ISSN : 2347-503X

Research Chronicler

International Multidisciplinary Research Journal

Vol II Issue III : March 2014

Editor-In-Chief

Prof. K. N. Shelke

www.research-chronicler.com

Research Chronicler

A Peer-Reviewed Refereed and Indexed International Multidisciplinary Research Journal

Volume II Issue III: March – 2014

CONTENTS

Digital Video Watermarking Using DWT and PCA in Encrypted Domain

Mr. Chaitanya V. Mahamuni
Dept. Electronics & Telecommunication Engineering, PHCET, Rasayani, (M.S.), India

Abstract

This paper presents a unique method for insertion of a binary logo watermark image in the sequence of video frames in the encrypted domain. The suggested method combines cryptography and steganography techniques to develop a highly secure and protected digital multimedia system. The cryptography scheme implemented encrypts the video by Advanced Encryption Standard (AES) which uses perceptual cipher. The watermarking scheme employed is a highly robust and imperceptible watermarking scheme which combines the two image transforms namely Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA).The combination of two image transforms have improved the efficiency of the watermarking algorithm. The experimental results show no visible difference between watermarked frames and original frames and show robustness against a wide range of attacks like rotation,transform1 i.e. salt and pepper noise addition and transform2 i.e. Gaussian noise addition.

Key Words: Advanced Encryption Standard, perceptual cipher, video watermarking, Discrete Wavelet Transform, Principal component Analysis

1. Introduction

In the world of network and technology, the digital multimedia systems and applications are increasing rapidly. The digital multimedia files used in the multimedia services consists of the data in the form of digital audio, video or text.

It becomes very important to ensure the security and ownership of the multimedia files when broadcasted over the web where a multiple numbers of users can access the file. This can be accomplished by using a technique known as “Data Encryption”.

The data encryption is a mechanism by means of which the information contained in the digital multimedia message can be restricted only to the intended users and the third party cannot obtain the information present in our message. This is possible because as soon as the message is digitized by the encoder, an encryption key which is a random signal i.e. a mathematical function (usually a pseudo random number) is multiplied with the digitized message, it generates a scrambled message which can be intercepted only if the decryption key is available with the person who has obtained the message by tapping the network connection.

The data becomes unreadable, invisible or unintelligible during transmission when it is encrypted as the content is scrambled. The owners of the digital multimedia products intend to preserve the market standard and dignity of the product designed by them. Any other party cannot illegally copy the original product and pirate it if the product is available across the web has some specific mark or identity of the owner that authenticates it and maintains a unique identity of it.

The watermarking techniques are employed by the owners of the digital multimedia product in order to protect the ownership and integrity of it.

Jayashree Nehete [1] proposed an encryption algorithm for MPEG videos using Advanced Encryption Standard (AES) to meet the real time requirements for video encryption. C. Narsimha [2] developed a fast and secure real time encryption algorithm with a better computational efficiency. The various factors like type of video, bit stream format, requirement of codec modification and the post encryption operations to be performed on the video influence the development of the encryption scheme used for the network security.

The recent trend in the watermarking is to combine an image transform with some feature extracting algorithm to improve the efficiency of watermarking algorithm. Salwa [3] proposed a novel technique to insert a binary logo watermark in the video frames. In this scheme, the original video is directly subjected to apply Discrete Wavelet Transform (DWT) followed by Principal Component Analysis (PCA).The challenge is to implement the same watermarking scheme to watermark the video which is encoded, encrypted and achieve the watermarking results same as obtained after watermarking the original video without encryption.

This paper proposes a unique method for insertion of binary logo watermark in the sequence of video frames in encrypted domain. The encryption scheme employs 128 bit AES algorithm and Discrete Cosine Transform (DCT). The design used selectively encrypts fixed length code words (FLC) in MPEG video bit streams under the control of perceptibility factors. The encrypted video is then watermarked by using a highly robust hybrid imperceptible video watermarking scheme which combines two image transforms namely DWT and Block based PCA. The combination of the two image transforms has improved the efficiency of the watermarking algorithm.

2. Video Encryption Using AES

In cryptography, the Advanced Encryption Standard (AES) is an encryption standard adopted by U.S government. The standard comprises three block ciphers AES-128, AES-192 and AES-256.The standard adopted from a larger collection is Rijndael. Each AES cipher has a 128-bit block size, with keys of 128, 192,256 bits respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES). AES is based on design principle known as substitution permutation network. It is compact in both software and hardware, is relatively easy to implement, and require less memory.AES has a fixed block size of 128 bits and key size 128, 192 or 256 bits. The fixed block size of 128 bits i.e. 16 bytes is achieved. AES operates on 4x4 arrays of bytes. Most of the AES calculations are performed in a specific finite field. The AES cipher specified a number of repetitions of transformations rounds that convert an input plain-text into the final output cipher text. Each round consists of several processing steps including the one which requires the encryption key. A set of reverse rounds are applied to transform the cipher text back into the original plain text using the same encryption key.

According to the MPEG standards, the following FLC data elements exist in an MPEG video bit stream , 4-byte start codes (000001xx-hexadecimal), all information present in various headers, sign bits of non-zero DC coefficients, differential DC coefficients in intra blocks, ESCAPE DCT coefficients, sign bits and residuals of motion vectors. To maintain the format- compliance to the MPEG standard after the encryption the first two types of data elements must not be encrypted. The last four Fixed Length Codeword (FLC) data elements are considered which are divided into three categories according to their contributions to the visual quality: intra DC coefficients, sign bits of non-intra DC coefficients, AC coefficients, ESCAPE DCT coefficients, sign bits and residuals of the motion vectors. There are three control factors psd, psr and pmv to control the visual quality and perceptibility in three different dimensions: the low resolution rough (spatial) view, the high resolution (spatial) details, and the temporal motions. The factor psr is the probability with which intra-DCT coefficients are encrypted, psr is the probability with which the sign bits of non zero DCT coefficients are encrypted and pmv is the probability with which sign bits and residuals of motion vectors are encrypted. The encryption of selected FLC data elements can be carried out with either a stream cipher or a block cipher. When a block cipher is used, the consecutive FLC data elements should be first concatenated together to form a longer bit stream and then each part of the longer bit stream is encrypted. The encrypted FLC data element is then placed back into the video stream. The block cipher and stream cipher are embedded securely in order to provide security against any cryptographic attacks. The video to be encrypted is selected from the popup menu and the maximum of frames comprised by the video is decided by the user. The visual quality of the encrypted video is controlled by setting the values of the perceptibility factors that are used. The psr value lies s and the decreasing value of psr signifies that spatial perceptibility changes from ‘almost imperceptible’ to ‘perfectly perceptible’. The value of psd lies in the range 0 to 1 and the decreasing value of psd means spatial perceptibility changes from ‘roughly perceptible’ to ‘perfectly perceptible’. From the decreasing value of pmv, we can interpret that temporal (motion) perceptibility changes from ‘almost perceptible’ to ‘perfectly perceptible’. The psr and psd variables are used to determine the quality scaling and pmv determines the value of coefficient quantization matrices i.e. whether intra quantization or inter quantization blocks to be used depending on the type of frame.

2.1 Algorithm for Video Encryption

The AES is a key iterated cipher. The algorithm used is same at the time of encryption and decryption side except at the time of decryption reverse operations are performed. The input to the cipher is one dimensional array of plain text which is converted into a state matrix for each round of the transformation round key is derived using cipher key and never specified directly. Each round transformation is composed of four different transformations such as ByteSub, ShiftRow, MixColumn and AddroundKey. The ByteSub is a non-linear byte transformation operating on each set of the state bytes independently. In ShiftRow, rows of the state are cyclically shifted over different offsets. In Mixed Column is every column is transformed by multiplying it with a specific multiplying polynomial. In AddRoundKey, round key is applied to the state by simple bitwise XOR operation and it is self-inverse.

MPEG video encryption aims to prevent the unauthorized users from decoding the programs by encrypting them with some new key. The general scheme is to apply an invertible transformation Ek1 to apply to the video stream S called plain text that produces a bit stream C called cipher text.

$$C = Ek1\ (S)$$

An authorized receiver who has the secret decryption key can decrypt the video by applying the transformation

$$Dk2 = Ek1$$

The decryption process is described as

$Dk2 = Ek1^{-1}(C) = Ek1^{-1}(Ek1(S)) = S.$

where k1 is called as encryption key and k2 is called as decryption key. The MPEG algorithm used is a selective algorithm which operates sign bits of DCT coefficients and motion vectors of the MPEG compressed video.

The AES encryption operation randomly changes the sign bit of the coefficients. Based on the secret used in the encryption, sign bit is either changed or unchanged Even if some of the coefficients are changed, these changes will propagate in most of inverse DCT (IDCT) coefficients while decoding. The algorithm achieves the goal of reducing and bounding its computation time by limiting the maximum no of bits selected. For those who have the secret key, they can decrypt the video file and the original video. The decryption function is same as that of encryption but the inverse operation is performed. The encryption and the decryption keys are same. For those who don't have the secret key, their codec will play quite different images from the original video, because most of the image pixels have been changed.

3. Watermarking Scheme Using DWT and PCA

Principal Component Analysis (PCA) is a mathematical procedure which uses an orthogonal transformation to convert a set of observations of possibly correlated variables into linearly uncorrelated values called as principal components depending upon the field of application. PCA is also known as Karhunen Loeve Transform (KLT Transform) or Hotteling Transform or Proper Orthogonal Decomposition (POD). It is a useful tool in exploratory data analysis and making predictive models. The advantage of PCA is high energy concentration and complete decorrelation which is suitable for data hiding. It is used as a tool in exploratory data analysis and to make predictive models.

3.1 Watermark Insertion Algorithm

The following steps are involved in watermark insertion algorithm.

1) The given video input file is divided into frames and then 2N x 2N RGB frames are converted into YUV components.

2) The luminance component 'Y' is taken and DWT is applied to it. The DWT transform uses Haar wavelets and decomposes the image in spatial domain into four spectral subbands namely LL, LH, HL and HH bands. This is known as spectral decomposition. The subbands LH and HL are overlapping spectral subbands so discard them. The LL and HH bands are selected for feature extraction and watermark insertion because they are non-overlapping spectral subbands and the following two reasons: LL band has transform coefficients with maximum energy and HH band offers excellent features for high frequency alteration.

3) The non-overlapping spectral subbands are converted into n x n non-overlapping blocks.

3.1.1 Application of PCA and Watermark Insertion In Ll Band (Method A)

1) Let $I\alpha$ be the wavelet subband where α represents either LL or HH spectral subband, the dimension of the wavelet subband being N x N.

2) Now a new variable k is defined as follows: $k = (N \times N) \div (n \times n)$

3) Then each block vector is defined as $I\alpha = (I\alpha 1, I\alpha 2, - - - - -, I\alpha k)$

4) Zero mean block Ai of each block is computed by using the equation

$$Ai = E\,(I\alpha i - mi)$$

where E represents mathematical expectation and mi is the mean of the block.

5) The co-variance matrix is calculated as follows : $C = Ai\, Ai'$.

6) The eigen vector (basis function) corresponding to each eigen value of the matrix is calculated as follows

$$Ci\, \mu = \lambda i\, \mu$$

where Ci is the matrix of eigen vectors and λi is the matrix of eigen values.

$\mu = (\, e1, e2, - - - ,e\, nxn\,)$

$\lambda i = (\, \lambda 1, \lambda 2,- - - - -, \lambda\, nxn\,)$

such that $\lambda 1 \geq \lambda 2 \geq \lambda 3 - - - - - - \geq \lambda n$.

7) The principal component of block i i.e. modified PCA is calculated by the following equation

$$Yi = \mu'\, Ai.$$

8) The inverse PCA is applied by the following equation $A = \mu\, Yi$.

9) Let β be the strengthening factor, W represents the watermark image then the watermark is inserted into the principal component of LL spectral subband to get modified PCA by using following equation

$$Y1' = Y1 + \beta\, W$$

10) Inverse PCA is applied to modified PCA and modified wavelet coefficients are obtained.

11) IDWT is applied to these wavelet coefficients and watermark luminance component is obtained and then the actual interpolation takes place.

3.1.2 Application of PCA and Watermark Insertion in Hh Band (Method B)

1) Let $I\alpha$ be the wavelet subband where α represents either LL or HH spectral subband, the dimension of the wavelet subband being N x N.

2) Now a new variable k is defined as follows: $k = (N \times N) \div (n \times n)$

3) Then each block can be defined as a 2D array as follows: $B\alpha = (B\alpha1, B\alpha2, - - - - -, B\alpha k)$

where the array represents block no I of size n x n.

4) Zero mean block Ai of each block is computed by using the equation

$$Ai = E\,(B\alpha i - mi)$$

where E represents mathematical expectation and mi is the mean of the block.

5) The co-variance matrix is calculated as follows : $C = Ai\, Ai'$.

6) The eigen vector (basis function) corresponding to each eigen value of the matrix is calculated as follows with the equation stated below:

$Ci\, \mu = \lambda i\, \mu$

where Ci is the matrix of eigen vectors and λi is the matrix of eigen values.

$\mu = (e1, e2, - - - - - ,e\ nxn)$

$\lambda i = (\lambda 1, \lambda 2,- - - - -, \lambda\ nxn)$

such that $\lambda 1 \geq \lambda 2 \geq \lambda 3 - - - - - - \geq \lambda n$.

7) The principal component of block i i.e. modified PCA is calculated by the following equation

$$Yi = \mu'\, Ai.$$

8) The inverse PCA is applied by the following equation $A = \mu\ Yi$.

9) The watermark image of dimension 32 x 32 is taken and it is converted into a vector as follows:

W = (W1, W2, W3, - - - - - -, W32x32).

10) In HH band, the watermark image is represented as Wm and defined as p0 or p1which are the pseudo random numbers for two different values of the watermark bit ‘w ‘.

$$Wm = p0 \text{ for } w=0$$
$$=p1 \text{ for } w=1$$

11) The watermark insertion equation for HH band is $Y1' = Y1 + \beta 2\ Wm$

where $\beta 2$ is the strengthening factor and $Y1'$ is the modified PCA .

12) Inverse PCA is applied to modified PCA and modified wavelet coefficients are obtained.

13) IDWT is applied to these wavelet coefficients and watermark luminance component is obtained and then the actual interpolation takes place.

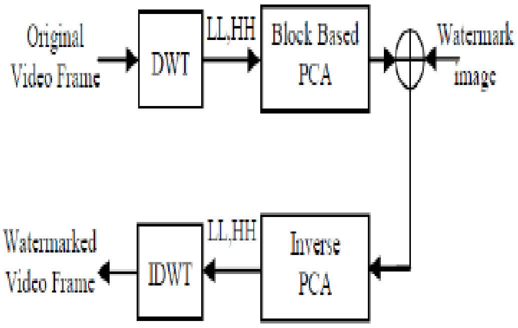

Fig.1: Watermark insertion algorithm

3.2 Watermark Extraction Algorithm

The following steps are involved in watermark insertion algorithm.

1) The watermarked (and may be attacked) video input file is divided into frames and then 2N x 2N RGB frames are converted into YUV components.

2) The luminance component ‘Y’s is taken and DWT is applied to it. The DWT transform uses Haar wavelets

and decomposes the image in spatial domain into four spectral subbands namely LL, LH, HL and HH bands. This is known as spectral decomposition. The subbands LH and HL are overlapping spectral subbands so discard them. The LL and HH bands are selected for feature extraction and watermark insertion because they are non-overlapping spectral subbands and the following two reasons: LL band has transform coefficients with maximum energy and HH band offers excellent features for high frequency alteration.

3) The non-overlapping spectral subbands are converted into n x n non-overlapping blocks.

4) Apply PCA to each block in the chosen subbands LL by using method A (see 3.1.1) and HH by method B (see 3.1.2)

5) The watermark image of dimension 32 x 32 is taken and it is converted into a vector as follows: W = (W1, W2, W3, - - - - - -, W32x32).

6) In LL band, the watermark image is extracted by the following equation:

$$W' = (Y1' - Y1) \div \beta 1$$

7) In HH band, the watermark image is represented by Wm^1 and extracted by the following equation

$$Wm' = (Yb' - Yb) \div \beta 2$$

The original image W is obtained by the correlation between the pseudo random numbers p0, p1 and predefined threshold Th as follows:

W = 0 if $cor(p0, Wm^1) > cor(p1, Wm^1)$ and $cor(p0, Wm^1) > Th$

W = 1 If $cor(p1, Wm^1) > cor(p0, Wm^1)$ And $cor(p1, Wm^1) > Th$.

8) The extraction fidelity of the extracted watermark is computed by the Normalized Correlation (NC) whose peak value is 1 and given by the formula vector as follows: W = (W1, W2, W3, - - - - - -, W32x32).

$$NC = \frac{\sum_i \sum_j W(i,j) \cdot W'(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2} \sqrt{\sum_i \sum_j W'(i,j)^2}}$$

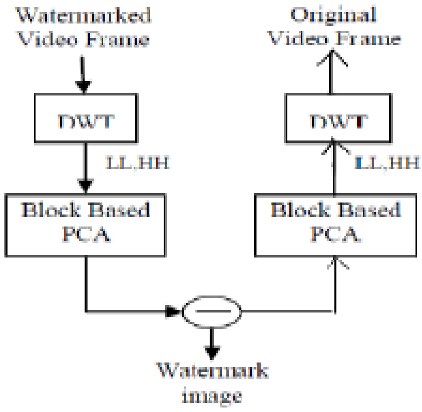

Fig.2: Watermark extraction algorithm

6) In LL band, the watermark image is extracted by the following equation:

$$W' = (Y1' - Y1) \div \beta 1$$

4. Project Implementation

The graphical user interface has been created in MATLAB7.9 to demonstrate the encryption technique and watermarking technique together as shown below:

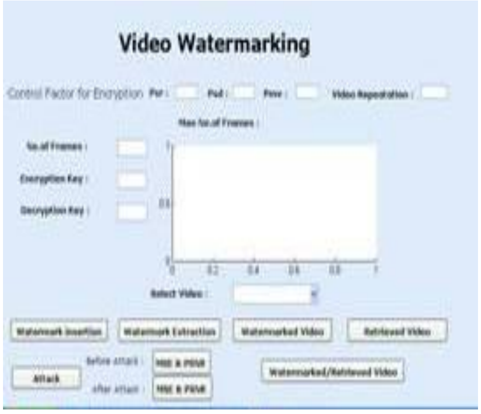

Fig.3:GUI created for demonstration.

The original video in GUI is as shown below:

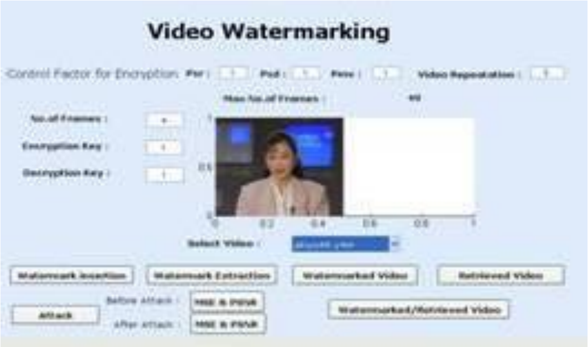

Fig.4: Original video in GUI.

The watermarked video and the retrieved video are as shown below

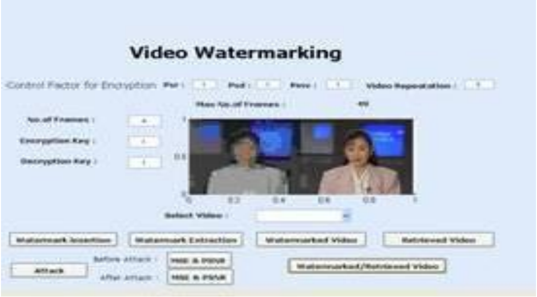

Fig.5: Watermarked & original video.

The original and extracted watermark is as shown below:

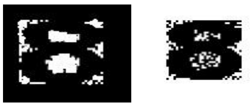

Fig.6: Original & extracted watermark.

Peak Signal-to-Noise Ratio, often abbreviated PSNR, is a common term that gives the ratio of the maximum possible power of a signal and the power of Peak Signal-to-Noise Ratio, often abbreviated PSNR, is a common term that gives the ratio of the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.

Mean Squared Error i.e. MSE is used to quantify the difference between the pixel values of the adjacent pixels of the image.

The graph of PSNR & MSE of the watermarked frames versus the no of video frames is as shown below:

1) PSNR in dB versus no of video frames:

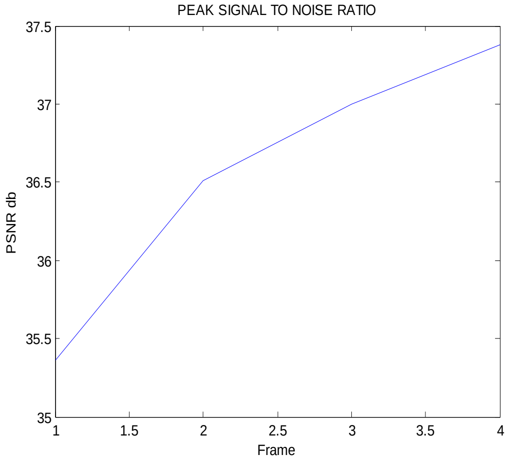

Fig.7: PSNR in dB versus no of video frames

The results show that as no number of video frames increases the PSNR of the value also increases. Thus to achieve a fair value of PSNR the no of frames selected should be considerably high.

2) MSE in dB versus no of video frames:

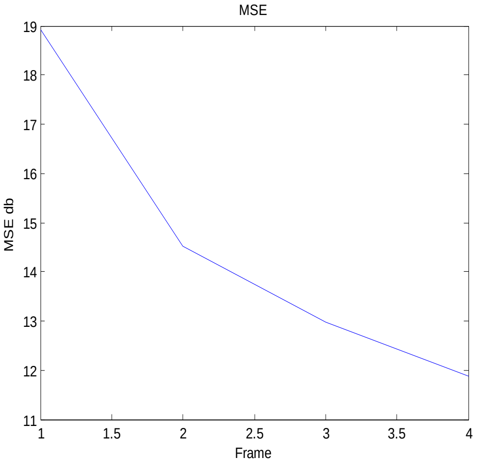

Fig.8: MSE in dB versus no of video frames.

Thus we see that the as the no of frames in the given input increases the MSE between the successive frames decreases. Hence to have minimum value of MSE between the successive frames of the video, the no of frames in the input video should be increased.

The results of PSNR and MSE of the watermarked video frames are used to test the efficiency of the watermarking algorithm employed in the paper. It is found that after watermarking the selected video using the watermarking algorithm the PSNR increases with the no of video frames. The maximum no of frames in the selected video, the PSNR will increase and thus a better visual quality of the watermarked frames. The decrease in MSE of the watermarked frame with increase in the number of frames of the video also indicates that the watermarking algorithm is highly effective robust and we get an optimum quality of the visibility in the watermarked video.

5. Experimental Result

The performance of the video watermarking scheme has been tested for different video inputs.

The performance has been evaluated in terms of imperceptibility and robustness against various attacks. The peak signal to noise ratio (PSNR) is used to measure the visual quality of the watermarked and attacked frame and is defined as

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

where MSE (Mean Square Error) between the original and distorted frames is defined as follows:

where m,n gives the size of the frame and I(i,j) and I(i,j) are the pixel values at the locations (i,j) of the original and the distorted frame. However, the robustness is measured by NC as stated above.

The various attacks like rotate, transform-1 i.e. addition of salt and pepper noise to the watermarked frame and transform-2 i.e. addition of white noise or Gaussian noise to the watermarked frame are performed on the watermarked video input file. The PSNR and MSE values are recorded before attack and after attack as shown below.

5.1 Result

1) Name of the video: akiyo49.y4m

2) Control factors for encryption: psr=1, psd=1, pmv=1.

3) Video repetition: 5

4) No of frames: 4

5) Maximum no of frames: 49

6. Encryption and decryption key: 1

Before attack:

1.) Encode time: 4 seconds

2) Decode time: 2 seconds

3) NC for LL band: 0.2023

4) NC for HH band: 0.5842

5) PSNR & MSE:

Frame no	PSNR	MSE
1	35.3618	18.9189
2	36.5113	14.5195
3	37.0010	12.9712
4	37.3802	11.8868
Average	36.5633	14.5741

Table.1: PSNR & MSE before attack

Results after attack no.1 i.e. rotation: 1.) Encode time: 4 seconds

2.) Decode time: 2 seconds

3.) NC for LL band: 0.2023

4.) NC for HH band: 0.5842

5.) PSNR & MSE:

Frame no	PSNR	MSE
1	2.6026	162.3604
2	2.5922	166.2919
3	2.5903	167.0345
4	2.5884	167.7569
Average	2.5933	167.1109

Table.2: PSNR & MSE after attack no.1

Results after attack no.2 i.e. Transform1:

1) Encode time: 4 seconds
2) Decode time: 2 seconds
3) NC for LL band: 0.2023
4) NC for HH band: 0.5842
5) PSNR & MSE:

Frame no	PSNR	MSE
1	35.3618	18.9189
2	36.5113	14.5195
3	37.0010	12.9712
4	37.3802	11.8868
Average	36.5637	14.5741

Table.3: PSNR & MSE after attack no.2

Results after attack no 3 i.e. Transform2:

1) Encode time: 1second
2) Decode time: 1 second
3) NC for LL band: 0.1949
4) NC for HH band: 0.6248
5) PSNR & MSE:

Frame no	PSNR	MSE
1	2.6026	162.3604
2	2.5922	166.2919
3	2.5903	167.0345
4	2.5884	167.7569
Average	2.5933	165.8609

Table.4: PSNR & MSE after attack no.3

Thus the video was encoded, encrypted and then watermarked. The various parameters related to the encryption scheme and the watermarking scheme employed by us were calculated and tabulated.

Various attacks like rotation, transform-1 and transform-2 were performed on the watermarked video frame and the various parameters related to the attacked frame were also calculated and tabulated.

The variations in the value of the error metrics like PSNR and MSE of the encrypted, watermarked video frame and attacked video frame can be studied with the help of the tabulated result.

Conclusion

The proposed scheme to insert a binary logo watermark in the sequence of the video frames was successfully implemented. The video input was successfully encrypted by using the encryption scheme based on 128-AES algorithm and DCT. The encrypted video was then watermarked by using watermarking algorithm based on DWT and PCA. The advantage of proposed watermarking algorithm is that since feature extracting algorithm i.e. PCA is applied on the spectral subbands after applying DWT, it is the most imperceptible watermarking algorithm.

Future Scope

The scope for future research is to develop an encryption algorithm which gives much better results for the post encryption operations to be performed on the encrypted video. The watermarking scheme can be improved further by finding the most suitable wavelet for given video sequence to enhance the robustness and imperceptibility of the implemented technique.

The list of tables and list of figures is as shown below.

LIST OF FIGURES

LIST OF TABLES

References

1. Jayashri Nehete, K. Bhagyalakshmi, M.B. Manjunath, Shashikanth Chaudhari, T.R. Rammohan, *A Real-Time Video Encryption using AES*", Central Research Laboratory, Bharat Electronics Ltd, Banglore-560013.

2. C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C.V. Jawahar, *Fast and Secure Real Time Encrytion*, International Institute of Information Technology, Hyderabad, India-500032.

3. Salwa, A.K. Mostafa, A.S.Tolba, F.M. Abdelkader, Hisham L Elhindy, 'Video Watermarking based on Principal Component Analysis and Wavelet transform." ICJNS *International Journal of Computer Science & Network Security*, Vol.9 No.8, August 2009.