VIDEO WATERMARKING SCHEMES BASED ON DWT AND PCA ALGORITHM- A NOVEL APPROACH

R.S.Deshmukh
Department of Electronics and Telecommunication, RCOE, Mumbai-50

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

The popularity of digital video based applications is accompanied by the need for copyright protection to prevent illicit copying and distribution of digital video. Copyright protection inserts authentication data such as ownership information and logo in the digital media without affecting its perceptual quality. In case of any dispute, authentication data is extracted from the media can be used as an authoritative proof to prove the ownership. As a method of copyright protection, digital video
watermarking has recently emerged as a significant field of interest and a very active area of research. Watermarking is the process that embeds data called a watermark or digital signature into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. For the purpose of copyright protection digital watermarking techniques must meet the criteria of imperceptibility as well as robustness against all attacks for removal of the watermark. Many digital watermarking schemes have been proposed for still images and videos. Most of them operate on uncompressed videos, while others embed watermarks directly into compressed videos. Video watermarking introduces a number of issues not present in image watermarking. Due to inherent redundancy between video frames, video signals are highly susceptible to attacks such as frame averaging, frame dropping, frame swapping and statistical analysis. Video watermarking approaches can be classified into two main categories based on the method of hiding watermark bits in the host video. The two categories are: Spatial domain watermarking where embedding and detection of watermark are performed by directly manipulating the pixel intensity values of the video frame. Transform domain techniques, on the other hand, alter spatial pixel values of the host video according to a pre-determined transform and are more robust than spatial domain techniques since they disperse the watermark in the spatial domain of the video frame making it difficult to remove the watermark through malicious attacks like cropping, scaling, rotations and geometrical attacks. The commonly used transform domain techniques are Discrete Fourier Transform (DFT), the Discrete Cosine Transform (DCT), and the Discrete Wavelet Transform (DWT).

In this research paper, it was propose in the studies to imperceptible and robust video watermarking algorithm based on Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA). DWT is more computationally efficient 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 imperceptibly. 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 a more robust watermarking scheme that is resistant to almost all possible attacks. The watermark is embedded into the luminance component of the extracted frames as it is less sensitive to the human visual system (HVS).

The objectives of research work comprises as follows. Section II contains the watermarking scheme. Section III contains the experimental results and finally Section IV gives the conclusion.

II. DESIGN METHODOLOGY

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. So DWT was innovated which increased the robustness of the watermarking scheme. 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 un-coded video.

2.1 Algorithm

Algorithm 1: The PCA approach is applied to the transform coefficients of wavelet sub band SB\(\theta\) where \(\theta\) represents (LL or HH) as shown in the following steps:

Step 1: The wavelet sub band SB\(\theta\) 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\(\theta\)\(i\), SB\(\theta\)\(2\), SB\(\theta\)\(3\)… 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\(\theta\)\(3\)… 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 COi of the zero mean block Z is calculated as:

\[
COi = Zi ZiT
\] .......................... (1)

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

Method 1: for a vector block as Zi=EX (SB\(\theta\)\(i\) –mei).
Method 2: for 2D array block as \( Z_i = E(X \cdot (B \cdot \theta_i - m_{ei}) \). Where \( m_{ei} \) is the mean of block and \( E \) denotes expectation operation.

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

\[
CO_i \Phi = \lambda_i \Phi \\
\]………………………… (2)

Where \( \Phi \) is the matrix of eigenvectors and \( \lambda \) is the matrix of eigen values 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 \( \lambda_i = (\lambda_1, \lambda_2, \lambda_3 \ldots \lambda_{n}) \). \( \Phi \) vectors are sorted in descending order according to \( \lambda_i \), where \( (\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \ldots \geq \lambda_{n} \) or \( (\lambda_{nxn}) \). The matrix \( \Phi \) 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 \( \Phi \):

\[
PC_i = \Phi^T Z_i \\
\]…………………………… (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)

\[\text{Figure 3: Block layout of video watermark}\]

2.2 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:

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

### 2.3 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 \( n \times n \) 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 \( \text{BW} = \{bw1, bw2… bw32x32\} \) 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 \( \alpha_1 \) into the first principle component of each PC block \( \text{PCi} \). From equation (3), for the PC block \( \text{PC1, PC2, and PC3… PCk} \), we can define \( \text{PCi} = (\text{PC1 (1), PC2 (1), PC3 (1)… PCk (1))} \) and the embedding equation:

\[
\text{PCI}' = \text{PCI} + \alpha_1 \text{BW} \quad \text{.......................... (5)}
\]
Step 7: For HH band, use two pseudorandom sequences (PNS); ps0 and ps1 with different keys k1 and k2 to embed the watermark bit bw ‘0’ and ‘1’ respectively [12,13]. So, we can represent BWm as follows:

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

When bit bw = 0, embed ps0 with strength $\alpha_2$ to the mid-band coefficient of PC block PCi and when bit bw = 1, embed ps1 with strength $\alpha_2$ to the mid-band coefficients of PC block PCi. If PCB includes the mid-band coefficients then the embedding equation is:

$$PCB' = PCB + \alpha_2 BWm \quad \cdots \quad (7)$$

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.

Figure 4: Layout of watermark embedding
2.4 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 = {bw1, bw2… bw32x32} 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:

\[ BW' = \frac{(PCI' - PCI)}{\alpha_1} \quad \ldots \ldots \quad (8) \]

Step 7: For the HH band, re-generate the two (PNS) sequences p0 and p1 with the same keys k1 and k2 used in embedding. Afterwards, the (PNS) sequences are extracted from the mid-band coefficient of each PC block YB by:

\[ Wm' = \frac{(YB' - YB)}{\alpha_2} \quad \ldots \ldots \quad (9) \]

The embedded bits are estimated depending on the correlation value Corr between p0 and p1 and extracted sequences Wm' and a predefined threshold Thr as follows.

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:

\[ NC = \frac{\sum \sum BW'(i,j)BW'(j,i)}{\sqrt{\sum \sum BW'(i,j)^2} \sqrt{\sum \sum BW'(j,i)^2}} \quad \ldots \ldots \quad (11) \]
III. 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. 6 and 7 show the original and the watermarked video frames respectively. Fig. 8 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.

Figure 5: Layout of Watermark Extraction

Figure 6. Original video frame  Figure 7. Original watermark  Figure 8. Extracted Watermark
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:

\[ \text{PSNR}=10\log_{10} \frac{255^2}{\text{MSE}} \] ........................ (12)

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

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

**Figure 10: Salt and Pepper noise**  
**Figure 9: Frame after rotation 60degree**  
**Figure 11: Gaussian noise**

<table>
<thead>
<tr>
<th>Attack</th>
<th>PSNR</th>
<th>NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotation</td>
<td>27.825</td>
<td>0.6510</td>
</tr>
<tr>
<td>Salt and pepper</td>
<td>23.459</td>
<td>0.6548</td>
</tr>
<tr>
<td>Geometric Transform</td>
<td>40.0710</td>
<td>0.5313</td>
</tr>
</tbody>
</table>

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**

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.
REFERENCES


