Robust Video Steganographic Model for Banking Application by Cascading the Features of SVD and DWT

Boopathy.R†, Ramakrishnan.M††, Victor.S.P†††

[1]Research Scholar in Manonmaniam Sundaranar University, Thirunelveli.
††Prof & Head, Dept.of Information Technology, Velammal Engineering College,Chennai.
†††Head ,Department of Computer Science,St. Xavier College, Pallayamkottai.

Summary
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). Steganography becomes a proficient mean of securing multimedia documents. In the Proposed method we show how to use the DWT and SVD for hiding the secret text message which is encrypted by using our own methodology for providing another layer of security. DWT is applied on cover image for decomposition of images into sub bands which gives linear flexibility of images in terms of resolution and distortion and do image compression without any data loss. By adding SVD in the sub bands of DWT, the encrypted message is embedded in the SVD transformed image using LSB algorithm. The decomposition level of DWT and Scaling Factor of SVD can be chosen at runtime. We have selected LL plane for SVD transformation and other planes are also used for different purpose, the appropriate coefficients are properly used which is different from other conventional methods. The Capacity issue in using the SVD is accomplished by taking the video and converting the video into frames then selecting the random number of frames for embedding is done here. The Proposed method is tested with various statistical attacks including Salt & pepper noise .The Experimental results shows that the proposed method is robust against various statistical attacks then PSNR and NC values are maintained as 77db and 0.999 respectively for all the frames. Email is used as communication channel. Finally comparison of the proposed method with other existing methods has been carried out.

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

1. Introduction

Research in information hiding has blossomed during the past decade. Research is focused on how to avoid the illegal copies or piracy. Cryptography, watermarking, and steganography are the data hiding techniques that are mainly used for this purpose. (Chang and Kieu, 2010).Cryptography may attract the attention of interceptors so data hiding techniques evolved. Digital watermarking is used for copyright protection whereas steganography is used for covert communications. Extensive research has been carried out by combining cryptography and steganography[1]. Digital watermarking [2] usually alters the cover image in order to embed the owner's identifier. Steganography is exclusively used for secret communications. The major difference between these two is mainly in its goal 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 the some of the weakness in sending the secret text message. In banking transactions we use mobile as medium to send the pin code, one time password and etc for fund transfer or any other transactions. 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. For this application this paper is designed. 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

Manuscript received October 5, 2014
Manuscript revised October 20, 2014

transforms and singular value decomposition. Embedding Capacity is also determined by (Desoky, 2009). [6,7].

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

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 Stegoframe 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 current watermarking and steganography methods. It is found that most of the schemes having their weakness against statistical attacks.
(2)Capacity, Imperceptibility and Robustness: The proposed video steganography methods show 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

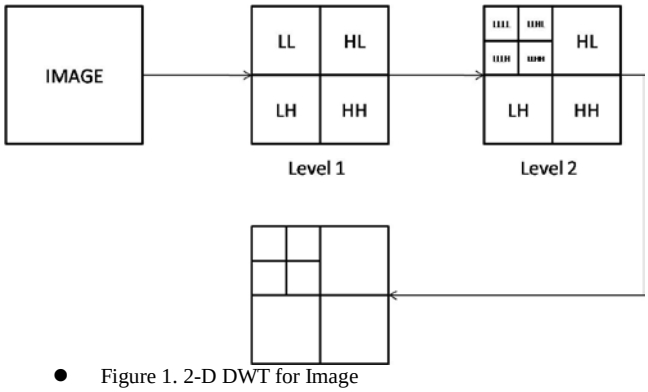
Two types of transformations are used here namely Discrete wavelet transforms (DWT) and Singular value decomposition (SVD).

2.1 The Discrete Wavelet Transform (DWT)

- Discrete wavelet transform (dwt), transforms a discrete time signal to a discrete wavelet representation.
- DWT converts the input series $x_0, x_1, \ldots..x_m$, into one high-pass and low-pass wavelet coefficient series (of length n/2 each) given by:
- $\mathbf{H_i} = \sum_{m=0}^{k-1} \mathbf{X_{2i-m}} \mathbf{.s_m(z)}$
- $\mathbf{L_i} = \sum_{m=0}^{k-1} \mathbf{X_{2i-m}} \mathbf{.t_m(z)}$
- Where $s_m(z)$ and $t_m(z)$ be 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 that 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 this algorithm is we need not depend on the fixed level of compression provided by a method such as JPEG or gif compression, but we have choose 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 be able to request information as required to rebuild an "acceptable" image. If you can exist with a fuzzy image you can certainly choose to get a much smaller array of values than the original. There may be a number of variations of the SVD decomposition as well. We can apply 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, say A. We then by

decomposition of the matrix A we get $A= USV^T$ 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 (s_1 , s_2, s_3 , ..., s_k , 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 suggesting 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. Watermark also can be extracted and the extracted image can be tested under peak signal to noise ratio (PSNR) and Accuracy rate (AR). 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, they determined pixel classification into three levels based on boundary values .In [13] they 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] they proposed 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 they have embedded the secret data. Embedding the data in video codec H.264/AVC video quality has been preserved and also encoding and decoding time is maintained. In[15]they introduced boosted steganography method for increasing the undetectability of stegoimages, they applied preprocessing methods on cover image, authors suggesting that existing methods used to increase the embedding capacity may reduces the detection risk of stegoimages , this BSS method has the own flexibility for the steganographer to select the cover images from the databases to increase the the security and embedding capacity. In [16] Video steganography is done here 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 can be hidden and recovered from images using chaotic approaches but secret key is needed

In [18] by OSAMA S.FARAGALLAH the authors given 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 presented a data hiding technique that exploits a decomposition representation of the data instead of frequency based transformations of the data. they used the singular value decomposition .they have shown how to use the orthogonal matrices in the SVD as a vessel in which to embed the information they have not addressed the undetectability and robustness. In [20] the authors says 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 it also avoids blocking artifacts, and it is proved that DCT is time consuming.

3. Proposed methodology

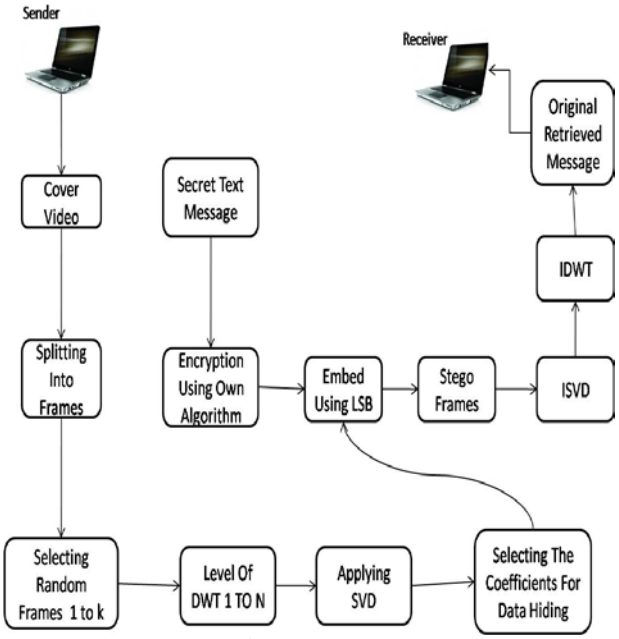


Figure 2. Block diagram of the proposed steganographic method

3.1 Implementation of DWT-SVD scheme for steganography

The proposed DWT-SVD scheme for steganography is formulated as given below

EMBEDDING SECTION

STEP1: Read the Original Uncompressed Video and is separated into k frames .

STEP2: Select the Random frames from 1to k and convert it into greyscale image.

STEP3: The image is transformed into DWT domain and the level of Wavelet decomposition (Level= 1to 3)will be decided by user at runtime

STEP4: The resultant image will be divided into LL, HL, LH, and HH Planes.

STEP5:Apply SVD on LL plane. (i.e.)

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

STEP6: Take only S values to hide the data .Let it be Simg

$$Stego\_image = Uimg * S_{stego\_image} * V_i^T(img)$$

STEP7: Read the Secret Text Message

STEP8:Covert the ASCII Value of Letter into corresponding binary Value.

STEP9: Encrypt the message using the given algorithm [5].

STEP10: The Encrypted secret image is embedded using the LSB algorithm. The Scaling Factor α is added with Simg to Strengthen the Embedding Process.

$D_i(img)=S_i(img) + \alpha * Stego\_image(i,j)$

STEP 11:Apply SVD on $D_i(img)$ matrix of each frame selected to obtain SV_S

$D_i(img) = U_{stego\_image} * S_{stego\_image} * V^T_{stego\_image}$

STEP12: Obtain the stegoimage by performing the inverse DWT using modified and non modified DWT coefficients.

3.2 Retrieving the original secret text message

EXTRACTION SECTION:

1) The obtained stegovideo is divided into groups of k frames.

2) Every group of frame is converted into greyscale frames.

3) Apply desired level Haar DWT to decompose the stego image *into* four sub bands:

into LL, HL, LH, and HH Planes.

4) The Embedded wavelet coefficients are selected according to Figure3.

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

$$Stego\_image(i,j) = (Dimg(i,j) – Simg\_temp(i,j)) / \alpha$$

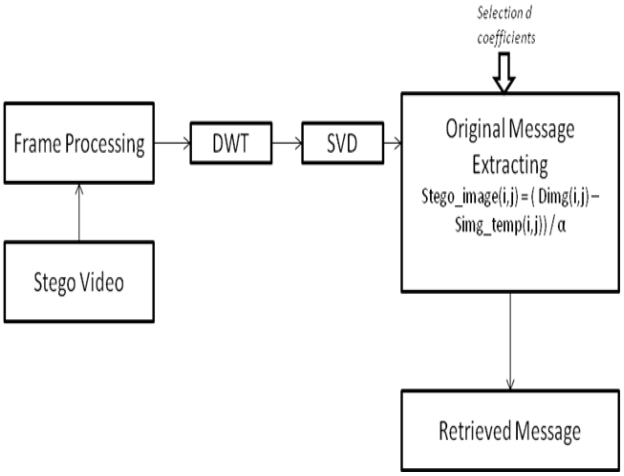


Figure 3. Block diagram for extracting the original secret message.

4. Results and discussion

Here using MATLAB coding we have executed the above algorithm ,we have taken real time video and

performed steganography 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 .

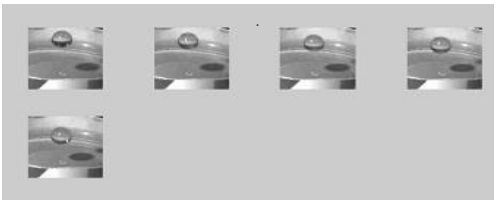


Figure 4. Frames selected for steganography.

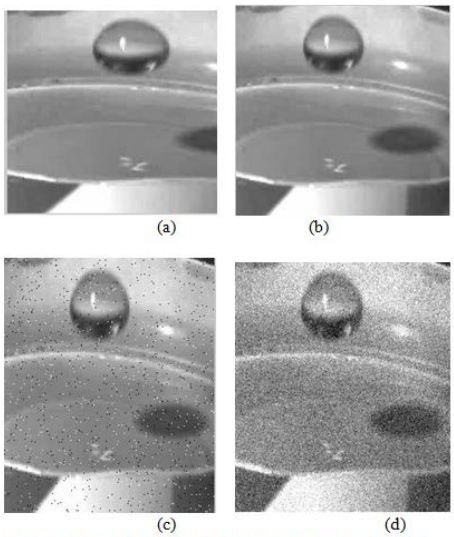


Figure 5. a) Original frame, b) Stegoframe, c) Stegoframe after Salt & Pepper Attack, d) Stegoframe after Gaussian attack.

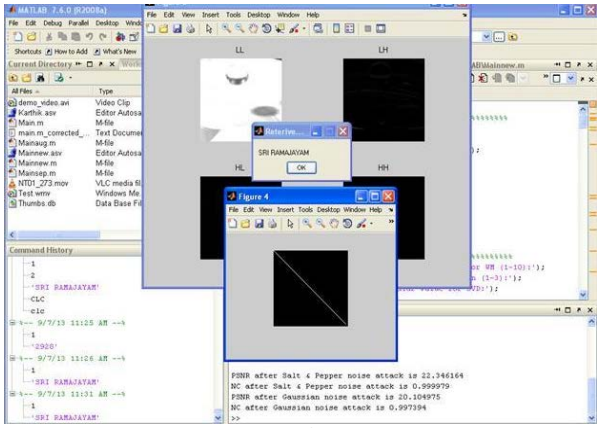


Figure 6. MATLAB Results of Extracted original message

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. Normalized correlation (NC) is obtained as per table1. We have also performed rotation , cropping , scaling ,our proposed method withstands all the above attacks .

4.1 Comparison with other existing methods.

We have compared our method with other existing method[21]. In [21] they 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 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 SVD is robust against statistical attacks we have combined both .

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", Proc IEEE conference, pp 665-669 ,march 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.

[6] Series:Advances in Intelligent Systems and Computing,(Springer) Vol. 236 2014, XX, 1248 p. 558 illus.(accepted and to be published).

[7] 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

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

[9] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121–128 Mar. 2002

[10] 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.

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

[12] 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

[13] 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.

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

[15] 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.

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

[17] 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)

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

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

[20] 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.

[21] 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.

[22] 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.

R.Boopathy received M.Sc., degree in Computer Science and M.Phil., degree in Computer Science from Bharathidasan University ,Tiruchirappalli,Tamil Nadu, India . He is having fifteen years of teaching experience as Assistant Professor. He has published one paper in Journal and 10 Papers in both national and International Conferences. His area of interest is image processing and Mobile computing .He is currently pursuing his doctorate degree in Manonmaninam Sundaranar University .

Dr. M.RAMAKRISHNAN is the Professor and Head of Information Technology. He completed his under graduation and post graduation from Madurai Kamaraj University and Doctorate from Anna University Chennai. His research areas of expertise are Parallel Computing, Neural Networks and Network

Security. He has 22 years of teaching experience and he has published many research papers in International/National journals and conferences. He is guiding six Ph.D scholars and M.E research scholars in his area. He has written books on Fundamentals of Computing and Object-oriented Programming. He is also a life member of ISTE and IACSIT, Singapore. He has organized FDPs, Workshops and Conferences.

Dr. S.P.VICTOR completed his MCA and Ph.D degrees and working as a Associate Professor and Head in the Department of Computer Science, in St.Xaviers College,Palayamkottai, TamilNadu. His area of interest is Parallel Algorithm Data Mining. He has published 15 papers in various journal and conferences. Two students completed their Ph.D under his guidance .He is guiding 10 research Scholars and 15 M.Phil., Students.