Invisible Video Watermarking For Secure Transmission Using DWT and PCA

[1]SnehasmitaSahoo, [2]SupriyaSonone, [3]PriyankaYeole, [4]Prof. S.T. Khot

Savitri BaiPhule University, BharatiVidyapeeth's College of Engineering for Women Pune, India

Abstract: **In this paper, we are developing a new approach towards video watermarking which resulting better robustness, data security and higher embedding capacity. We propose an imperceptible and robust video watermarking algorithm based on discrete wavelet transform (DWT) and principal component analysis (PCA).DWT is more computationally efiicient than other transform methods like DFT and DCT. Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify areas in the host video frame where a watermark can be embedded imperceptible. It is known that even after the decomposition of the video frame using the wavelet transformation there exist some amount of correlation between the wavelet coefficients. PCA is basically used to hybridize the algorithm as it has the inherent property of removing the correlation amongst the data i.e. the wavelet coefficients and it helps in distributing the watermark bits over the sub-band used for embedding thus resulting in robust watermarking scheme that is resistant to almost all possible attacks. The watermark is embedded into the luminance component of the extracted frame as it is less sensitive to the human visual system.**

Keywords: **Digital video; binary watermark; Discrete Wavelet Transform; Principal Component Analysis.**

I. INTRODUCTION

Digital data are distributed across high-speed networks like the Internet and World Wide Web. This data is easily accessible for sharing. Due to this access possibility of tempering data and republishing it as own is increased. This leads the motivation of techniques providing security to this multimedia content. Digital watermarking is the technique used for this purpose. Various techniques of watermarking are used to insert data about ownership of contents, which help to keep the integrity of data.A watermark is information about origin, ownership, copy control etc. This information is embedded in multimedia content with taking care imperceptibly and robustness.The watermark is embedded and extracted as per requirement. Video watermarking is different from image watermarking, because additional data are available here that allows information to be more redundantly and reliably embedded.Digital video is a sequence or collection of consecutive still images. The amount of information that can be embedded in the video sequence is called payload. In reality video watermarking techniques need to meet other challenges than that in image watermarking schemes such as large volume of the inherently repeated sequence of data between frames.The watermark embedding scheme can either embed the watermark into the host signal or to a transformed versionof the host signal. Transform domain watermarking is a scheme that is used to transform image frequency domain in such a way to modify the transform coefficient. Some common transform domain watermarking for image data can be Discrete Cosine Transform (DCT) based [2, 3] or Discrete Wavelet Transform (DWT) based [4]. This scheme is very useful for taking advantage of perceptual criteria in the embedding process for designing watermark techniques. Spatial domain watermarking on the other hand has the capability of performing some transformation directly on image pixels. The use of perceptual models is also an important component in generating an effective and acceptable watermarking scheme for audio just as it is used in image watermarking [3, 4].The technology of embedding and retrieving information into and from video data is video watermarking. Literature survey proposes a concoction of robust and fragile watermarking methods for resolving proof ownership problems [1, 2], copyright protection [3, 4] and video authentication [5]. Various algorithms have been proposed in the scientific literature by numerous authors for robust watermark embedding in video.The crucial components implicated in robust watermarking are watermark embedding, attack, and watermark extraction or detection. In the first phase of watermark embedding, a secure watermark sign (Text, Image or Audio etc) is designed using several technologies like encryption scrambling etc. This secured watermark is then ingrained into an original signal (Video in context with this paper) exploring any of the domains (spatial/frequency/feature etc) of watermarking. Successful embedding algorithms generate the watermarked Video. The third phase is the extraction or detection of the watermark. A triumphant extraction algorithm is one in which the watermark sign could be extracted even after the subjection of an assortment of attacks to the watermarked video. During watermark detection, the watermark detector is specified with a test signal that may be watermarked, attacked or not. The watermark detector reports whether the watermark is present or not on investigating the signal at its input.

The paper is organized as follows. Section II contains the watermarking scheme. Section III contains the experimental results and finally Section IV gives the conclusion.

II. WATERMARKING SCHEME

The watermarking algorithm basically utilizes two mathematical techniques:

DWT and PCA. The significance of using these techniques in watermarking has been explained first.

A. Discrete Wavelet transforms:

Image is represented as a two dimensional (2D) array of coefficients, every coefficient representing the brightness level at that point. Most natural images have smooth color variations, with the fine details being described as sharp edges in between the smooth variations. Technically, the smooth variations in color could also be termed as low frequency components and therefore the sharp variations as high frequency components. The low frequency components constitute base of an image, and also the high frequency components add upon them giving a detailed image. Hence, the averages/smooth variations are demanding a lot of importance than the details [imp DWT]. DWT is used to implement a simple watermarking scheme. The 2-D discrete wavelet transforms (DWT) decomposes the image into sub-images. The approximation look like the original, only on the 1/4 scale. The 2-D DWT is an application of the 1-D DWT in both the horizontal and also the vertical directions. The DWT decompose an image into a lower resolution approximation image (LL) as well as horizontal(HL)vertical (LH) and diagonal (HH) detail components.Due to its excellent spatial-frequency localization properties DWT is very suitable to identify areas in the host video frame where a watermark can be embedded imperceptibly. Embedding the watermark in low frequencies obtained by wavelet decomposition increases the robustness with respect to attacks that have low pass characteristics like lossy compression, filtering, and geometric distortions. Video is nothing but collection of still images. Original video is converted into frames discrete wavelet transform (DWT) and principal component analysis (PCA) are applied on each frame. Watermark image is converted into vectors and embedded in the low frequency (LL) DWT sub-bands of each decomposed frame. Embedding the watermark in both LL and HH makes the scheme robust to a variety of low and high frequency characteristic attacks [1]. Then inverse DWT and inverse PCA is applied to get watermarked video. One frame is chosen from watermarked video for implementation.

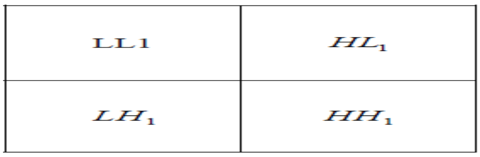

Figure1. DWTsubbands

B. Principal Component Analysis:

In digital image processing field, PCA is considered as a linear transform technique to convey most information about the image to principal components. PCA is a method of identifying patterns in data, and expressing the data in such a way so as to highlight their similarities and differences. Once these patterns in the data have been identified, the data can be compressed by reducing the number of dimensions, without much loss of information. It plots the data into a new coordinate system where the data with maximum covariance are plotted together and is known as principal component. PCA transform is used to embed the watermark in each colour channel of each frame of video. The main advantage of this approach is that the same or multi-watermark can be embedded into the three colour channels of the image in order to increase the robustness of the watermark.

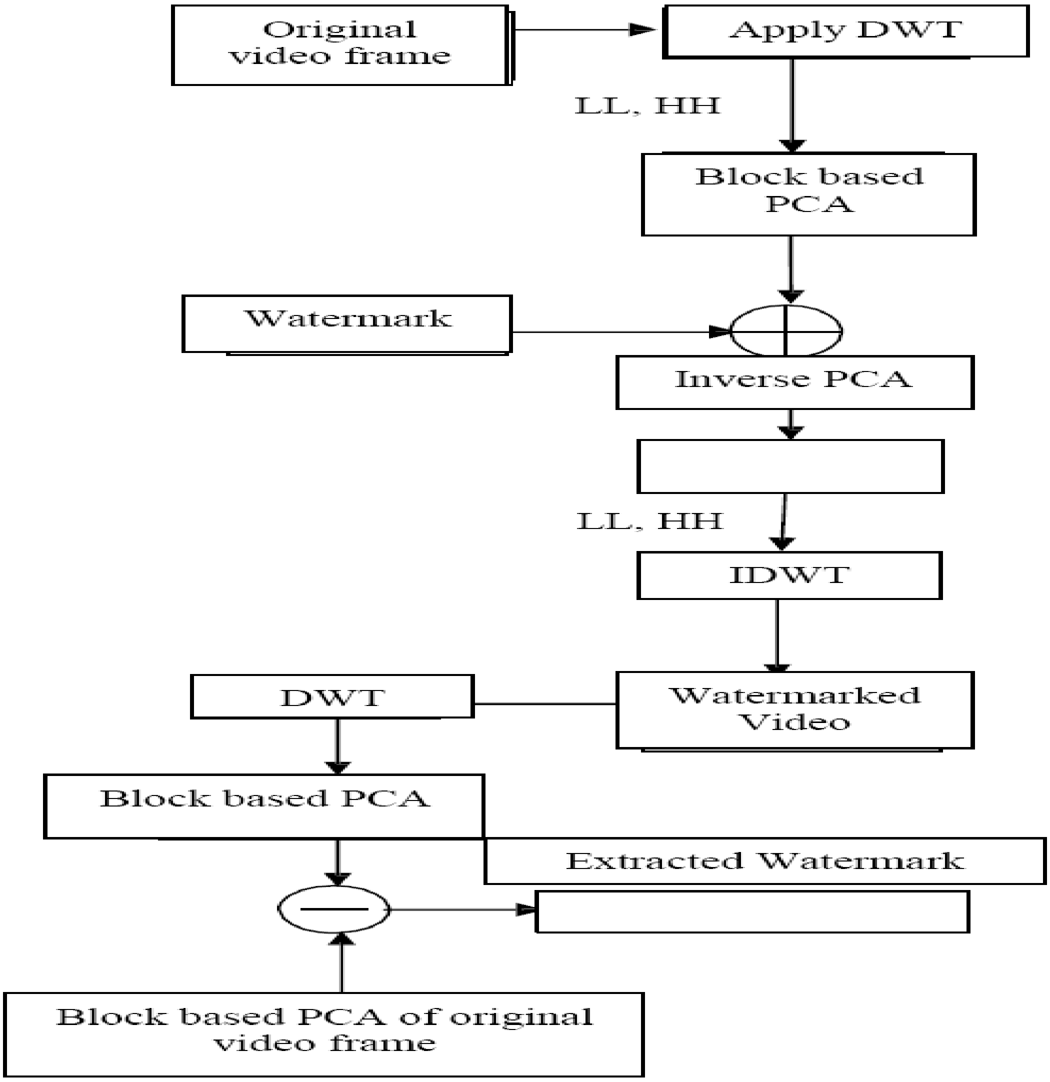

Figure: 2. Block Diagram of Watermarking

Algorithms for watermarking using DWT AND PCA

Algorithm 1:

a) Embedding Procedure:

Step 1: Convert the n × n binary watermark logo into a vector wm= { w_1, w_2 , ……, $w_{n \times n}$ } of ‘0’s and ‘1’s.

Step 2: Divide the video (2N × 2N) into distinct frames.

Step 3: Convert each frame from RGB to HSV colour format.

Step 4: Apply 1-level DWT to the value (V component) of each video frame to obtain four sub-bands LL, LH , HL and HH of size N x N .

Step 5: Divide the HH sub-band into k non-overlapping sub-blocks each of dimension n × n (of the same size as the watermark logo).

Step 6: The watermark bits are embedded with strength α into each sub-block by first obtaining the principal component scores by Algorithm 2. The embedding is carried out as equation 1.

$y_i = y_i + \alpha(wm)$ ...(1)

Where y_i represents the principal component matrix of the ith sub-block.

Step 7: Apply inverse PCA on the modified PCA components of the sub-blocks of the HH sub-band to obtain the modified wavelet coefficients.

Step 8: Apply inverse DWT to obtain the watermarked value component of the frame. Then convert the video frame back to its RGB components.

b) Extraction Procedure:

Step 1: Divide the watermarked (and possibly attacked) video into distinct frames and convert them from RGB to HSV format.

Step 2: Choose the value (V) component of a frame and apply the DWT to decompose the V component into the four sub-bands LL , HL , LH , and HH of size N×N.

Step 3: Divide the HH sub-band into n × n non-overlapping sub-blocks.

Step 4: Apply PCA to each block in the chosen subband HH by using Algorithm 2.

Step 5: From the HH sub-band, the watermark bits are extracted from the principal components of each sub-block as in equation 2.

$y1=abs(y-y1)/\alpha \ldots (2)$

where y1 is the watermark extracted.

III. EXPERIMENTAL RESULTS

The proposed algorithm is applied to a sample video sequence ‘bus.avi’ using a 100 × 100 watermark logo. The grayscale watermark is converted to binary before embedding. Fig. 3(a) and 3(b) show the original and the watermarked video frames respectively. Fig. 4(a) is the embedded watermark and Fig. 4(b) is the extracted binary watermark image.

The performance of the algorithm has been measured in terms of its imperceptibility and robustness against the possible attacks like noise addition, filtering, geometric attacks etc.

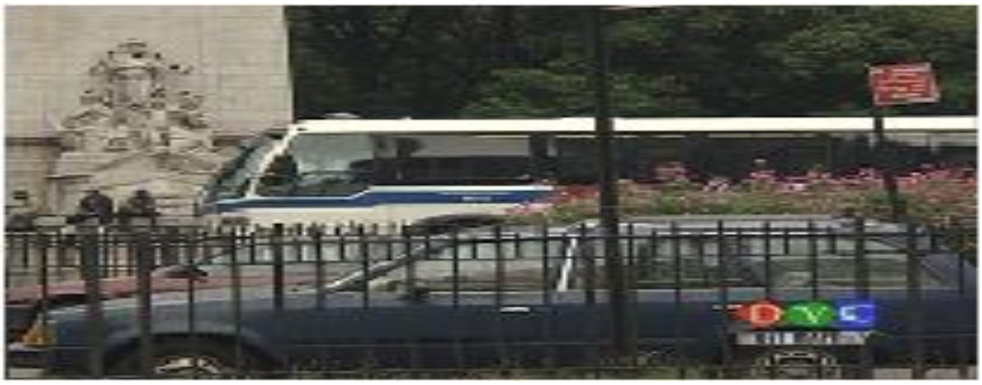

Fig. 3(a) Original Frame

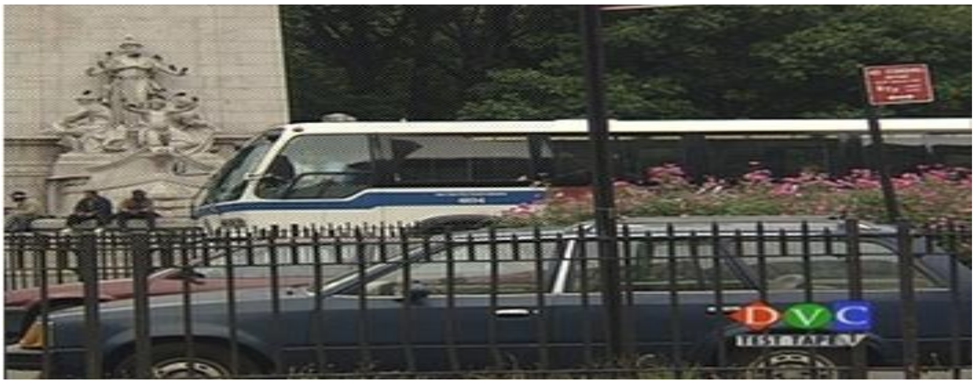

Fig. 3(b) Watermarked Frame

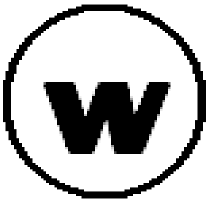

Fig. 4(a) Watermark

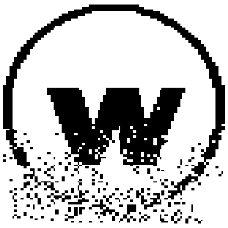

Fig. 4(b) Extracted Watermark

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

$$PSNR = 10 Log_{10}(255^2 / MSE) \qquad (3)$$

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

$$MSE= (1/N*M)\sum_{n=1toN}\sum_{m=1toM}[x(i,j) - x'(i,j)]^2 \qquad (4)$$

where x and x' 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).

NC: The normalized coefficient (NC) gives a measure ofthe robustness of watermarking and its peak value is 1.

$$NC = \frac{\sum_i\sum_J W(i,j) \cdot W(i,j)}{\sqrt{\sum_{Ij}\sum y(i,j)}\ \sqrt{\sum_{Ij}\sum y'(i,j)}} \qquad (5)$$

Where y and y' represent the original and extracted watermark respectively.

After extracting and refining the watermark, a similarity measurement of the extracted and the referenced watermarks is used for objective judgment of the extraction fidelity. The following images represents the watermarked video after attacks have been carried on it.

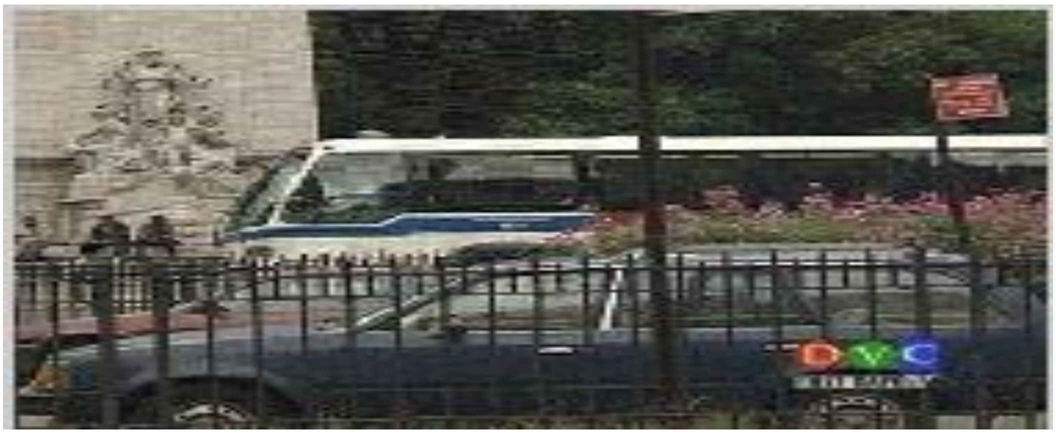

Fig. 5(a) Video frame after adding Gaussian noise

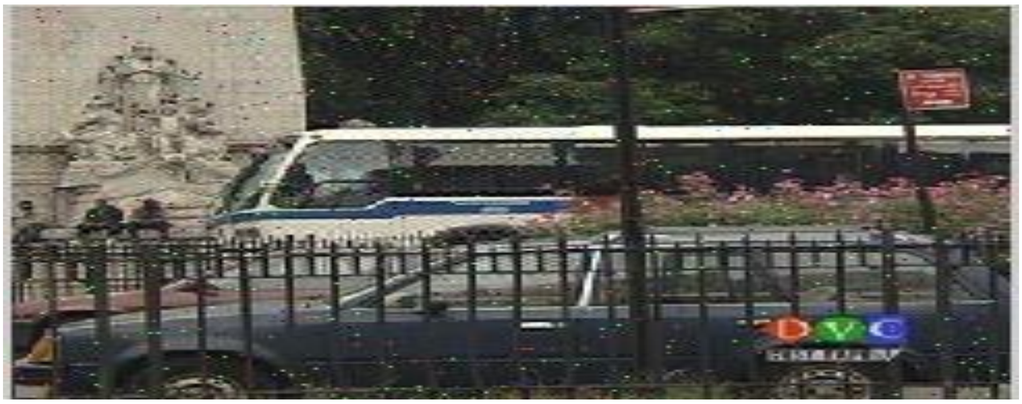

Fig. 5(b) Video frame after adding Salt and Pepper noise

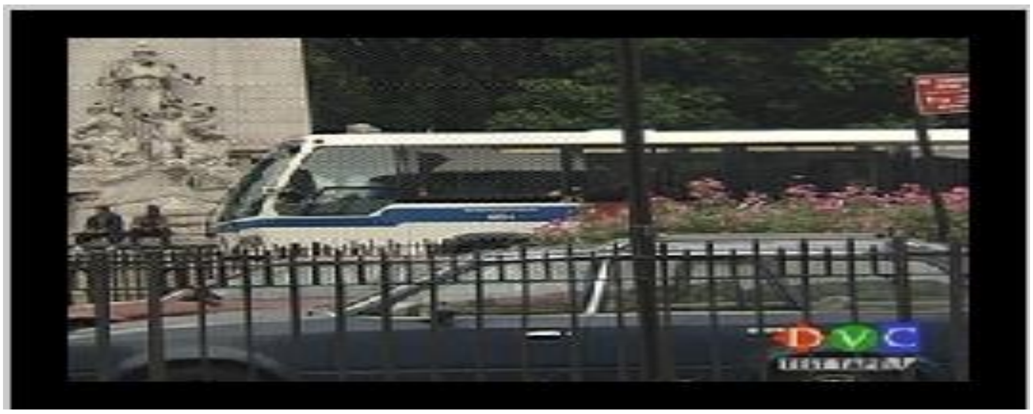

Fig. 5(c) Video frame after cropping

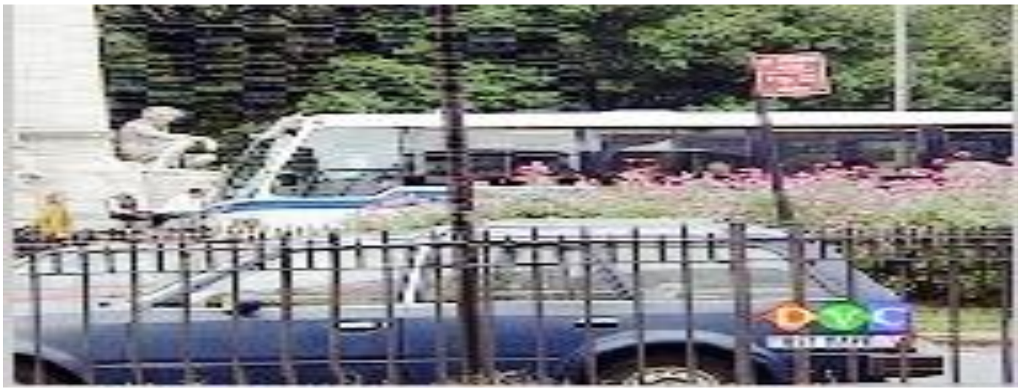

Fig.5(d) Video frame after histogram equalization attack

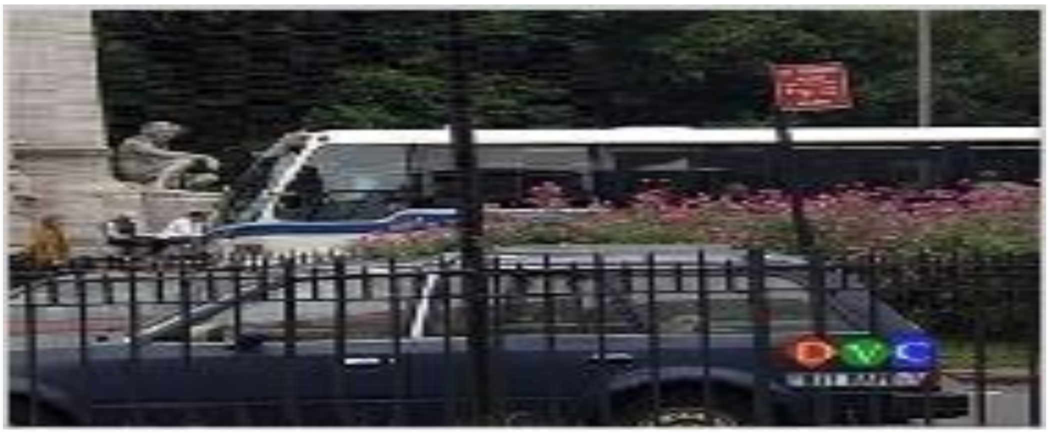

Fig. 5(e) Video frame after contrast adjust attack

Fig.5(f) Video frame after median filtering attack

Fig. 5(g) Video frame after rotational attack

The following table shows the value of the data collected from the watermarked video after performing the various attacks as shown previously.

Table 1: Result Analysis

Attack	**PSNR**	**NC**
Gaussian Noise	39.3665	0.9619
Salt and Pepper Noise	42.2514	0.9618
Cropping Noise	35.0547	0.9620
Histogram Equalization Attack	30.6258	0.8857
Contrast Adjust Attack	37.4374	0.9320
Median Filtering Attack	40.1588	0.9464
Rotational Attack	32.2829	0.9661

Frame dropping: Frame dropping means dropping oneor more frames randomly from the watermarked video sequence. If we drop too many frames, the quality of the watermarked video will decrease rapidly. In our experiment, we only drop one frame randomly. Due to embedding the same watermark into each frame, it will not affect the extraction of the watermark completely from attacked watermarked video by frame dropping except that number of the extracted watermarks will differ.

Frame swapping: Frame swapping means switching theorder of frames randomly within a watermarked video sequence. If we swap too many frames, it will degrade the video quality. We have extracted all the watermarks from the video after frame swapping.

Frame averaging: Since the frames are watermarkedwith the same information, the watermarked videos are not subject to the risk of watermark estimation by frame averaging since the watermark signal gets amplified on averaging.

Thus from the experimental results it is quite evident that the watermarking algorithm is robust against all possible attacks. Other than its computational complexity it has no disadvantages.

IV. CONCLUSION

The algorithm implemented using DWT-PCA is robust and imperceptible in nature and embedding the binary watermark in the high HH sub band helps in increasing the robustness of the embedding procedure without much degradation in the video quality. Because HH sub band don’t have much valuable information. As a future work the video frames can be subject to scene change analysis to embed an independent watermark in the sequence of frames forming a scene, and repeating this procedure for all the scenes within a video.

ACKNOWLEDGEMNT

The authors would like to thank the department of electronics and telecommunication for the careful proofreading for preparing this manuscript.

REFERENCES

[1] International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011 ”Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis”Sanjana Sinha, PrajnatBardhan, SwarnaliPramanick, Ankul Jagatramka, Dipak K. Kole, Aruna Chakraborty. Department of Computer Science & Engineering St Thomas’ College of Engineering and Technology Kolkata, India.{aruna.stcet@gmail.com, dipak. kole @gmail.com, sanjana sinha89@gmail.com}

[2] Palaiyappan , Raja JeyaSekhar. “A Block Based Novel Digital Video Watermarking Scheme Using DCT” IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p- ISSN: 2278-8735. Volume 5, Issue 2 (Mar. - Apr. 2013), PP 34-44 www.iosrjournals.org www.iosrjournals.org

[3] Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish, Member, IEEE, and OrlyYadid-Pecht.“Hardware Implementation of a Digital Watermarking System for Video Authentication”IEEE transactions on circuits and systems for video technology, vol. 23, no. 2, february 2013.

[4] Vipula Madhukar Wajgade1, Dr. Suresh Kumar2 1MTech(CSE) IInd Year, SGT Institute of Technology And Management, Gurgaon, Haryana, India 2HOD, Department Of Computer Science, SGT Institute of Technology And Management, Gurgaon, Haryana, India.“Enhancing Data Security Using Video Steganography “International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013)549

[5] Harshitha K M, Dr. P. A. VijayaAbbas Cheddad,JoanCondell,KevinCurran,PaulKevitt,”Enhancing Steganography In Digital Images”. Proc. Canadian Conference on Computer and Robot Vision. “Secure Data Hiding Algorithm Using Encrypted Secret message” International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012 1 ISSN 2250-3153 www.ijsrp.org.