A Novel Image Encryption Supported by Compression Using Multilevel Wavelet Transform

Ch. Samson[1]
Dept. of Information Technology, SNIST,
Hyderabad, India,

V. U. K. Sastry[2]
Dept. of Computer Science & Engineering., SNIST,
Hyderabad, India,

Abstract— **In this paper we propose a novel approach for image encryption supported by lossy compression using multilevel wavelet transform. We first decompose the input image using multilevel 2-D wavelet transform, and thresholding is applied on the decomposed structure to get compressed image. Then we carry out encryption by decomposing the compressed image by multi-level 2-D Haar Wavelet Transform at the maximum allowed decomposition level. These results in the decomposition vector C and the corresponding bookkeeping matrix S. The decomposition vector C is reshaped into the size of the input image. The reshaped vector is rearranged by performing permutation to produce encrypted image. The vector C and the matrix S serve as key in the process of both encryption and decryption. In this analysis, we have noticed that the reconstructed image is a close replica of the input image.**

Keywords- Image compression; wavelet transform; thresholding; image encryption; compression ratio.

I. INTRODUCTION

An image is to be compressed so as to reduce the storage space and increase the speed of transmission. Image compression [1] is of two types: lossy or lossless. In lossless compression, the recovered data is identical to the original, whereas in the case of lossy compression the recovered data is a close replica of the original with minimal loss of data. Lossless compression can be used for text, medical images and legal documents etc. whereas lossy compression is used for natural images, speech signals etc. Images are widely used on several processes, including the Internet, and hence protecting confidential image data from unauthorized access has become an important issue in information security. Cryptography plays a vital role in information security. Cryptography [2] is the art or science that transforms a message (plaintext) into an unintelligible form (ciphertext) and then retransforms that message back to its original form.

Wavelets [3] have gained widespread acceptance in signal processing and image compression applications due to their utility in multi-resolution analysis. A basic wavelet is an oscillatory function that has limited duration. Wavelets are obtained from a single prototype wavelet called mother wavelet by dilations and shifting. Mathematically a wavelet is denoted by the function.

$$\psi_{a,b}(t) = \frac{1}{\sqrt{|a|}}\psi(\frac{t-b}{a})$$

where a is the scaling parameter and b is the shifting parameter. The transform based on wavelets is called wavelet transform. Wavelet decomposition of an image is used to analyze the image at different frequencies with different resolutions that gives specific information. This information can be used for processing the image, such as image compression. Wavelet transforms are of two types. One is Continuous Wavelet Transform and the other one is Discrete Wavelet Transform. Several researchers [4-10] have dealt with image compression using wavelet transform.

An alternative representation to wavelet transform is the multiwavelet transform [11-12]. Multiwavelets are very similar to wavelets but have some important differences. In particular, wavelets have an associated scaling function Φ(t) and wavelet function Ψ(t), whereas multiwavelets have two or more scaling and wavelet functions. Multilevel wavelet transforms find a wide variety of applications. They can be used can be used for compression, denoising, egde detection and encryption. In a recent investigation, Debayan et al. [13] have developed an algorithm for text encryption using multilevel 1-D wavelet transform.

In the present paper, our objective is to develop a novel method for image encryption supported by compression using multilevel 2-D Wavelet Transform. Firstly, we compress the input image using multilevel 2- dimensional wavelet transform and the compressed image is then encrypted by using a multilevel 2- dimensional Haar Wavelet Transform.

In what follows we present the plan of the paper. In section 2, we explain the proposed method. Section 3 describes the process of image compression using wavelet packet transform. We present a novel approach for wavelet-based image encryption in section 4. We provide an illustration in section5. Finally in section 6, we deal with computations that are carried out in this analysis and draw conclusions.

II. PROPOSED METHOD

When network bandwidth and storage space are limited, image has to be compressed. It is necessary to protect the image data during transmission from unauthorized access. Therefore to reduce the time for encryption, the image is first compressed prior to encryption. Reverse operations are performed at the receiving end to reconstruct the original image. The Schematic diagram of the proposed method is shown in Figure 1.

The proposed method is implemented by the following steps.

1. Decomposition: Choose a multilevel 2-D wavelet transform having the number of decomposition levels as N. Compute the wavelet decomposition of the input image at level N.

2. **Thresholding**: For each level from 1 to N, a threshold is selected and global thresholding is applied to the detail coefficients.

3. Encryption: The compressed image is encrypted by using multilevel 2-D Wavelet Transform (Haar).

4. Decryption: The reverse process of encryption is performed to get the compressed image.

5. Reconstruction: Perform multilevel 2-D wavelet reconstruction of the decrypted image to get a close replica of the original input image.

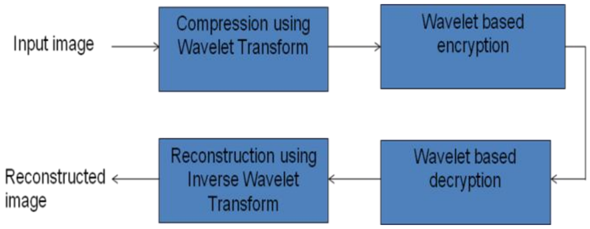
Input image
Compression using Wavelet Transform
Wavelet based encryption
Wavelet based decryption
Reconstruction using Inverse Wavelet Transform
Reconstructed image

Figure 1. Schematic diagram of the proposed method

The algorithm for wavelet based image encryption is given below.

Algorithm for image encryption

1) *Read the input (compressed) image.*

2) *Decompose the input image at the maximum allowed level, using multilevel 2-D Haar Wavelet Transform to get decomposition vector C and the corresponding bookkeeping matrix S.*

3) *Store the vector C and the matrix S.*

4) *Reshape the coefficients of the decomposition vector C to have the size of the input image (N -by-N).*

5) *Rearrange the vector coefficients by performing permutation to produce encrypted image.*

By performing inverse operations for the above steps in the reverse order, we get back the input compressed image which is the decrypted image. It is to be noted here that the decomposition vector C and the corresponding bookkeeping matrix S serve as key for both encryption and decryption.

III. Wavelet Approach For Image Compression

Image compression is one of the most successful applications of wavelet transform. The Wavelet Transform can be implemented using specially designed digital filters. Let us consider an image F(x,y) of size N×N. The samples of the input image are passed through a low pass filter and a high pass filter simultaneously, and the filter outputs are down-sampled by two along rows. Then the filter outputs can be further decomposed using the same filters and down-sampled by two again along columns, giving the approximation coefficients matrix (LL) and the detail coefficients matrices (LH, HL and HH) each of size N/2× N/2 as shown in Figure 2.

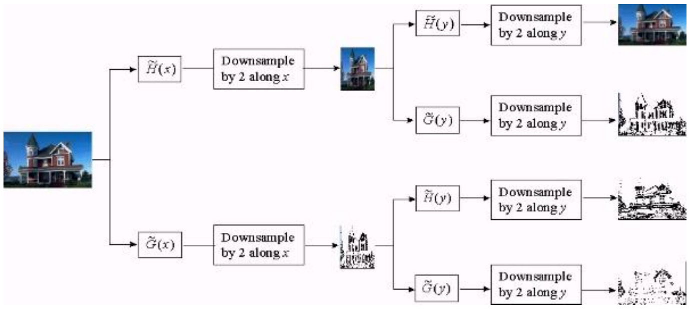
$\tilde{H}(x)$
Downsample by 2 along x
$\tilde{G}(x)$
Downsample by 2 along x
$\tilde{H}(y)$
Downsample by 2 along y
$\tilde{G}(y)$
Downsample by 2 along y
$\tilde{H}(y)$
Downsample by 2 along y
$\tilde{G}(y)$
Downsample by 2 along y

Figure 2. Wavelet Transform implementation.

To have a clear idea, Figure 2 can be seen as shown below.

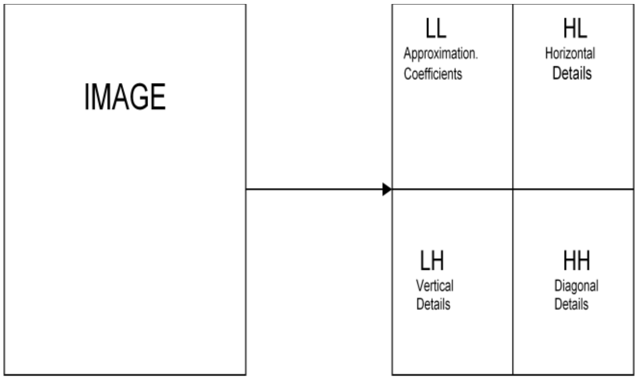

Figure 3. Wavelet Decomposition

The approximation coefficients matrix (LL) is called low resolution sub image. The sub images HL, LH and HH give horizontal, vertical and diagonal details respectively. multiwavelet decompositions produce two low pass subbands and two high pass subbands in each dimension. This kind of decomposition can be repeated to further increase the frequency resolution and the approximation coefficients decomposed with high and low pass filters and then down-sampled. In this analysis, we have conducted experiments using multilevel wavelet transforms based on Haar, Biorthogonal, Coiflet, Discrete Mayer Wavelet, Symlet, and we have taken the number of decomposition levels 3 to 5. However we have included levels 3 and 4 only in our analysis (See table I in section 6) for brevity in representation.

In the process of multilevel wavelet decomposition, many of the wavelet coefficients we have obtained are close to or equal to zero. Most of the information is included among a small number of the transformed coefficients. So, we truncate or quantize the coefficients including little information using thresholding. Thresholding can modify the coefficients to produce more zeros. Three types of thresholding [1] techniques can be used: local thresholding, global thresholding and dynamic thresholding. Local tresholding is one in which a different threshold is applied to each sub image where as a single threshold is applied to all sub images in global thresholding. Dynamic thresholding uses different thresholds for each coefficient separately. In our analysis, level-dependent global thresholds are selected based on Birge-Massart strategy and applied on detail coefficients as approximation coefficients cannot be thresholded. This will produce many consecutive zeros which can be stored in much less space and transmitted more quickly.

It is to be noted here that the low pass filter and the high pass filter are related to each other and they are known as the quadrature mirror filters which will make image reconstruction possible.

IV. Wavelet Based Image Encryprtion

In this section we present a novel method for image encryption using Wavelet Transform. The compressed image which we have obtained in section III is decomposed by multilevel 2-D Haar Wavelet Transform at the maximum allowed decomposition level and get the decomposition vector C and the corresponding bookkeeping matrix S. We reshape the decomposition vector C into a matrix form of size N×N. We rearrange the vector coefficients by performing permutation to obtain the encrypted image.

By performing inverse operations in the reverse order, we get back the input (compressed) image. The advantage of wavelet based image encryption is that the encryption time gets reduced and the decryption time also becomes small.

V. Illustraion of the method involving compression and encryption

Consider the image of Gandhiji of size 256x256 which is shown in Figure 4, given in section VI. Let us focus our attention on a portion P of the image of size 8x8 which lies in between the rows 1 to 8, and the columns 1 to 8. On representing this portion of the image in terms of its pixel values, we get the matrix given below.

$$P = \begin{bmatrix} 204 & 204 & 202 & 201 & 203 & 205 & 203 & 199 \\ 200 & 198 & 197 & 197 & 201 & 204 & 202 & 197 \\ 201 & 199 & 197 & 198 & 204 & 207 & 206 & 201 \\ 206 & 204 & 201 & 201 & 205 & 208 & 208 & 206 \\ 207 & 205 & 202 & 200 & 199 & 200 & 203 & 205 \\ 207 & 204 & 201 & 198 & 195 & 194 & 198 & 203 \\ 208 & 205 & 202 & 200 & 198 & 197 & 200 & 204 \\ 210 & 206 & 203 & 203 & 203 & 203 & 204 & 207 \end{bmatrix}$$

On decomposing P by using multilevel 2-D Wavelet Transform at the decomposition level 3, we get decomposition vector c and the corresponding bookkeeping matrix s in the form

c = (1.0e+003) *[1.6179 -0.0006 -0.0001 -0.0121 -0.0010 -0.0033 -0.0077 -0.0048 0.0055 0.0107 0.0037 -0.0087 -0.0010 0.0003 0.0023 -0.0018 0.0050 -0.0050 0.0005 -0.0015 0.0045 -0.0035 0.0015 -0.0020 0.0015 -0.0010 0.0050 -0.0055 0.0015 -0.0035 0.0035 -0.0035 0.0010 0.0020 0.0025 0.0035 0.0005 -0.0005 0.0025 0.0010 -0.0025 -0.0030 0 0.0005 0.0045 0.0035 -0.0035 -0.0035 -0.0010 0 -0.0005 -0.0005 0.0005 -0.0005 -0.0005 0.0010 0.0005 0 -0.0010 0.0005 -0.0005 0.0015 0.0015 -0.0005],

and

$$s = \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 2 & 2 \\ 4 & 4 \\ 8 & 8 \end{bmatrix}$$

Level-dependent thresholds are obtained by using a wavelet detail coefficients selection rule based on Birge-Massart strategy [12]. However, we have to remember that the approximation coefficients cannot be thresholded. On using level-dependent thresholds, the decomposition vector c and the corresponding bookkeeping matrix s, compression is performed, and the resultant compressed image is obtained in the form

$$CP= \begin{bmatrix} 201 & 201 & 201 & 201 & 204 & 204 & 204 & 204 \\ 201 & 201 & 201 & 201 & 204 & 204 & 204 & 204 \\ 201 & 201 & 201 & 201 & 204 & 204 & 204 & 204 \\ 201 & 201 & 201 & 201 & 204 & 204 & 204 & 204 \\ 204 & 204 & 203 & 203 & 201 & 201 & 201 & 201 \\ 204 & 204 & 203 & 203 & 201 & 201 & 201 & 201 \\ 204 & 204 & 203 & 203 & 201 & 201 & 201 & 201 \\ 204 & 204 & 203 & 203 & 201 & 201 & 201 & 201 \end{bmatrix}$$

The compressed image matrix CP is decomposed by the multilevel 2-D Haar Wavelet Transform at the maximum allowed decomposition level to get the decomposition vector C and the corresponding bookkeeping matrix S. The decomposition vector C is reshaped into a matrix form of size N×N, and it is given by

$$rs = \begin{bmatrix} 402 & 0 & 0 & 0 & 0 & 0 & 0 & 408 \\ 402 & 0 & 0 & 0 & 0 & 0 & 0 & 408 \\ 408 & 0 & 0 & 0 & 0 & 0 & 0 & 402 \\ 408 & 0 & 0 & 0 & 0 & 0 & 0 & 402 \\ 402 & 0 & 0 & 0 & 0 & 0 & 0 & 408 \\ 402 & 0 & 0 & 0 & 0 & 0 & 0 & 408 \\ 406 & 0 & 0 & 0 & 0 & 0 & 0 & 402 \\ 406 & 0 & 0 & 0 & 0 & 0 & 0 & 402 \end{bmatrix}$$

The bookkeeping matrix S is given by

$$S = \begin{bmatrix} 4 & 4 \\ 4 & 4 \\ 8 & 8 \end{bmatrix}$$

We obtain the encrypted image matrix by performing permutation. Thus we have

$$E = \begin{bmatrix} 255 & 255 & 0 & 0 & 0 & 0 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

On performing inverse permutation on E, we get the decomposition vector in the form of a matrix of size 8x8. On reshaping it into vector form, we get a column vector given by

rC = [402 402 408 408 402 402 406 406 408 408 402 402 408 408 402 402 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 $]^T$.

Here T denotes transpose of the vector. We have obtained the decrypted matrix D based on the multi-level wavelet decomposition structure [rC,S]. This is given by

$$D = \begin{bmatrix} 201 & 201 & 201 & 201 & 204 & 204 & 204 & 204 \\ 201 & 201 & 201 & 201 & 204 & 204 & 204 & 204 \\ 201 & 201 & 201 & 201 & 204 & 204 & 204 & 204 \\ 201 & 201 & 201 & 201 & 204 & 204 & 204 & 204 \\ 204 & 204 & 203 & 203 & 201 & 201 & 201 & 201 \\ 204 & 204 & 203 & 203 & 201 & 201 & 201 & 201 \\ 204 & 204 & 203 & 203 & 201 & 201 & 201 & 201 \\ 204 & 204 & 203 & 203 & 201 & 201 & 201 & 201 \end{bmatrix}$$

It is to be noted here that the decrypted matrix D and the compressed matrix CP are the same.

Thus, by performing multilevel 2-D wavelet reconstruction based on the decomposition vector c and its corresponding bookkeeping matrix s, we have reconstructed the matrix rP which is a close replica of the original input matrix P. This is given by

$$rP = \begin{bmatrix} 204 & 204 & 202 & 201 & 203 & 205 & 203 & 199 \\ 200 & 198 & 197 & 197 & 201 & 204 & 202 & 197 \\ 201 & 199 & 197 & 198 & 204 & 207 & 206 & 201 \\ 206 & 204 & 201 & 201 & 205 & 208 & 208 & 206 \\ 207 & 205 & 202 & 200 & 199 & 200 & 203 & 205 \\ 207 & 204 & 201 & 198 & 195 & 194 & 198 & 203 \\ 208 & 205 & 202 & 200 & 198 & 197 & 200 & 204 \\ 210 & 206 & 203 & 203 & 203 & 203 & 204 & 207 \end{bmatrix}$$

It may be noted here that the reconstructed matrix rP is an exact replica of the original input matrix P as the elements of the rP are rounded off to the nearest integer.

Here the decomposition vector and the corresponding bookkeeping matrix serve as key in the process of encryption and in the process of decryption.

VI. Computations And Conclusions

In this paper we have implemented a novel approach for image encryption supported by compression using multilevel wavelet transform in MATLAB[14] .

We have considered multilevel 2-D Wavelet Transforms, namely, 'haar' 'bior6.8','coif5','dmey' 'sym8' for image compression and multilevel 2-D Haar wavelet transform for image encryption. We have conducted experiments using the above wavelets for three test images 'Lena', 'Gandhiji' and 'Lady'. The input image of Gandhiji of size 256x256 and its corresponding compressed, encrypted, decrypted and reconstructed images are shown below for the decomposition level 4.

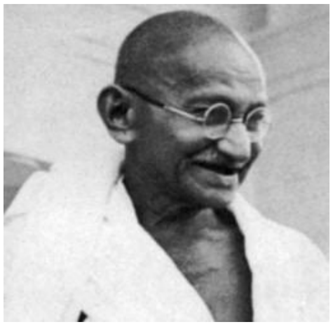

Figure 4. Input image of Gandhiji

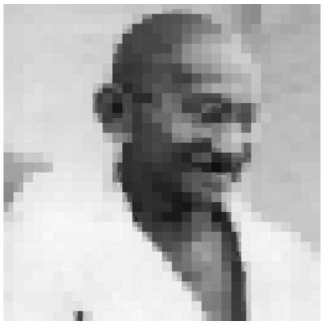

Figure 5. Compressed image

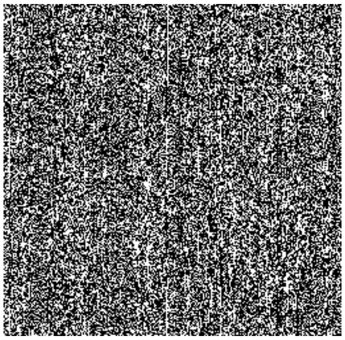

Figure 6. Encrypted image.

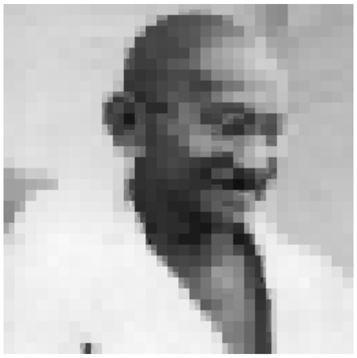

Figure 7. Decrypted image

We have calculated output parameters like compression score, compression ratio that determine the efficiency of the proposed system. Compression score is given by

Compression score in percentage = 100*(number of zeros of the current decomposition)/ number of coefficients)

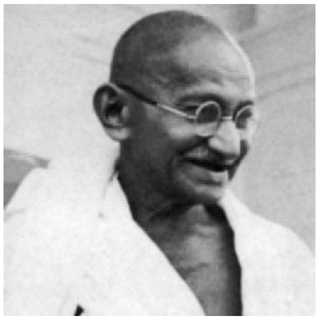

Figure 7. Reconstructed image

Compression ratio (C_R) is defined as

$$C_R = \frac{Uncompressed\ File\ Size}{Compressed\ File\ Size}$$

The performance comparison of five traditional wavelets for three test images is given below in table 1.

TABLE I. Performance comparison

Image	Type of wavelet used	Compression score (%)		Compression ratio	
		N=3	N=4	N=3	N=4
Lena	haar	92.27	97.95	12.94	49.0
	bior6.8	87.10	93.95	7.75	16.5
	coif5	83.09	90.27	5.91	10.2
	dmey	66.14	74.17	2.95	3.87
	sym8	87.4	94.21	7.94	17.2
Gandhiji	haar	92.27	97.9	12.94	49.2
	bior6.8	87.1	93.95	7.75	16.5
	coif5	83.09	90.27	5.91	10.2
	dmey	66.14	74.17	2.95	3.87
	sym8	87.40	94.21	7.94	17.2
Lady	haar	92.27	98.06	12.94	51.68
	bior6.8	87.10	93.95	7.75	16.54
	coif5	83.09	90.27	5.91	10.28
	dmey	66.14	74.17	2.95	3.87
	sym8	87.40	94.21	7.94	17.28

In this analysis, we have found that wavelet transform is very powerful and extremely useful for compressing data such as images. It is quite interesting to see that both compression and encryption are carried out by using wavelet transform.

Wavelet transform 'sym8' demonstrates better performance. It is observed that for a fixed decomposition level, the increase in value of threshold results in greater compression while for a fixed value of threshold, compression score/ratio decreases with increase in decomposition level. Wavelet based image encryption could be useful in a lot of commercial applications whereby large image databases can be rendered illegible to unauthorized users. We conclude that the compression ratio depends on the type of image and type of transforms because there is no filter that performs the best for all images pertaining to different applications.

REFERENCES

[1] Rafael C. Gonzalez & Richard E. Woods,― Digital Image processing, 2ndEdition Pearson Education 2004.

[2] William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, Pearson, 2003.

[3] K.P. Soman, K.I. Ramachandran, Insight into Wavelets from theory to practice, Second edition, PHI, 2006.

[4] S. Mallat, A Wavelet Tour of Signal Processing, (AcademicPress, 1999).

[5] Bryan Usevitch, "A Tutorial on Modern LossyWavelet Image Compression : Foundations of JPEG 2000," IEEE Signal Processing Magazine, 2001.

[6] Sachin P. Nanavati, Prasanta K. Panigrahi, "Wavelet Transform- A new mathematical microscope", (Resonance, March 2004)

[7] DONOHO D. Compressed sensing [J], IEEE Transactions on Information Theory, 2006, 52(4):1289-1306.

[8] CANDES E. Compressive sampling[A], Proceedings of the International Congress of Mathematicians[C]. Madrid, Spain, 2006, 3: 1433-1452.

[9] Jatan K. Modi, Sachin P. Nanavati, Amit S. Phadke,Prasanta K. Panigrahi, "Wavelet Transforms- Application to Data Analysis – 1",(Resonance, November 2004).

[10] S. Singh, V. Kumar. H. K. Verma ," DWT-DCT hybrid scheme for medical image compression", *Journal* of Medical Engineering & Technology, Vol 31, Issue 2 , pp.109 – 122, March 2007 .

[11] Martin M., "Applications of Multiwavelets to Image Compression," PhD Thesis, Deptartment of Electrical Engineering, Virginia Polytechnic Institute & State University, June 1999.

[12] Sudhakar R. and Jayaraman S., "Image Compression Using Multiwavelets and Wavelet Difference Reduction Algorithm," in Proceedings of the International Conference on Resource Utilization and Intelligent Systems, pp. 1-8, January 2006.

[13] Debayan Goswami, Naushad Rahman, Jayanta Biswas, Anshu Koul, Rigya Lama Tamang,Dr. A. K. Bhattacharjee,' A Discrete Wavelet Transform based Cryptographic algorithm', IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.4, April 2011.

[14] Alasdair Mcandrew, ―Digital Image processing with MatLab, Cengage learning 2004.

AUTHORS PROFILE

Dr. V. U. K. Sastry is presently working as Professor in the Dept. of Computer Science and Engineering (CSE), Director (SCSI), Dean (R & D), SreeNidhi Institute of Science and Technology (SNIST), Hyderabad, India. He was Formerly Professor in IIT, Kharagpur, India and worked in IIT, Kharagpur during 1963 – 1998. He guided 12 PhDs, and published more than 80 research papers in various international journals. He received the best Engineering College Faculty Award in Computer Science and Engineering for the year 2008 from the Indian Society for Technical Education (AP Chapter) and Cognizant- Sreenidhi Best faculty award for the year 2012. His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic Algorithms.

Mr. Ch. Samson obtained his Diploma from Govt. Polytechnic, Hyderabad in 1994, B. E. from Osmania University in 1998 and M. E from SRTM University in 2000. Presently he is pursuing Ph.D. from JNTUH, Hyderabad since 2009. He published 10 research papers in various international journals and two papers in conferences. He is currently working as Associate Professor and Associate Head in the Dept. of Information Technology (IT), SNIST since June 2005. His research interests are Image Processing, Image Cryptography and Network Security.