ROBUST VIDEO STEGANOGRAPHIC MODEL FOR BANKING APPLICATION BY CASCADING THE FEATURES OF SVD AND DWT.

BOOPATHY. R[1]*, RAMAKRISHNAN. M. [2], VICTOR. S.P [3]

[1].Research Scholar, Manonmaniam Sundaranar University,Thirunelveli;
[2]. Head of the Department of Information Tech.Velammal Engineering College, Chennai:
3. Associate Professor& Head .Dept.of Computer Science,St.Xavier College, Pallayamkottai.
*Corresponding author E-mail: boopathyr123@gmail.com

ABSTRACT

Secret communication is attained by Steganography. Imperceptibility and Robustness are the two main imperative components of Steganography. This paper presents a new combined approach to improve the imperceptibility and robustness by cascading the features of Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT). This proposed method show the effective usage of DWT and SVD for hiding the already encrypted secret text message which adds as another layer of security. The frame separation is done and 2D-DWT is applied on desired frames, we have chosen lower resolution approximation image (LL sub band) as well as (HL, LH) detail components for SVD transformation and embedding, low frequency approximate coefficients are properly used in this method which is different from other conventional methods. Results proved that original message is extracted without any loss and minimum distortion is noticed in the reconstructed video. High capacity is accomplished by taking the video and converting into frames for embedding. The Experimental results show that the proposed method is robust against various noise addictive attacks including Salt & Pepper noise, average PSNR and NC values are also maintained as 77db and 0.999 respectively for all the frames, it is noticed that the original and disturbed frames are almost identical. Finally comparison of the proposed method with other existing methods has been carried out.

Keywords: *DWT, LSB, Steganography, SVD, Wavelet decomposition*

1. INTRODUCTION

Research in information hiding has blossomed during the past decade. Cryptography, Watermarking, and Steganography are the techniques that are mainly used for information security. (Chang and Kieu, 2010).Cryptography may attract the attention of interceptors so other data hiding techniques are evolved. Digital watermarking is used for copyright protection. Watermarking is mainly focused on how to avoid the illegal copies or piracy whereas steganography is used for covert communications. Extensive research has been carried out by combining Cryptography and steganography[1]. In general Watermarking [2] usually alters the cover image to embed the owner's identifier; Steganography is exclusively used for secret communications. The major difference between these two is mainly in their goals and applications. Many information hiding techniques are based on DCT quantization [3] in which they have used RSA algorithm and digital signature. Some categories of adaptive steganography methods can be easily detected by steganalysis methods [4].

Robustness against geometric distortion is one of the crucial important issues in watermarking/steganography. The major issues in steganography apart from robustness are capacity and imperceptibility. A new singular value decomposition-discrete wavelet transform (SVD-DWT) composite image steganography algorithm is proposed in this paper to address some of the weakness in sending the secret text message. Banking transactions normally use mobile phone as medium to send the pin code, one time password and etc for fund transfer or any other transactions. Normal way of sending the secret code may be hacked. In that case if we hide the secret pin number or secret message inside the image/frame it will not bring the attention of eavesdroppers. This paper is designed to handle the secret way of sending passwords for banking transactions. We have used video as cover object and video is converted into frames .The random frames selected for the process is transformed into DWT domain using Haar Wavelet transform with desired level of decomposition, we obtained four different frequency images(LL,HL,LH,HH). Apply SVD to LL, HL, LH planes. Secret text message is first encrypted by our previous work [5] and then embedded in LL planes using LSB algorithm, additional information is also embedded in HL and LH planes to divert the attention of hackers .This is distinct from traditional viewpoint that assumes data hiding should be embeds in low or middle frequency to have good robustness. To improve imperceptibility performance we use combination of two transforms such as DWT along with SVD is called combined new approach of steganography It can combine the features of discrete wavelet transforms and singular value decomposition. Embedding Capacity is also determined by equation – (1). (Desoky, 2009)[6,7]

$$C= \frac{\text{bits of secret message}}{\text{bits of stego cover}} \qquad (1)$$

Mean Square Error(MSE), Peak signal to noise ratio (PSNR) and Normalized correlation (NC) are calculated to measure the quality of the original frame and stegoframe. Our experimental Results proved that the quality of the Stego frame is maintained with the average value of 77dB. Robustness of proposed algorithm is tested for various attacks including salt and pepper noise, Gaussian noise, Rotation, Scaling, cropping, and histogram equalization.

Our major contributions in this paper

(1) *Survey*: We have done survey on current watermarking and steganography methods .It is found that most of the schemes have their weakness against statistical attacks.

(2) *Capacity, Imperceptibility and Robustness*: The proposed video Steganography method shows good capacity by deploying random video frames for hiding message. The Results proved that by cascading the features of SVD and DWT the improved security and robustness against the attacks are achieved.

(3)*Effectiveness*: The Secret text data is encrypted by our previous work [5] and embedded in LL planes, but the additional information is embedded in other planes to divert the hackers. We have used LSB algorithm for embedding and embedding capacity is also predetermined .The original message can be retrieved by only the intended receiver.

2. RELATED WORK

Two types of transformations are used here namely Discrete wavelet transforms (DWT) and Singular value decomposition (SVD).

2.1. The Discrete Wavelet Transform (DWT)

Discrete wavelet transform (dwt), transforms a discrete time signal to a discrete wavelet representation. The 2-D DWT for image is given in Figure1.

- DWT converts the input series x0, x1, …..xm, into one high-pass and low-pass wavelet coefficient series (of length n/2 each) given by:

$$H_i = \sum_{m=0}^{k-1} X_{2i-m} .s_m(z) \qquad (2)$$

$$L_i = \sum_{m=0}^{k-1} X_{2i-m} .t_m(z) \qquad (3)$$

- Where sm(z) and tm(z) are the wavelet filters, and k indicates the distance end to end of the filter, i=0 to [n/2]-1.

- We use such transformation recursively on the low-pass series until we get the desired number of iterations.

ADVANTAGES OF DWT OVER DCT

- While using DWT no need to divide the input coding into non-overlapping 2-d blocks, it has higher compression ratios avoid blocking artifacts.
- Localization is achieved both in time and spatial frequency domain.
- Transformation of the whole image→ introduces inherent scaling
- Having higher flexibility: wavelet function can be freely chosen

- Better identification of which data is relevant to human perception→ higher compression ratio (64:1 vs. 500:1)

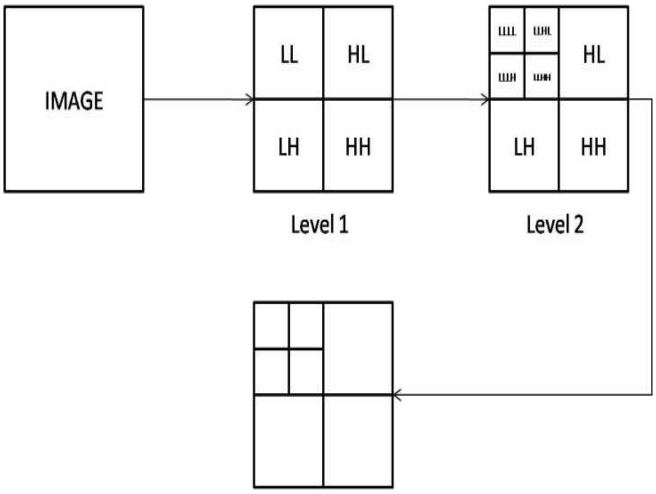


Figure.1 : 2-D DWT For Image

2.2. Singular Value Decomposition (SVD)

A technique which has many practical applications, one such application is applying SVD to compress an image by extracting and storing "enough" significant data about the matrix in the compressed file. So the unruffled thing about SVD algorithm is it does not depend on the fixed level of compression provided by other methods such as JPEG or gif compression, but we have chosen how much coded information that is needed to store in order to recover an "approximate" image. This method is mainly useful for image transmission over distances where the receiver is able to request information as required to rebuild an "acceptable" image. There may be a number of variations of the SVD decomposition by applying the SVD method [8] to the whole image or to various blocks sizes of the image. The basic idea in SVD compression algorithm is to signify an image as an m x n matrix, let it be A, by decomposition of the matrix A we get A= USVT where U is an m x n orthogonal matrix and V is an n x n orthogonal matrix. S is a diagonal matrix such that S = diagonal (s1 , s2, s3 , ..., sk , 0, 0, ..0) where si's are the singular values of A and are in descending order.

We have performed complete survey on existing methods to understand the work carried out on image steganography and watermarking methods based on DCT,DWT and SVD Esra satir, Hakan Isik (2012) proposed a compression based text steganography method to improve the capacity and security issues .they used textual data in steganography so the data compression algorithm is to be lossless. Hence they chosen LZW data compression algorithm .the advantage of their algorithm is not being language specific. Second advantage of the algorithm is protecting the originality of the cover media. In [9] high capacity blind information hiding schemes using tchebichef moments by Elshoura and Megherbi in (2010) gives basic idea about the geometric attacks on the watermarked images such as compression, rotation, cropping and also gives the basic idea for detection of peak signal to noise ratio (PSNR) and accuracy rate.

In [10] the authors suggest a method of non blind transform domain watermarking based on DWT-DCT-SVD. In this paper DCT coefficients of the DWT Coefficients are used for hiding the watermark. The authors concluded that DCT-SVD based method is very time consuming because it offers better capacity and imperceptibility. DWT-SVD is almost similar to DCT-SVD so they suggested a new method that was robust against different attacks. In [11] an efficient approach to still image copy detection based on SVD and block partition for digital forensics by Xiao Bing Kang and Sheng Min Wei in 2009 gives the basic idea about the singular value decomposition for digital images in which images are considered as matrices and then separate the singular values finally add watermark according to the singular values separation of original images, extracted watermark is tested under various parameters such as peak signal to noise ratio (PSNR) and accuracy rate (AR). Thus SVD is motivated to improve the robustness and discriminability of images.

In [12] authors projected a adaptive steganogrpahy to improve the embedding capacity that is decided by local complexity of the cover image, authors determined pixel classification into three levels based on boundary values .In [13] authors proposed data hiding scheme that is using complementary hiding method, they use to embed one secret bit both horizontally and vertically into the cover pixel by decreasing the odd value pixel and increasing the even value pixel by one, this method is very simple and it uses additions and subtractions. In [14] authors present a data hiding method by using intra prediction modes, usually intra prediction modes are divided into four groups consists of modes of closed prediction directions, by this method they have improved hiding capacity and encoding and decoding times are preserved. By applying modifications between the same groups of different modes secret data is embedded . Embedding the data in video codec H.264/AVC video quality has been preserved and also encoding and decoding time is maintained. Boosted steganography (BSS) method for increasing the undetectability of stego_images is introduced in[15], preprocessing methods on cover image is done , authors suggested that existing methods used to increase the embedding capacity may reduces the detection risk of stego images.BSS method has the own flexibility for the steganographer to select the cover images from the databases to increase the security and embedding capacity. In [16] Video steganography is done by concentrating internal dynamics of video compression , based on the work of Fridrich et al's they have introduced technique called Perturbed motion estimation. In[17] Information has been hidden and recovered from images using chaotic approaches but secret key is needed In [18] OSAMA S.FARAGALLAH designed a video watermarking based on Singular Value Decomposition performed in DWT domain, an error correction code is applied and embeds the watermark with spatial and temporal redundancy, here high and middle frequency bands used for SVD transformation and watermark is embedded. This method proves that when DWT is combined with SVD method watermarking method outperforms the conventional DWT methods with respect to robustness to scaling, rotation compression and cropping attacks. The Watermark is protected against bit errors and obtains excellent perceptual quality. In [19] the authors present a data hiding technique that exploits a decomposition representation of the data instead of frequency based transformations of the data, by using singular value decomposition the authors discussed the usage of orthogonal matrices in the SVD as a vessel to embed the information. perhaps not addressed the undetectability and robustness. In [20] the authors discussed that compression is the process of minimizing the size in bytes without degrading the quality of image, by conducting several experiments the authors concluded that DWT gives higher compression ratio than DCT and also avoids blocking artifacts, and proved that DCT is time consuming.

3.1. Implementation Of DWT-SVD Scheme For Steganography

The proposed DWT-SVD scheme for steganography is formulated as per Figure 2 and procedure for the same is described here.In the proposed DWT-based SVD video steganogrphic method, the original video is divided into frames. The encrypted secret text message is embedded in the SVs(S matrix) of selected wavelet approximate coefficients as well as detail coefficients. The wavelet decomposition of the every frame of the original video is done using the 2D-DWT. SVD is performed on selected wavelet approximate as well as detail coefficient for each video frame selected. Later these SV matrices are used to reconstruct the stego video. We have chosen a Haar Wavelet decomposition using L=2.The secret text message which is encrypted is embedded in the LL, LH,HL and sub-bands. The original secret message is embedded only in the SVD transformed approximate coefficients; the other planes are also used for hiding the undesired message to digress the attention of eavesdroppers.

EMBEDDING SECTION.

STEP 1:Read the original uncompressed video and is separated into k frames .

STEP 2: Select any five random frames from the host video and convert it into grayscale frames.

STEP 3.The image (img) is transformed into DWT domain by applying two-level Haar Wavelet decomposition.

STEP 4.The resultant image will be divided into LL, HL, LH, and HH Planes.

STEP 5: Apply SVD to LL,HL,LH planes for each frame of the original video.

i.e. $A(img) = U_i(img)S_i(img)V_i^T(img)$ and also apply SVD to LH HL sub bands also . approximate coefficients from low pass filter are taken for each frame.

STEP 6: Read the secret plain text message (M)

STEP 7: Encrypt the secret text message by using the algorithm in [5].

STEP 8: The Encrypted secret message (E_M) is embedded in the selected coefficients of the host image using the LSB algorithm. The

Scaling Factor α is added with Simg to control the robustness and imperceptibility.

$D_i(img)=S_i(img) + \alpha \; * (E_M)$

STEP 9:Apply SVD on $D_i(img)$ matrix of each frame selected to obtain SV_S

$D_i(img) = U_i E_M(img) S_iE_M(img) V_i^T E_M(img)$

STEP 10: The $S_iE_M(img)$ matrices of eachframes are used to get the stegoimage

$AE_M(img) = Ui(img) S_iE_M(img) V_i^T(img)$

STEP 11: After changing the grayscale image to color image and performing the inverse DWT using modified and non modified DWT coefficients stegovideo is obtained.

3. PROPOSED METHODOLOGY

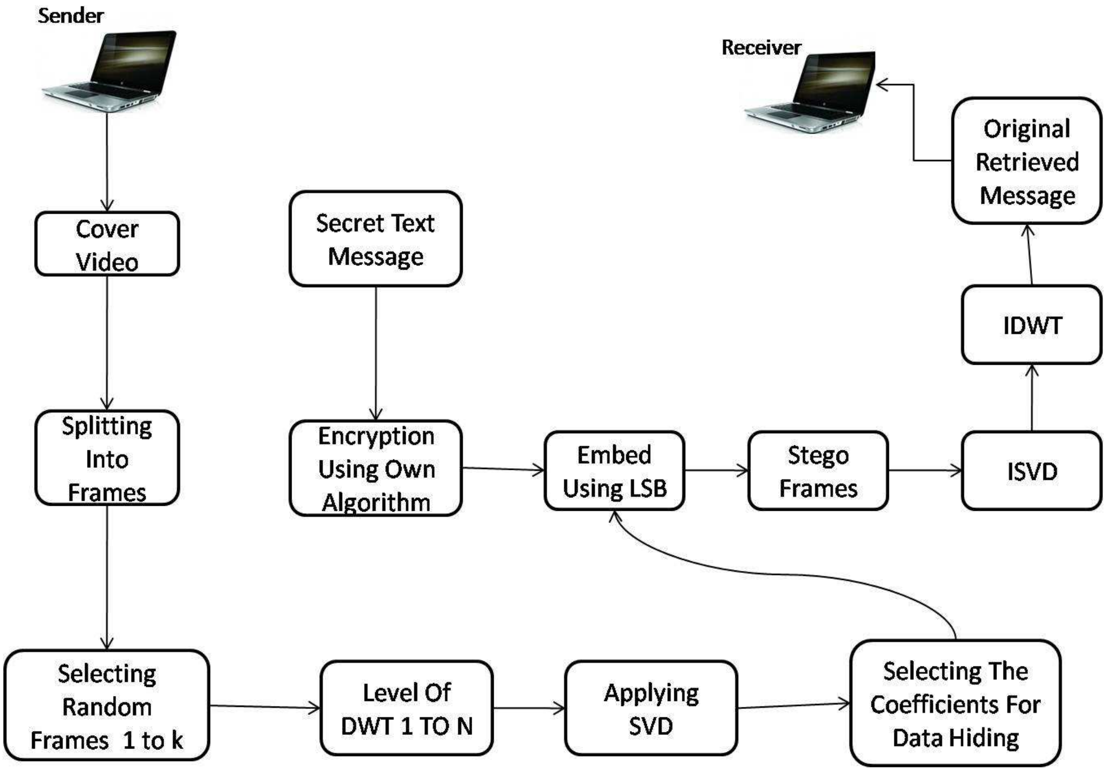


Figure 2 Block Diagram Of The Proposed Steganographic Method

3.2. Retrieving The Original Secret Text

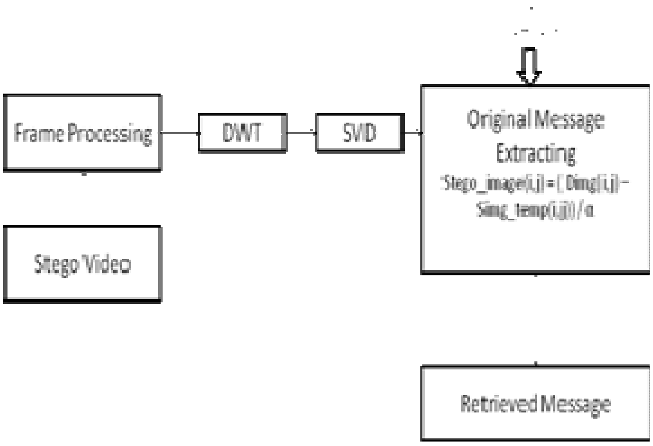


Figure. 3.: Block Diagram For Extracting The Original Secret Message.

EXTRACTION SECTION:

STEP1: The obtained stegovideo is divided into groups of k frames

STEP2: Every group of frame is converted into greyscale image.

STEP 3: Apply two-level Haar DWT to decompose the stego image into four sub bands:

into LL, HL, LH, and HH Planes.

STEP 4: The Embedded wavelet coefficients are selected according to Figure3.

STEP5: Apply SVD to the LL ,LH and HL sub bands to obtain the SVs of each one .

STEP 6: Calculate $A^*E_M(img) = U_i^*\ (img)\ S_i^*E_M(img)\ V_i\ ^{*T}\ (img)$

STEP 7: Extract the original secret message from each frame.

Compute $D_i^*(img) = U_i\ E_M(img)\ S_i^*EM(img)\ V_i\ ^TE_M\ (img)$

Original secret message $M^* = D_i^*img - S_i(img) / \alpha$

4. RESULTS AND DISCUSSION

Here using MATLAB coding we have executed the above algorithm ,we have taken real time video then selected few random frames to perform steganography as per Figure.4. A 2D-DWT has been performed on every frame selected to transform the frames into high ,low and medium frequencies , then SVD is performed based on the above algorithm. We have embedded the encrypted secret text message using LSB algorithm and PSNR values are calculated as per below table , we obtained the PSNR values between 70 and 80 db and the stegovideo looks visually similar to the original video and the original secret message is extracted without any loss.

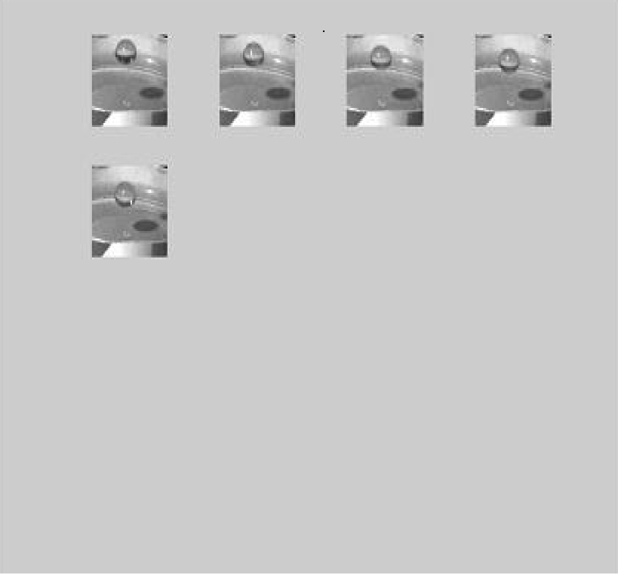


Figure4.: Frames Selected For Steganography

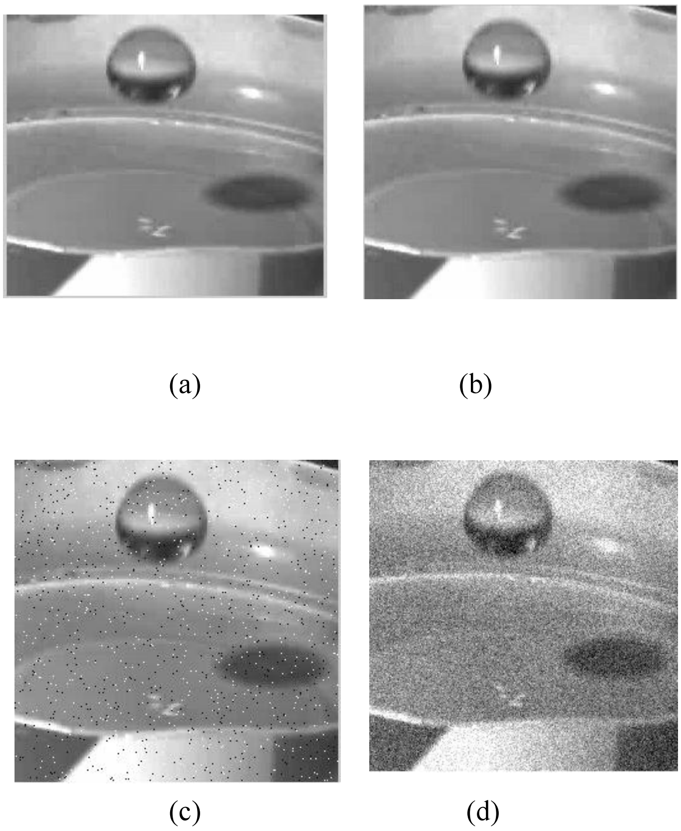
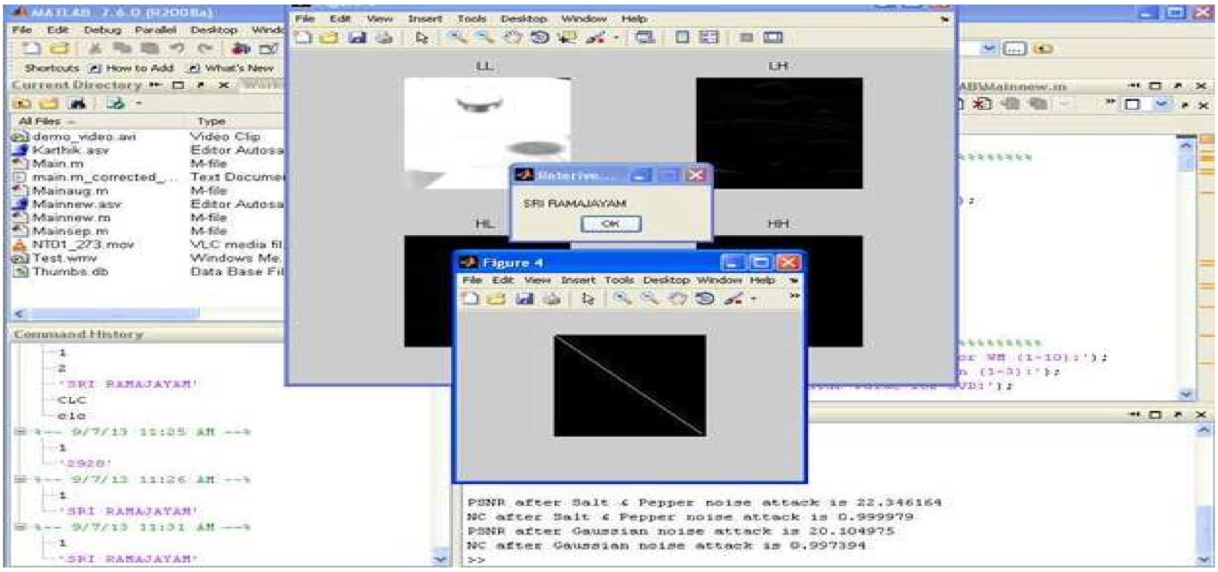


Figure 5. A) Original Frame, B) Stegoframe, C) Stegoframe After Salt & Pepper Attack, D) Stegoframe After Gaussian Attack

Another important experiment is testing the robustness of the Stegovideo is also done by adding the Gaussian noise of mean 0 and variance 0.02% and adding the Salt and Pepper noise with density 0.02 % we were able to extract the original secret message. MATLAB results of original frame and stegoframe then after adding the salt & pepper noise and Gaussian noise is shown in Figure.5. Normalized correlation (NC) is obtained as per table1. We have also performed rotation, cropping, scaling, our proposed method withstands all the above attacks. Final MATLAB results of extracted original message without any loss is shown in Figure.6

Comparison with other existing methods.

We have compared our method with other existing method [21]. In [21] authors claimed that DCT performance is good for image steganography while comparing with DST and other methods , but DCT is having certain disadvantages because DCT works mostly only on JPEG files on the other hand DWT provides higher compression ratio [20] than DCT, and DWT is having its own multi resolution characteristics ,so we have used DWT .Since singular value matrix value is stable when a little distortion is added into a image we used SVD and combined with DWT.


MATLAB 7.6.0 (R2008a)
File Edit Debug Parallel Desktop Window
Shortcuts How to Add What's New
Current Directory
File Edit View Insert Tools Desktop Window Help
LL
LH
HL
HH
Figure 4
File Edit View Insert Tools Desktop Window Help
OK

All Files	Type
demo_video.avi	Video Clip
Karthik.asv	Editor Autosa
Main.m	M-file
main.m_corrected_...	Text Docume
Mainaug.m	M-file
Mainnew.asv	Editor Autosa
Mainnew.m	M-file
Mainsep.m	M-file
NTD1_273.mov	VLC media fil
Test.wmv	Windows Me
Thumbs.db	Data Base Fi

```
Command History
  1
  2
  'SRI RAMAJAYAM'
  CLC
  clc
%-- 9/7/13 11:25 AM --%
  1
  '2928'
%-- 9/7/13 11:26 AM --%
  1
  'SRI RAMAJAYAM'
%-- 9/7/13 11:31 AM --%
  1
  'SRI RAMAJAYAM'
```

Retrieve...

SRI RAMAJAYAM

```
PSNR after Salt & Pepper noise attack is 22.346164
NC after Salt & Pepper noise attack is 0.999979
PSNR after Gaussian noise attack is 20.104975
NC after Gaussian noise attack is 0.997394
>>
```

Figure 6 MATLAB Results Of Extracted Original Message

Table 1. Experimental Results.

Frame Number	PSNR (dB)	NC	NC value after Salt&Pepper noise	NC value after Gaussian noise
1	82.43	0.999	0.998	0.997
2	82.81	0.998	0.997	0.996
3	81.71	0.999	0.998	0.996
4	75.76	0.999	0.997	0.995
5	75.77	0.998	0.996	0.995

5. CONCLUSIONS AND FUTURE WORK

This Method aims to propose the new methodology by cascading the features of discrete wavelet transform (DWT) and singular value decomposition (SVD).To overcome the capacity issue in using the SVD we have taken video as cover object and converted the video into frames then selecting the sufficient number of frames for message embedding. The bmp image of frame is taken because it is having uncompressed data. The frames are selected randomly, we have applied DWT to all the frames selected .the decomposition level is selected by k value, then SVD is applied to the LL band, then Secret message is encrypted by using our previous work [5]. We have utilized other planes also to deviate attention of the eavesdroppers; the Encrypted message is embedded into SVD portion of the frame by using LSB algorithm. The original message is retrieved using IDWT as shown in figure 3. Our experimental results show that PSNR value is maintained as an average of 77 db. We have tested our stegoframes by applying various attacks like Salt and Pepper Noise and Gaussian noise as shown in results, but message is not altered, and encryption phase in our method added another level of security. In these paper features of DWT, SVD are properly utilized by selecting the appropriate detailed coefficients and LSB algorithm is in addition used to embed the secret message. As future work, we aim to secure the communication medium also and we aim to apply this method for Mobile Ad-hoc Networks.

ACKNOWLEDGMENT

I would like to thank the Management of Velammal Engineering College, Chennai, in which where I am working as Assistant Professor for providing me the infrastructure and support to carry out this research.

REFERENCES

[1] Khalil Challita and Hikmat Farhat, Combining Steganography and Cryptography: New Directions,issue Number: Vol. 1, No. 1. Year of Publication: Jun - 2012. Page Numbers: 199-208. Publisher: The Society of Digital Information and Wireless Communication.

[2] Yusnita Yusof and Othman O. Khalifa , “Digital Watermarking For Digital Images Using Wavelet Transform”, Proceedings of IEEE conference, PP 665-669, Mar, 2007.

[3] Fadhil Salman Abed, Nada Abdul Aziz Mustafa. A proposed Technique for Information Hiding Based On DCT. DOI: 10.4156/ijact.vol2.issue 5.16.

[4] Luo X Y,Liu F L, Yang C F,et al. Modification ratio estimation for a category of adaptive steganography.Sci China Inf Sci, 2010, 53:2472-2484,doi:10.1007/s11432-010-4105-7.

[5] Boopathy.R, Ramakrishnan.M, VictorS.P .Modified LSB method using new Cryptographic algorithm for steganography. Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28-30, 2012. Series:Advances in Intelligent Systems and Computing,(Springer) Vol. 236 2014, XX, 1248 p. 558 illus. D.O.I 10.1007/978-81-322-1602-5_63

[6] Esra satir, Hakan Isik,A compression-based text steganography method. Journal of Systems and Software(2012) Elsevier Inc.http://dx.doi.org/10.1016/j.jss.2012.05.027

[7] Desoky,A.,2009.Listega:List-based steganography methodology. International Journal of Information Security 8(4),247-261.

[8] R. Liu and T. Tan, “An SVD-based watermarking scheme for protecting rightful

ownership," IEEE Transactions. Multimedia, Vol. 4, pp. 121–128 Mar. 2002.

[9] Elshoura and Megherbi, High capacity blind information hiding schemes using tchebichef moments 7th IEEE International Conference on Signals and Electronic Systems (ICSES '10), Gliwice, Poland, September 2010.

[10] Sumit Kumar Prajapati, Amit Naik, Anjulata Yadav , Robust digital watermarking using DWT-DCT-SVD, International Journal of Engineering research and Applications Vol. 2,Issue 3, May-Jun 2012,pp.991-997.

[11] Xiao Bing Kang and Sheng Min Wei," An efficient approach to still image copy detection based on SVD and block partition for digital forensics" IEEE Signal Processing Magazine in 2009

[12] Lou,D.,Wu,N.,Wang.C.,Lin,Z.,Tsai,C.S.,2010.A novel adaptive steganography based local complexity and human vision sensitivity. Journal of Systems and Software 83(7),1236-1248.

[13] Chang,C.,Kiew,T.d.,2010.A reversible data hiding scheme using complementary embedding strategy.Information Sciences 180(16),3045-3058.

[14] Samira Bouchama, Latifa Hamami, and Hassina Aliane : H.264/AVC Data Hiding Based on Intra Prediction Models for Real-time Applications. In: Proceedings of the World Congress on Engineering and Computer Science .Vol. 1.WCECS 2012,USA.

[15] Sajedi, H.,Jamzad,M., 2010. BSS:boosted steganography scheme with cover image preprocessing. Expert Systems with Applications 37(12),7703-7710.

[16] Yun Cao, Xianfeng Zhao,Denqquo Feng,Rennong Sheng. Video steganography with Perturbed Motion Estimation . DOI 10.1007/978-3-642-24178-9_14 .pp 193-207 (2011)

[17] Seyyed Mohammad Reza Farschi.H.Farschi .A novel chaotic approach for information hiding in image.DOI 10.1007/s 1071-012-0367-5.

[18] Faragallah OS. Efficient video watermarking based on singular value decomposition in the discrete Wavelet transforms.IntJElectronCommon (AEU)(2012).http:dx.doi.org/10.1016/j.aeue.2012.07.010.

[19] Clifford Bergman and Jennifer Davidson, Unitary Embedding for Data hiding with the SVD. Security, Steganography, and Watermarking of Multimedia contents VII, SPIE Vol.5681, San Jose,Ca,Jab.2005.

[20] Amanjot Kaur,Jaspreet Kaur Comparison of DCT and DWT of Image Compression. International Journal of Engineering Research and Development ISSN:2278-067X,Vol 1,Issue 4 (June 2012). PP.49-52.

[21] Prashasti Kanikar, Ratnesh N Chaturvedi, Vibhishek Kashyap and Pooja Likhite. Article: Image Steganography using DCT, DST, Haar and Walsh Transform. International Journal of Computer Applications 65(17):34-37, March 2013. Published by Foundation of Computer Science, New York.