International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Embedding with Pca Based Svd Framelet Transform with Visual Cryptography in Video

Maheswari.S, Reeba Korah

Abstract*: The goal of watermarking or steganography is not to restrict access to the original image, to ensure that embedded data remain recoverable. Digital watermarking is a technique providing embedded secure information in images, digital watermarking is the process of inserting data into an image in a way that it can be used to make an assertion about the image. But the proposed system studies a comprehensive approach of embedding secret information inside the video. A hybrid video steganographic scheme based on Framelet transform (FT) with Principal Component Analysis (PCA) is introduced. The main purpose of using PCA is to reduce correlation among wavelet coefficients from wavelet decomposition of each video frame. Using this decomposition, the secret message can be dispersed into the uncorrelated coefficients. Framelet transform helps to decompose video file into several frames. The secret message is embedded inside the principal components of low frequency wavelet coefficients. Achieving high bit rate data embedding is the main task. The proposed system is robust against numerous attacks like geometric attack, filtering, contrast adjustment. After embedding the secret information , (2,2_VSSS) as Visual cryptographic encryption is implemented to maintain the secrecy of this information against hackers.The main aim of this study is to obtain impercibility which is the human eye may not be able to detect differences between the original video and reconstructed image. Even after embedding, the quality of the stego image is good, which is proved by achieving better a PSNR value, and the stego image does not give much variation irrespective of different imaging conditions in the proposed VDWT mechanism. The proposed method achieves high PSNR than the existing methods, and nominal computational time is achieved for retrieving the secret information.

***Keywords* : Principal Component Analysis (PCA), Singular value decomposition(SVD),2,2 Visual secret sharing scheme (2,2_VSSS), Framelet Transform (FT)**

I. INTRODUCTION

Digital information science has emerged to seek answers to the question: can any technique ensure tamper-resistance and protect the copyright of digital contents by storing, transmitting and processing information encoded in systems. This chapter reviews the theoretical analysis and performance investigation of representative watermarking systems in transform domains and geometric invariant regions. Moreover, it is concluded that various attacks operators are used for the assessment of stegno systems, which supplies an automated and fair analysis of substantial other methods for chosen application areas.

Mostly digital Watermarking was used by the researchers which may be a technology used for the copyright protection of digital applications. During this study, a comprehensive approach for embedding secret information inside the digital video is introduced, and a hybrid digital video steganographic scheme based on Framelet Transform (FT) and Principal Component Analysis (PCA). PCA helps in reducing correlation among the wavelet coefficients obtained from wavelet decomposition of each video frame thereby dispersing the watermark bits into the uncorrelated coefficients. The video frames are first decomposing using FT and also the binary watermark is embedded in the principal components of the low frequency wavelet coefficients. An imperceptible high bit rate data embedded is robust against various attacks that will be carried out on the watermarked video, like filtering, geometric attacks and contrast adjustment. The main aim of this study is to obtain impercibility which is the human eye should not be able to detect differences between the stegno image and original image from the video frames.

II. RELATED WORK

Cryptography is defined as the science of writing secret code by ciphering and deciphering of the secret message. It is also the art of protecting the sensitive information. It is a mechanism of transforming the secret information from readable format to unreadable. Certain terminologies refer to cryptography are plain text, cipher text, encryption, and decryption. An art to defend useful information by altering it into an unreadable pattern is termed cipher text. Conversion of cipher text into plain text is called as deciphering which needs secret key. Deciphering is otherwise called as decryption. Certain unexpected codes break the encrypted message through cryptanalysis. However, the recent cryptography techniques are virtually unbreakable. Main application of cryptography extends to protect credit card information, corporate data and e-mail messages. Cryptography schemes can be widely classified into symmetric-key and public-key schemes. In Symmetric key scheme, the sender and recipient use a single key as a secret key. But the public-key systems use two different keys. A public key is known to everyone and the recipient uses only the private key.

Manuscript published on 30 September 2019.
*Correspondence Author(s)
Maheswari.S*, Research Scholar, Department of Electronics and Communication Engineering, Sathyabama University, Chennai, India.
Associate Professor, Department of Electronics and Communication Engineering, St.Joseph's College of Engineering, Chennai,India.
Dr.Reeba Korah, Professor, Alliance University, Bangalore, India

Visual Cryptography (VC) is one of the cryptographic techniques used for encrypting the images. It is done by classifying the ordinary image into unknown transparencies. These transparencies can be sent to the other end determined person. At the other end, the received transparencies have undergone decryption to get the original image. Using this Visual technology, the end user recognises an image in the incorrect form. While transmission itself, VC algorithm can encrypt the image. Here the sender obtains two or more transparencies of the original image. The encrypted transparencies can be stored and sent to the other intended person by other means.

Zhi Zhou (2006) has discussed about the VC encoding. Visual cryptography encodes single binary image into different. These shares are defined by random binary patterns. The basic sharing scheme explained by Naor and Shamir's for encoding a binary pixel into two shares as shown as an example in Figure 2.4.

A subset of transparencies has superposed may called as deciphering. If the shares are xeroxed onto transparencies, the recovery of original image is only obtained. But no secret information can be obtained and these shares also have no meaning visually. A technique named halftone visual cryptography is proposed by the author. This is suggested by the author so that visual cryptography can be achieved via halftoning. The principle with blue-noise dithering has proposed to encode binary images by Zhi et al (2006). It uses cluster algorithm which gives encoded half tone shares. All the shares carry significant information. Visual cryptography can be used in a number of applications as a category of secret sharing scheme which includes access control. Two-out-of-three threshold scheme can insisted for encoding.

III. EMBEDDING USING PCA BASED SVD FRAMELET TRANSFORM

Initially the standard video from the internet is chosen as input video and this video is divided into frames. Sample RGB frames of this input video are first converted into YUV plane frames. From each sample frame, only the luminance component has chosen here for Framelet transform. Framelet transform is implemented on frame for obtaining four sub bands. The different levels of sub bands are obtained which are LL (Low low), LH (Low high), HL (High low) and HH (High high).Again these sub bands are sub divided into different blocks. The covariance matrix calculation is executed for each block. Each block has undergone Principal Component Analysis (PCA) transformation to obtain PCA components.

Figure 3.1 shows Flow diagram of Video Embedding process through skin tone detection

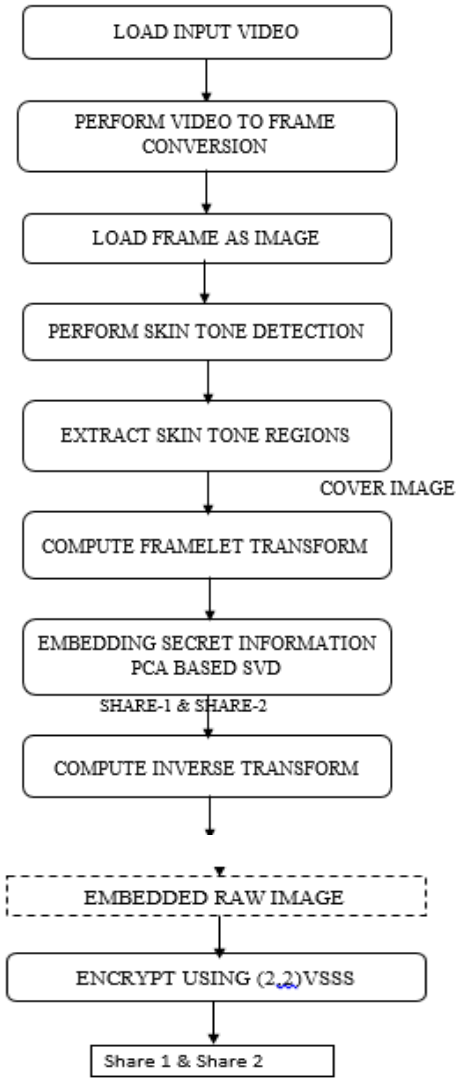


Figure 3.1 Flow diagram of Video Embedding process through skin tone detection

An image size either 20*50 or 100*120 is chosen as secret image. This secret image is embedded inside the frames based on PCA SVD technique. RGB secret color image is converted into binary image as a preprocessing step. Here the entire binary secret image is translated into vector zeros and ones using VDWT. These region vector is termed as Ψ. Further, this vector is subdivided into four separate regions (R1,R2,R3 and R4). These four regions of secret image are embedded inside the four decided sub bands. The whole embedding process is named as PCA based SVD FT. After embedding, inverse Framelet transform is applied to get the embedded raw image. The embedded raw image has undergone Visual cryptographic encryption technique as (2, 2_VSSS) discussed in chapter 6 for achieving security of the secret information. This secret sharing scheme takes an embedded image which has been segregated into two shares (Share 1 and share 2). Moreover ,a raw image has undergone various attacks namely Gaussian noise, image cropping and Image resizing attack. Hence the assessment of stego system is analyzed clearly and efficiently.

A Algorithm for Embedding and Extraction of information using PCA Based SVD Framelet Transform

Step 1: Video Acquisition using Frame converser system is processed for embedding.
Step 2: Video to Frame conversion is to be achieved.
- Read all video frames
- Get the number of frames

Step 3: Create a movie structure from the video frames.
Step 4: Load the frames as an image
Step 5: Resize an image based on the video's width and height
Step 6: Obtain an image using skin tone detection which can be used as a cover object.
Step 7: Perform frequency Transformation using Framelet transform.
Step 8: Embed the secret information into the cover image using PCA based SVD FT.
Step 9: Perform Inverse transformation.
Step 10: Obtain the embedded raw image.
Step 11: Resize figure based on the video's width and height
Step 12: Encrypt the image using (2,2 _VSSS)
Step 12: The secret message is recovering from cover object.
Step 13: Reconstruct the video from video frames after decryption.

B Extraction Process

Here the stego video is first divided into frames and obtain YUV plane frames from RGB plane frame. Then the luminance component of each frame is chosen to apply Framelet Transform. The resulting different four sub bands from FT are subdivided into various blocks. PCA is applied on each block and then covariance matrix is calculated for each block. Then each block has undergone transformation to get PCA components. On the other hand the same RGB stego image is converted into a binary image. This binary image is translated into a vector of zeros and ones using VDWT. Further, this vector is subdivided into four separate regions (R1, R2, R3 and R4).The four sub bands are embedded inside these regions. Inverse PCA is applied on the modified sub bands to obtain the modified wavelet block. The luminance components of the frames are obtained through the application of inverse Framelet transform. The original video is obtained finally by converting YUV frames to RGB frames.

IV. PERFORMANCE EVALUATION

Samples of results acquired for foreman video are depicted in Figure 3.2. Where (a) represents an image has undergone frame conversion from the loaded foreman video. One of the frame has been chosen has undergone skin tone detection using heuristic thresholding.Hence identified skin regions from the video frame as shown in figure3.2 (b).(c) represents an image after extracting skin regions alone.

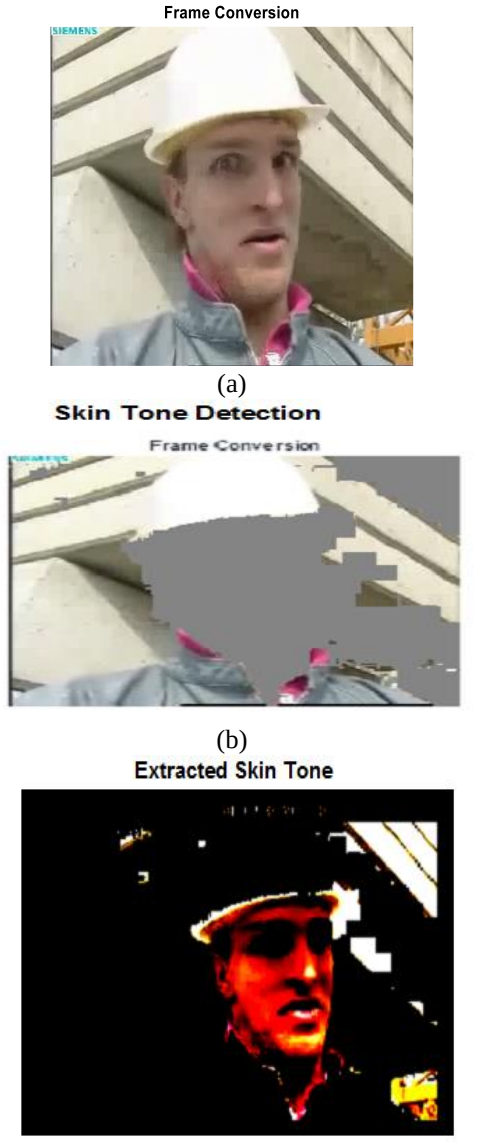
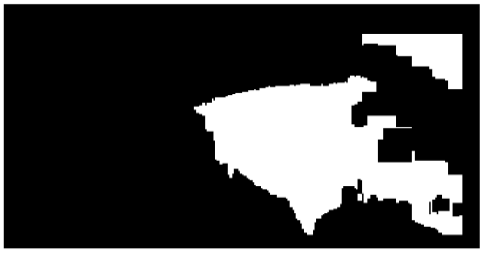


Figure 3.2 Video steganography Using PCA based SVD FT (a) Image after frame conversion from the loaded foreman video (b)Sin tone detection using heuristic thresholding (C) Extracted skin tone regions

The secret information like logo is ready to hide behind the identified and extracted skin regions as cover image shown in Figure 3.2 (d) Cropped Skin regions as cover object , (e) represents an enhanced embedded raw image and (f) is the filtered image of embedded image using Gaussian filter to reduce the noises.



(d)

(e)

(f)

Figure 3.2 Video steganography Using PCA based SVD FT (d) Cover image (e) Embedded raw image (f) Filtered image

Moreover, it has undergone various attacks like Gaussian noise, Speckle noise, Image cropping and Image resizing attack are used for the assessment of stegno systems, which supplies an automated and fair analysis of substantial other methods for chosen application areas.

Generally the Gaussian noise attack is made to check the resistance.Image with Gaussian noise attack (Attack 1) is shown in Figure 3.3(a). The speckle noise attack (Attack 2)is also made to check the resistance which is in Figure 3.3 (b). The attack (Attack 3)after cropping of the image and the attack (Attack 4)after image is being resized which has shown in the Figure 3.3 (c) and (d) respectively.

(a)

(b)

(c)

(d)

Figure 3.3 Output image against various attacks (a) Gaussian noise- Attack 1 (b) Speckle Noise- Attack 2 (c) Image Cropping- Attack 3 (d) Image Resizing –Attack 4.

The video is reconstucted from frames to a video is shown in Figure 3.4.

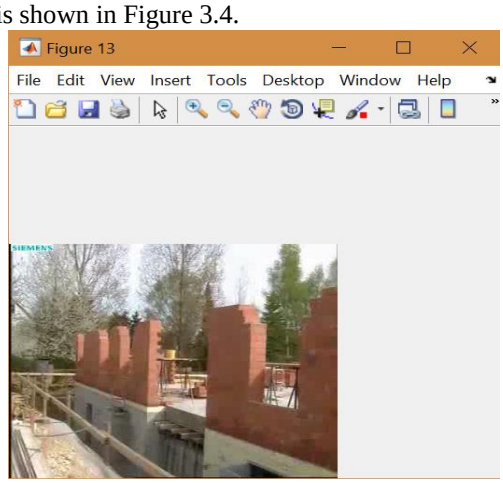


Figure 3.4 Reconstructed video

The computational time taken by the algorithm for hiding the secret information is 33.0313 and the time taken to recover the secret image is 7.4063.According to our knowledge, this technique recovers the secret image with low computational time. Figure 3.5 gives the PSNR value comparison between the image without attack and with attacks like Attack 1 to Attack 4.

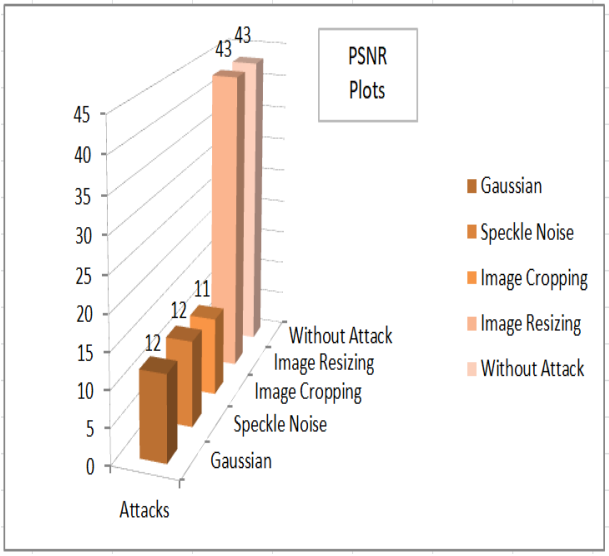


Figure 3.5 PSNR Comparison chart between with attacks and without attack

A kind of mathematical measure of image quality is obtained based on the pixel difference between two images. It is a quality estimation of Stego image obtained from converted frames compared with a cover frame. PSNR is calculated by using equation (3.1) whereas MSE stands for mean square error. The maximum possible pixel value of the image is taken as 255. If the PSNR value is greater than 36 DB then good visibility of Stego image is obtained like that of the cover image.

$$PSNR = 10 * \log_{10} \left(\frac{255^2}{MSE}\right) \text{ ------- (3.1)}$$

The equation (3.2) is used to calculate MSE which is computed by averaging the squared intensity of the cover and Stego image pixels.

$$MSE = \frac{1}{(M*N)} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - Y_{ij})^2 \text{ ------- (3.2)}$$

Similarly, the measure of getting perceptual similarity between images before and after stego processing is nothing but Image fidelity. Table 3.1 shows the performance measures like PSNR, Image fidelity and computational time of embedding and recovering process. Table 3.2 shows the comparative analysis of proposed method and existing methods.

Table 3.1 Quality measures of proposed PCA SVD FT Embedding

Embedding techniques	Payload	CT of Embedding Process	CT of Extraction Process	Image fidelity	PSNR
Proposed method using PCA Based SVD (Singular Value Decomposition) Framelet Transform	Handwritten Document (100*120)	33.0313	7.4063	0.995	43.52

Table 3.2 Comparison of proposed PCA SVD FT Embedding with Existing approach

Embedding techniques	Payload	Image Fidelity	Average PSNR
Proposed method using PCA Based SVD (Singular Value decomposition) Framelet Transform	Handwritten Document (120*120)	0.995	43.52
Video Steganography using LSB[5]	Binary Information	0.856	38.5
video steganography using LSB[7]	DNA alphabets	0.522	31.25

Figure 3.6. shows the outcome of encryption and decryption process. The embedded raw image has undergone Visual cryptographic encryption technique for more secured transmission of secret information. Using Lagrange permutation, embedded image is divided into two shares which are Share 1 and share 2.(Figure 3.6 (b) and(c) respectively).Finally the decrypted image is obtained by inverse PCA based SVD algorithm.

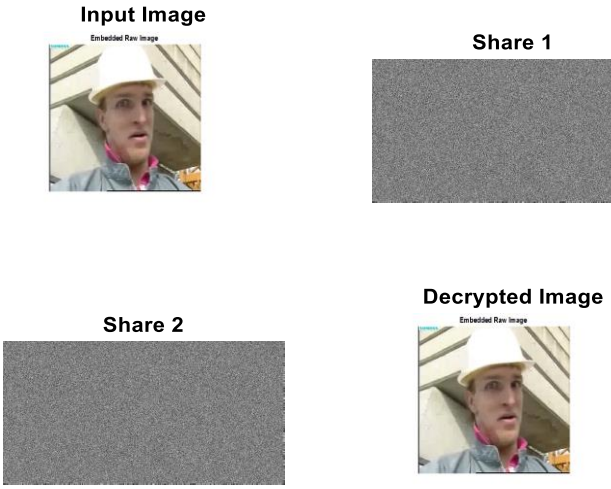


Figure 3.6 Outcome of Visual cryptography (2,2_VSSS) technique(a) Embedded raw image as input (b) Share1 (c) Share 2 (d)

V. CONCLUSION

We conclude that the goal of video steganography is to embed the secret handwritten document based on PCA SVD FT. The confidential document is communicated to the other end in highly secured manner based on (2,2 _VSS) scheme. The researcher has done a complete survey on the current watermarking and steganographic techniques. According to our knowledge, this stego system is the enhanced method of combining video steganographic and cryptology. This research work extends to implement embedding through skin tone detection in videos. This system is implemented based on transform domain as well as geometric invariant regions. This chapter deals with hiding the confidential data like handwritten documents or logo inside the video file. Existing systems concentrated on watermarking techniques in which watermarks are easily detected. Moreover those systems may not concentrate on invisible embedding / hiding the confidential data inside the videos. Steganographic techniques are popular and efficient than the watermarking techniques. Then PCA FT SVD video steganography method is proposed. For secure communication (2 ,2 _VSS) scheme is proposed.

Now a day, the digital media/information may be distributed easier and faster due to the extensive and rapid growth of network technologies. Due to insufficient cognizance issue multimedia content protection has become a major issue in recent days. More than watermarking, proposed and combined steganographic and crypto system may be one of the possible methods to protect the digital information or handwritten documents efficiently. 33.0313 seconds as Computation time for executing embedding of secret information and 7.4063seconds for recovering the same information are obtained by the proposed algorithm

REFERENCES

1. 1.Hemalatha S, “Wavelet transform based steganography technique to hide audio signals in image”.Science Direct, Procedia Computer Science 47 (2015) 272 – 281
2. Babloo Saha and Shuchi Sharma, “ Steganographic Techniques of Data Hiding using Digital Images”, Defence Science Journal, Vol. 62, No. 1, January 2012
3. Abbas Cheddad, “Digital Image Steganography: Survey and Analyses of Current Methods”, Signal processing, volume 90,Issue 3 ,March 2010,pages 727-752
4. Mansi S. Subhedara, Vijay H. Mankarb, “Current status and key issues in image steganography: A survey “computer science review 2014.
5. 5.S.A. El_Rahman, A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information, Computers and Electrical Engineering(2016) http://dx.doi.org/ 10.1016/j.compeleceng.2016.09.001
6. Junlan Bai a, Chin-Chen Chang b, Thai-Son Nguyen c, Ce Zhu a, Yanjun Liu b, A high payload steganographic algorithm based on edge detection, http: // dx.doi.org/ 10.1016/j.displa.2016.12.004, Displays 46 (2017) 42–51
7. Marwa M. Emam, An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 3, 2016
8. 8. N.F. Johnson, Z. Duric, S. Jajodia, Information Hiding: Steganography and Watermarking-Attacks and Countermeasures, Kluwer Academic Publishers,Boston, MA, 2001.
9. Mritha Ramalingam , Nor Ashidi Mat Isa, A data-hiding technique using scene-change detection for video steganography, Computers and Electrical Engineering, http dx.doi.org /10.1016 / j.compeleceng.2015.10.005
10. 10.M. Indra Sena Reddy, Dr. A.P. Siva Kumar,Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm, International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science 85 (2016) 62 – 69
11. Yu.-Yuan. Chen, Hsiang.-Kuang. Pan, Yu.-Chee. Tseng, "A Secure Data Hiding Scheme for Two-Color Images", *Proc. IEEE Symp. Computers and Comm.*, 2000.
12. Amlan Karmakar a, Amit Phadikar a, Baisakhi Sur Phadikar b, Goutam Kr. Maity, A blind video watermarking scheme resistant to rotation and collusion attacks, Journal of King Saud University –Computer and Information Sciences (2016) 28, 199–210

AUTHORS PROFILE

S. Maheswari, received her Bachelor’s degree in Electronics and Communication Engineering from Bharathidasan University. She received her Master’s degree in Applied Electronics from Sathyabama University, Chennai. She is currently working as an Associate Professor in the Department of Electronics and Communication Engineering, St Joseph’s College of Engineering Chennai. Her research area is Information hiding with secured Visual cryptography. Her areas of interest include Skin tone detection, Steganography, and Visual cryptography. She has published 6 papers in International Journal, 2 paper in International Conference.

Dr. Reeba Korah heads the Department of Electronics and Communication Engineering. She has a vast experience of over 24 years in the field of engineering, academics, administration and active research. She has about 40 research publications to her credit in reputed international journals and conference proceedings. She has authored five books pertaining to electronics engineering. Dr. Korah serves as a doctoral level research supervisor in Anna University and Sathyabama University, Chennai.

.