has been proposed. The singular values of the LL3 sub-band coefficients are modified by the singular values of the binary watermark image. The continuous distribution of Watermark in every scene of the video makes our proposed algorithm suitable for watermarking of video on a real time scale. The Video that will be watermarked with our proposed algorithm is tested against various attacks like lossy compression, Scaling with cropping, Adding Gaussian noise, adding salt pepper noise, Contrast Enhancement and median filtering. We illustrated the robustness of our video watermarking procedure for these attacks.The perceptible quality of the video frames is indicated by PSNR values. Watermark recovery is analysed by calculating cross correlation values and low bit error rate between embedded and extracted watermarks.. The algorithm is robust and showed an improvement over other similar reported methods.

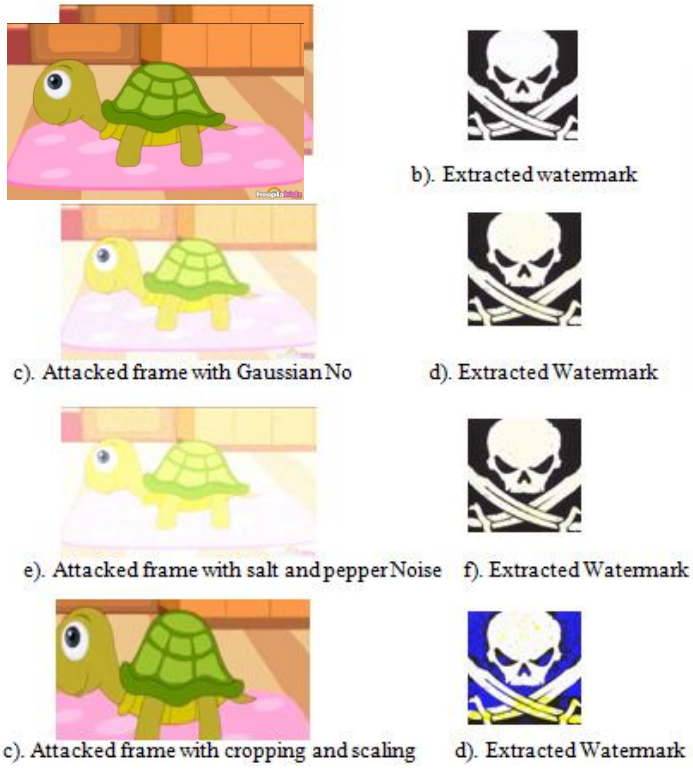


Table 1 Test against common attacks

Attacks	PSNR(dB)	NC(%)
Salt &Pepper 0.3	27.38	99.10
Salt &Pepper 0.5	22.92	98.23
Salt &Pepper 0.8	18.89	87.92
Cropping(10%) & scaling	30.82	98.96
Cropping(20%) & scaling	27.72	96.42
Cropping(30%) & scaling	22.76	91.76
Gaussian Noise 0.3	28.76	97.56
Gaussian Noise 0.5	24.26	94.72
Gaussian Noise 0.8	20.64	91.56

Fig 5 This shows the watermarks extracted after different attacks is applied to watermarked video.

ACKNOWLEDGMENT

This work was supported in part by the Govind Ballabh Pant University of Agriculture and Technology, Pant Nagar, India.

REFERENCES

[1] Boris Vassaux, Philippe Nguyen and Severine Baudry, "*SCRAMBLING TECHNIQUE FOR VIDEO OBJECTWATERMARKING RESISTING TO MPEG-4*" in 4th EURASIP - IEEE Region 8 International Symposium on Video / Image Processing and Multimedia Communications, June 2002

[2] M. KOUBAA, C. BEN AMAR," *Collusion-resistant video watermarking based on video mosaicing*", Proceedings of the Eighth IEEE International Symposium on Multimedia , 2006

[3] Lihua, Z. Nanning, X. Jianru, and X. Tao, ''*A Blind and Spatial-Temporal Based Video Watermarking for H.264/AVC*,'' in IEEE Asia-Pacific Services Computing Conf., 2008 (APSCC '08)

[4] Haohao Song, Zihua Qiu, Jian Gu *,"A Novel Semi-fragile Image watermarking Scheme Based on Wavelet*", 2010 IEEE

[5] Yadollah Zamanidoost and Antonio Navarro," *Robust Video Watermarking Against JPEG Compression in 3D-DWT Domain* ", International Conference on Intelligent Networks -2011

[6] Qing Liu , Jun Ying.," Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis",IEEE Symposium on Electrical & Electronics Engineering (EEESYM)-2012.
[7] Venugopala P S, Dr. H. Sarojadevi and Dr. Niranjan , "Video Watermarking by Adjusting the Pixel Values and Using Scene Change Detection",Fifth International Conference on Signals and Image Processing-2014
[8] Md. Moniruzzaman, Md. Abul Kayum Hawlader ,"An Image Fragile Watermarking Scheme Based on Chaotic System for Image Tamper Detection", 3rd INTERNATIONAL CONFERENCE ON INFORMATICS, ELECTRONICS & VISION 2014
[9] Md. Asikuzzaman , Md. Jahangir Alam, Andrew J. Lambert and Mark Richard Pickering," Imperceptible and Robust Blind Video Watermarking Using Chrominance Embedding:A Set of Approaches in the DT CWT Domain ", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 9, SEPTEMBER 2014
[10] Ryuji Ohura and Teruya Minamoto,"A recoverable visible digital image watermarking based on the dyadic lifting scheme",11th International Conference on Information Technology: New Generations-2014
[11] Meryem Benyoussef, Samira Mabtoul, Mohamed El marraki ,"Medical Image Watermarking for Copyright Protection Based on Visual Cryptography", 978-1-4799-3824-7/14/$31.00 ©2014 IEEE

