IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 4 (Mar. - Apr. 2013), PP 18-24
www.iosrjournals.org

Video Watermarking Scheme Based on DWT and PCA for Copyright Protection

Phadtare Saurabh[1], Dhebe Pooja[2], Bobade Sharayu[3], Jawalkar Nishigandha[4]
[1](Computer Engineering, Sinhgad College Of Engg,Pune./ University of Pune, India)
[2](Computer Engineering, Sinhgad College Of Engg,Pune./ University of Pune, India)
[3](Computer Engineering, Sinhgad College Of Engg,Pune./ University of Pune , India)
[4](Computer Engineering, Sinhgad College Of Engg,Pune./ University of Pune , India)

Abstract :*The distribution of digital products like audio and video are increasing rapidly over the networks, so the owners of such digital data are worried about their ownership protection. It may be possible that the third-party may claim the digital products as their own and misuse it in future. In order to overcome this problem, 'Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform for Copyright Protection', is introduced for preventing illegal copying of their digital products. In this system, a Binary logo watermark is embedded in video frames for copyright protection. Principal Component Analysis (PCA) is applied to each block of the two bands (LL – HH) which results from Discrete Wavelet transform of the video frame. The watermark is embedded into the principal components of the LL blocks and HH blocks at different levels. Combining the DWT and PCA transform improves the performance of the watermark algorithm. This watermarking scheme shows no visible difference between the watermarked frames and the original frames i.e. imperceptible to the Human Visual System (HVS). It depicts the robustness against a wide range of attacks such as geometric transformation, histogram equalization, and gamma correction.*

Keywords -*Advanced Encryption Standard (AES), Discrete wavelet transforms (DWT)**, Fixed-length codeword (FLC), Principle Component Analysis (PCA), Video Watermarking.*

I. Introduction

Existence of Digital Watermarking was founded in 1979. It gained popularity in 1990. No one person is recognized as the founder or inventor of the digital watermark. Digital watermarking in its growing stages is gaining more importance and reasons for applying, cases like Napster.

'Fingerprinting' is also known as digital watermarking. Copyright owners are allowed to integrate a digital watermark into their work to identify which information is invisible to the human eye. Whenever any kind of illegal copy of photos and music is found on the Internet by the respective copyright owner, he can take appropriate legal action by combining new tracking services that are offered by some of the same companies which are having watermarking technology.

Watermarks are usually of two types, visible and invisible. They can be viewed with either stand alone technology or plug-in play software. Digital watermarking technology is a unique identification code that can be traced to the copyright owner. It completes the copyright ownership information. A special feature pattern of bits is inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.). Copyright protection for intellectual property that is in digital format is the purpose of digital watermarks.

Purpose

Lately, the users of networks, especially the World Wide Web have increased rapidly. The procreation, manipulation and the distribution of digital multimedia via networks become faster and easier. Therefore, the owners of the digital products are concerned about illegal copying of their products. As a consequence of this, security and copyright protection are becoming essential issues in multimedia applications and services. The copyright information is embedded into multimedia data in order to protect the ownership, this is the purpose of the proposed system i.e. watermarking scheme.

In the beginning, video watermarking techniques were based on DCT and DFT which did not provide the advantage of both spatial domain and frequency domain [8]. So DWT was innovated which increased the robustness of the watermarking scheme [4]. DWT is used in watermarking algorithms to increase the security whereas PCA provides imperceptibility in watermarked video. Thus, in this watermarking scheme, both transformations i.e. DWT and PCA are applied. For video encoding and decoding purpose, AES algorithm is implemented. In this scheme, MPEG4 (Moving Picture Experts Group) standard videos are most preferably used. As the luminance component is less sensitive to the human eye than chrominance components, the watermark logo is embedded in the luminance (Y) component of each frame of the uncoded video.

II. Watermarking Scheme

2.1 Discrete Wavelet Transform (DWT)

Wavelet transform breaks down an image or video frame into a set of band fixed components which can be put together to rebuild the master copy [7, 9]. For 2-D images, using DWT agrees to work on the image with 2-D filters in each dimension. The filters will divide the input image into four non-overlapping multi-resolution sub bands which are lower resolution approximation image (LL1), horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components as shown in Fig.1. The process required to obtain a multiple scale wavelet decomposition. One of the advantages of DWT over DCT is that it can more accurately model the aspects of the HVS as compared to DCT [1, 5].

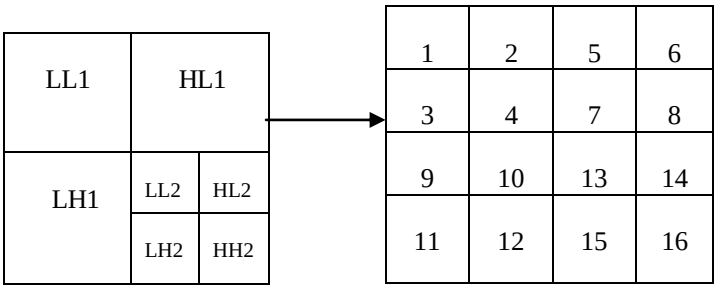

Fig 1: Two level wavelet decomposition and sub band numbering

2.2 Principal Component Analysis

Principal component analysis (PCA) is a mathematical process which utilizes an orthogonal transformation to change a set of observations of possible correlated variables into a set of values of uncorrelated variables called principal components. The number of principal components is less than or equal to the number of original variables. PCA highlights the similarities and differences of the data. Since patterns in data are difficult to find in data of high dimension, graphical representation is not available, PCA is a powerful tool for examining data. The other major advantage of PCA is to identify patterns in the data and then the data is compressed by reducing the number of dimensions, without a lot of information loss. It plots the data into a new coordinate system where the data with maximum covariance are plotted together and is known as the first principal component [3].

Similarly, there are the second and third principal components and so on. The maximum energy engrossment lies in the first principal component. The following block diagram (Fig.2 and Fig.3) shows the embedding and extraction process of the watermark. In the suggested method the binary watermark is embedded into each of the video frames by the decomposition of the frames into DWT sub bands followed by the application of block based PCA on the sub-blocks of the low frequency sub band. The watermark is embedded into the principal components of the sub-blocks. The extracted watermark is obtained through a similar process.

3.1 Algorithms for watermarking using DWT and PCA techniques

Algorithm 1:

The PCA approach is applied to the transform coefficients of wavelet sub band SB_θ where θ represents (LL or HH) as shown in the following steps:

Step1: The wavelet sub band SB_θ with NxN dimension is subdivided into n x n non overlapping blocks (the block size should be appropriate to the sub band size) where the number of blocks is given by nb = NxN/n x n.

Step 2: Each block in the LL band can be processed by method1 and each block in HH band can be processed by method2 as follows:

Method 1: Consider each block like a vector; data vectors can be expressed as:

$SB_\theta = (SB_{\theta 1}, SB_{\theta 2}, SB_{\theta 3} \ldots SB_{\theta k})^T$, where vector $SB_{\theta i}$ represents the block number i with n2 dimension.

Method 2: Each block can be considered as 2D array $BL_\theta = (BL_{\theta 1}, BL_{\theta 2}, BL_{\theta 3} \ldots BL_{\theta k})^T$, where array $BL_{\theta i}$ represents the block number i with size nxn.

Step 3: For each block, the covariance matrix CO_i of the zero mean block Z is calculated as:

$COi = Z_i Z_i^T$ …… (1)

Where TR denotes the matrix transpose operation and Z is defined by:

Method 1: for a vector block as $Z_i = EX (SB_{\theta i} - me_i)$.

Method 2: for 2D array block as $Z_i = EX (BL_{\theta i} - me_i)$.

Where me_i is the mean of block and EX denotes expectation operation.

Step 4: Each block is transformed into PCA components by calculating the eigenvectors (basis function) corresponding to the eigenvalues of the covariance matrix:

$CO_i \Phi = \lambda_i \Phi$ …… (2)

Where Φ is the matrix of eigenvectors and λ is the matrix of eigenvalues defined for:
Method 1: for a vector block as $\Phi = (egv_1, egv_2, egv_3 \ldots egv_{nxn})$ and $\lambda_i = (\lambda_1, \lambda_2, \lambda_3 \ldots \lambda_{nxn})$.
Method 2: for 2D array block as $\Phi = (egv_1, egv_2, egv_3 \ldots egv_n)$ and $\lambda_i = (\lambda_1, \lambda_2, \lambda_3 \ldots \lambda_n)$.
Φ vectors are sorted in descending order according to λ_i , where ($\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \ldots..\geq \lambda_n$ or (λ_{nxn})). The matrix Φ is an orthogonal matrix called basis function of PCA (PCA eigen images).
Step 5: Calculate the PCA components of the block. The PCA transforms the correlated block into uncorrelated coefficients by taking the inner product of the block with the basic functions Φ:
$PC_i = \Phi^T Z_i$…….. (3)
Where PC_i is the PC block which represents the principle component of the block i.
Step 6: Apply inverse PCA on the modified PCA components to obtain the modified wavelet coefficients. The inversion can be performed by the following equation:
$Z_i = \Phi\ PC_i$ **…**…… (4)

3.2 Watermark Embedding

Step 1: Divide video into frames and convert 2Nx2N RGB frames into YUV components.
Step 2: For each frame, choose the luminance Y component and apply the DWT to decompose the Y frame into four multi resolution sub bands NxN: LL, HL, LH, and HH.
Step 3: Divide the two sub bands LL and HH into n x n non overlapping blocks.
Step 4: Apply PCA to each block in the chosen sub bands LL by using method1 and HH by using method2
Step 5: Convert the 32x32 binary watermark logo into a vector BW = {bw1, bw2… bw32x32} of '0's and '1's.
Step 6: Embed the logo into LL and HH bands by different ways. For the LL band, the watermark bits are embedded with strength α_1 into the first principle component of each PC block PC_i. From equation (3), for the PC block $PC_1, PC_2, PC_3 \ldots PC_k$, we can define $PC_I = (PC_1\ (1), PC_2\ (1), PC_3\ (1) \ldots PC_k\ (1))^T$ and the embedding equation:
$PC_I\ ' = PC_I + \alpha_1\ BW$…….. (5)
Step 7: For HH band, use two pseudorandom sequences (PNS); ps_0 and ps_1 with different keys k_1 and k_2 to embed the watermark bit bw '0' and '1' respectively [12,13]. So, we can represent BWm as follows:

$$BWm = \begin{cases} ps0 \text{ if } bw = 0 \\ ps1 \text{ if } bw = 1 \end{cases} \quad \text{…….....} \ (6)$$

When bit bw = 0, embed ps_0 with strength α_2 to the mid-band coefficient of PC block PC_i and when bit bw=1, embed ps1 with strength α_2 to the mid-band coefficients of PC block PC_i.
If PCB includes the mid-band coefficients then the embedding equation is:
$PCB' = PCB + \alpha_2 BWm$…… (7)
Step 8: Apply inverse PCA on the modified PCA components of the two bands to obtain the modified wavelet coefficients.
Step 9: Apply the inverse DWT to produce the watermarked luminance component of the frame. Then reconstruct the watermarked frame.

3.3 Watermark Extraction

The watermark extraction procedure is as follows:
Step 1: Convert the watermarked (and may be attacked) video into frames and convert the 2Nx2N RGB frames into YUV components.
Step 2: For each frame, choose the luminance Y component and apply the DWT to decompose the Y frame into four multi resolution sub bands NxN.
Step 3: Divide the sub bands LL and HH into n x n non overlapping blocks.
Step 4: Apply PCA to each block in the chosen sub bands LL by using method1 and HH by using method 2
Step 5: Convert the 32x32 binary watermark logo into a vector $BW = \{bw_1, bw_{2\ldots}\ bw_{32x32}\}$ of '0's and '1's.
Step 6: For the LL band, the watermark bits are extracted from the first components of each block by:
$BW' = (PC_I\ ' - PC_I)/\ \alpha_1$……..... (8)
Step 7: For the HH band, re-generate the two (PNS) sequences ps_0 and ps_1 with the same keys k_1 and k_2 used in embedding. Afterwards, the (PNS) sequences are extracted from the mid-band coefficient of each PC block PCB by:
$BWm' = (PCB' - PCB)/\ \alpha_2$……..... (9)
The embedded bits are estimated depending on the correlation value Corr between ps_0 and ps_1 and extracted sequences BWm' and a predefined threshold Thr as follows:

$$BW' = \begin{cases} 0 \text{ if } \mathrm{Corr}(ps0, BWm') > Corr(ps1, BWm') \\ \quad \text{and } \mathrm{Corr}(ps0, BWm') > Thr \\ 1 \text{ if } \mathrm{Corr}(ps1, BWm') > Corr(ps0, BWm') \\ \quad \text{and } \mathrm{Corr}(ps1, BWm') > \mathrm{Thr} \end{cases} \quad \ldots\ldots (10)$$

Step 8: After extracting the watermark from LL and HH bands, similarity measurements of the extracted watermark BW' and the referenced watermarks BW are used for objective judgment of the extraction fidelity NC which is given by:

$$NC = \frac{\sum_i \sum_j BW(i,j).BW'(i,j)}{\sqrt{\sum_i \sum_j BW(i,j)^2} \sqrt{\sum_i \sum_j BW'(i,j)^2}} \ldots\ldots\ldots\ldots\ldots (11)$$

3.4 AES Algorithm

The U.S. government has adopted the Advanced Encryption Standard (AES) as one of the encryption standards in cryptography. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, acquired from a larger collection originally published as Rijndael. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as it overcomes the shortcomings of DES.

According to MPEG standards, the following FLC data elements exist in an MPEG-video bit stream:

• 4-byte start codes: 000001xx (hexadecimal);
• Almost all information elements in various headers;
• sign bits of non-zero DCT coefficients;
• (Differential) DC coefficients in intra blocks;
• ESCAPE DCT coefficients;
• Sign bits and residuals of motion vectors.

With the three control factors, the encryption procedure of PVEA can be described as follows:

1) Encrypting intra DC coefficients with probability psr;
2) Encrypting sign bits of non-zero DCT coefficients (except for intra DC coefficients) and ESCAPE DCT coefficients with probability psd;
3) Encrypting sign bits and residuals of motion vectors with probability pmv.

Either a stream cipher or a block cipher can be used to carry out the encryption of selected FLC data elements. When a block cipher is adopted, the consecutive FLC data elements should be first concatenated together to form a longer bit stream, then each block of the bit stream is encrypted, and finally each encrypted FLC data element is placed back into its original position in the video stream. Though the stream cipher or block cipher embedded in PVEA is secure, here we should assume some special consideration in order to ensure the security against various attacks.

In the above-described PVEA, the three factors control the visual quality, as follows:

• psr = 1 → 0: the spatial perceptibility changes from 'almost imperceptible' to 'perfectly perceptible' when psd = 0 or to 'roughly perceptible' when psd > 0;
• psr = 0, psd = 1 → 0: the spatial perceptibility changes from 'roughly perceptible' to 'perfectly perceptible';
• pmv = 1 → 0: the temporal (motion) perceptibility (for P/B-pictures only) changes from 'almost imperceptible' to 'perfectly perceptible'.

3.5 Working

The design used, selectively e crypts fixed length codeword (FLC) in MPEG video bit streams under the control of 3 perceptibility factors-Psr,Psd,Pmv. These factors mainly deal with video encoding and decoding issue.

The values

Psr- Control factor for intra DC coefficients (rough view)
Psd- Control factor for non intra DC, AC, ESCAPE DCT coefficients (details)
Pmv- Control factor for sign bits & residuals of motion vectors (related to motions)

are taken from the user whose values are independent of each other and are between 0 & 1.

These are further used for encryption procedure that can be described as follows. Encrypting intra DC coefficients with probability Psr.

Encrypting sign bits of non-zero Duct coefficients and ESCAPE DCT coefficients with probability Psd. Encrypting sign bits & residuals of motion vectors with probability Pmv.

The algorithms used are AES-128 algorithm and DCT. Since block cipher is adopted to be used in AES the consecutive FLC data elements should be first concatenated together to form a longer bit stream, then each

block of the bit stream is encrypted and finally each encrypted FLC data elements is placed back into its original position in the video stream.

The value of 'nf'(number of KeyFrames) and 'n'(PlayerIteration) is taken which are greater than 0 and encryption key that can be any alphanumeric value is taken from the user.

Now the video is selected from the pop-up menu and total number of frames comprised by the video is displayed above the video.

When the 'videoencryption'button is hit the following operations takes place:

Loading of the image file, saving of the image file, encryption of the video.

Psr and Psd variables are use to determine the scale for quality scaling and Pmv is used to determine the value of coefficient quantization matrices i.e. whether intra or inter quantization blocks to be used (based on the frame type)

Then input the decryption key that will be used for video decryption and also user id of sender and receiver.The user id of receiver is used for decrypting using AES algorithm.

To view the watermarked or retrieved video separately hit the 'Watermarked Video'or 'Retrieved Video' button respectively or to view the encrypted and decrypted video simultaneously hit the 'Watermarked/Retrieved Video'button.

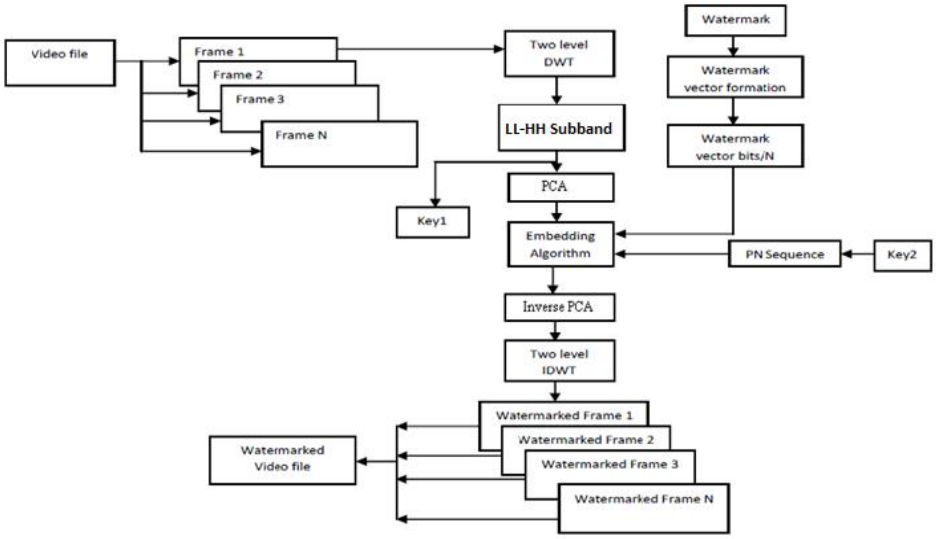

Fig 2: Watermark Embedding Block

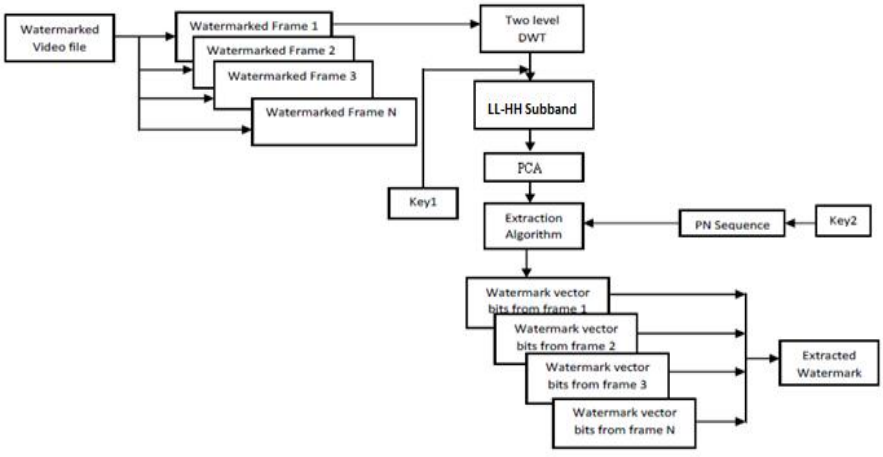

Fig 3: Watermark Extraction Block

III. Experimental Results

This scheme applies to a sample video sequence 'akiyo49.y4m' using a 32 × 32 binary watermark logo. The grayscale watermark is converted to binary before embedding. Fig. 4(a) and 4(b) show the original and the watermarked video frames respectively. Fig. 5(a) is the embedded watermark and Fig. 5(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.[10].

Fig.5 (a) Original Video frame

Fig.5 (b) Watermarked video (PSNR=38.4084)

Fig 6. (a) Original watermark

Fig 6. (b) Extracted binary watermark (LL NC = 0.94) (HH NC = 0.96)

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

$$\text{PSNR} = 10\log\frac{255^2}{\text{MSE}} \quad \text{..... (12)}$$

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

$$\text{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - I(i,j)]^2 \text{..... (13)}$$

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).

After several experiments, the PSNR values of nearly 100 watermarked frames of akiyo49 video are calculated then it gives an average PSNR value for all watermarked frames which is 37.2683 dB.

NC: The normalized coefficient (NC) gives a measure of the robustness of watermarking and its peak value is 1. The NC value gives the difference between the original watermark and extracted watermark.

The following images(Fig.7,Fig 8,Fig 9) represent diversity in values of PSNR and NC prescribed in Table 1, still taken from the watermarked video after the attacks:

Fig 7. Video frame after rotation by 60 degrees (matlab)

Fig 8. Video frame after addition of 'salt and pepper' noise

Fig 9.Video frame after addition of geometric attacks (matlab)

Table 1. Result Analysis

Attack	PSNR	NC
Rotation	27.825	0.6510
Salt and pepper	23.459	0.6548
Geometric Transform	40.0710	0.5313

Since we are using a nonblind hybrid watermarking scheme, we are able to rotate/resize the frame back to its original position/size after the rotation/resize attack.

IV. Conclusion and Future Work

In this watermarking scheme, the combination of PCA and DWT techniques achieve robustness and imperceptibility which results in high quality copyright protected video. Also the scheme is resistant against additive Gaussian noise attack, which can be seen from the NC values. With the help of AES algorithm, only authorized user can extract the watermark from video as well as all authentications, process details are encrypted. In future the degree of perfection can be increased in the watermark extraction procedure. This watermarking scheme can be tested for other newly emerging various noise attacks, JPEG compression (coding) etc. The quality of extracted watermark from video can be improved by using other effective methods like Hidden Markov Model (HMM), Support Vector machine (SVM) etc. Digital video watermarking can also be utilized for Labeling, Temper Proofing like applications.

Acknowledgement

It is our privilege to acknowledge with deep sense of gratitude to our project mentor, Prof.G.G.Chiddarwar for her valuable suggestions and guidance throughout our course of study and timely help given to us in the completion of our project titled, 'Video Watermarking scheme based on DWT and PCA for copyright protection'. We would like to dedicate this project to our parents without whose help and moral support it would not have been possible to complete this project.

References

[1] Salwa A.K Mostafa, A. S. Tolba ,F.M. Abdelkader, Hisham M. Elhindy, Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform ,*IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8*, August 2009.

[2] R. Reyes, C. Cruz, M. Nakano-Miyatake, Member IEEE and H. Perez-Meana, Senior Member IEEE, Digital Video Watermarking in DWT Domain Using Chaotic Mixtures, *IEEE Latin America Transactions, VOL. 8, NO. 3*, June 2010.

[3] Xiaoli Li, Student Member, IEEE, Sridhar (Sri) Krishnan, Senior Member, IEEE, and Ngok-Wah Ma, Senior Member, IEEE, A Wavelet-PCA-Based Fingerprinting Scheme for Peer-to-Peer Video File Sharing ,*IEEE Transactions on Information Forensics and Security, VOL. 5, NO. 3*, September 2010.

[4] Xiangui Kang, Jiwu Huang, Senior Member, IEEE, Yun Q. Shi, Senior Member, IEEE, and Yan Lin, A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression, *IEEE Transactions on Circuits and Systems for Video Technology, VOL. 13, NO. 8*, August 2003.

[5] Sanjana Sinha, Prajnat Bardhan, Swarnali Pramanick, Ankul Jagatramka, Dipak K. Kole, Aruna Chakraborty,Department of Computer Science & Engineering, St Thomas' College of Engineering and Technology, Kolkata, India, Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis, *International Journal of Wisdom Based Computing, Vol. 1 (2)*, August 2011.

[6] Nisreen I. Yassin1, Nancy M. Salem2, and Mohamed I. El Adawy National Research Centre, Cairo, Egypt, Block Based Video Watermarking Scheme Using Wavelet Transform and Principle Component Analysis , *IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3*, January 2012.

[7] S.K. Amirgholipour, A. R. Naghsh-Nilchi: Robust Digital Image Watermarking Based on Joint DWT-DCT, *International Journal of Digital Content Technology and its Applications Volume 3, Number 2, pp. 42-54*, June 2009.

[8] Martin Zlomek, Charles University in Prague, Faculty of Mathematics and Physics, Department of Software and Computer Science Education, Video Watermarking.

[9] M. Chandra, S. Pandey: A DWT Domain Visible Watermarking Techniques for Digital Images, *International Conference on Electronics and Information Engineering, pp. V2-421 - V2-427*, 2010.

[10] C.V. Serdean, M.A. Ambroze, M. Tomlinson and J.G. Wade, DWT Based Video Watermarking for Copyright Protection, Invariant to Geometrical Attacks, *Proceedings of the 3rd International Symposium on Communication Systems Networks and Digital Signal Processing – CSNDSP'02, Stafford, UK, 15-17*, July 2002.

[11] Angshumi Sarma, Dept. of Electronics & Communication Engineering IST, Gauhati University Guwahati, Assam, India,Amrita Ganguly, Dept. of Electrical Engineering Assam Engineering College Guwahati, Assam, India: An Entropy based Video Watermarking Scheme, *International Journal of Computer Applications (0975 – 8887) Volume 50 – No.7*, July 2012.

[12] S.-J. Kim, Suk-Hwan Lee, T.-S. Kim, B.-S. Kim, and K.-I. Lee, A Video Watermarking Using the Spread Spectrum Technique in the 3D Wavelet Transform Domain, *Proceedings of the International Conference on Imaging Science, Systems and Technology '04*, June 2004.

[13] Xin Y. and Pawlak M, M-ary Phase Modulation for Digital Watermarking, *International Journal of Applied Mathematics and Computer Science (AMCS'08), Vol. 18, No.1, pp. 93-104*,2008.