AN EFFICIENT METHOD OF CHAOS-BASED IMAGE-ENCRYPTION AND THEN COMPRESSION ALGORITHM

P.Kalaiselvi
Department of Computer science
Theivanai Ammal College for Women Villupuram

G.Mathurambigai Assistant professor
Department of Computer science
TheivanaiAmmal College for Women Villupuram

ABSTRACT

With the increasing growth of technology and the world has entered into the digital image, to handle a vast amount of information every time which often presents difficulties. So, the digital information must be stored and retrieved in an efficient and effective manner, in order for it to be put to practical use. A new algorithm is proposed which combines two techniques encryption and compression. In this technique, a chaos based encryption algorithm is used to encrypt the image and after that the encrypted image is compressed using the haar wavelet transform.

***Keywords* -** Image compression; image encryption; compression ratio.

INTRODUCTION

With the rapid development of multimedia and network technologies; the security of multimedia becomes more and more important; since multimedia data are transmitted over open networks more and more frequently. Typically the reliable security is necessary to content protection of digital images and videos. Encryption schemes for multimedia data need to be specifically designed to protect multimedia content and fulfill the security requirements for a particular multimedia application. Take example of real-time encryption of an entire video stream using classical ciphers requires heavy computation due to the large amounts of data involved, but many multimedia applications require security on a much lower level; this can be achieved using selective encryption that leaves some perceptual information after encryption.

Government, military and private business amass great deal of confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense) product, financial-status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer; if these confidential images about enemy positions ,patient ,and geographical areas fall into the wrong hands; than such a breach of security could lead to lots of war , wrong treatment etc. Protecting confidential images is an ethical and legal requirement. Then store information in computer system in the form of files. Therefore file is taken as a basic entity for keeping the information. And the problem of securing figure data or information on computer system can be defined as the problem of securing file data. The worldwide accepted fact that securing file data is very important, in today’s computing environment. Therefore good coding makes a source look completely random; traditional algorithms are unable to compress encrypted data.

For this reason, traditional systems make sure to compress before they encrypt. We are using the concept of public key encryption, for the encryption and decryption of image. In this public key's of sender and receiver is known to both but private key's are kept secret. Neither the security nor the compression efficiency will be sacrificed by performing compression in the encrypted domain.

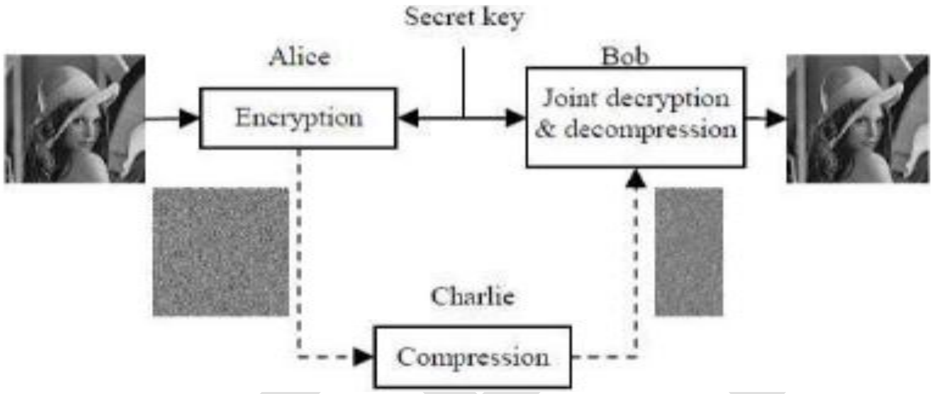

Figure1: ETC system

Consider an application scenario in which a content owner Alice wants to securely and efficiently transmit an image I to a recipient Bob, via an un-trusted channel provider Charlie. Conventionally, this could be done as follows. Alice first compresses I into B, and then encrypts B into Ie using an encryption function EK (•), where K denotes the secret key. The encrypted data Ie is then passed to Charlie, who simply forwards it to Bob. Upon receiving Ie, Bob sequentially performs decryption and decompression to get a reconstructed image I. Even though the above Compression-then-Encryption (CTE) paradigm meets the requirements in many secure transmission scenarios, the order of applying the compression and encryption needs to be reversed in some other situations. As the content owner, Alice is always interested in protecting the privacy of the image data through encryption.

IMAGE ENCRYPTION

Nowadays, when more and more sensitive information is stored on computer and transmitted over the internet; need to ensure information security and safety. Therefore, it is very important to protect our image from unauthorized access. Encryption provides an obvious approach to information security and encryption programs are readily available. Encryption algorithms available for textual data are highly efficient. But sometime the information is available in form of image. In such cases we need a specialized algorithm that is highly optimized to protect pictorial information. It is well known that images are different from texts in many aspects, such as high redundancy and correlation. The main obstacle in designing effective image encryption algorithms is the difficulty of shuffling and diffusing such image data by traditional cryptographic means. In most of the natural images, the value of any given pixel can be reasonably predicted from the values of its neighbors. Chaos based cryptosystem provides an efficient way to achieve image encryption. In the proposed block encryption/decryption algorithm, a 2D chaotic map is used to shuffle the image pixel positions. For image encryption, two-dimensional (2D) chaotic maps are naturally employed as the image can be considered as a 2D arrayof pixels. Traditional symmetric ciphers such as Advanced Encryption Standard (AES) are designed with good

confusion and diffusion properties. Two properties can also be found in chaotic systems of pseudo-randomness and periodicity which means a dynamical system that has the same behavior averaged over time as averaged over space, high sensitivity to initial conditions and parameters.

Confusion property obscures the relationship between the plain text and the cipher text and diffusion dissipates there dundancy in the plain text by spreading it out over the cipher text. Figure 2 and 3 shows that the encryption and decryption of an image respectively. Therefore the output showed in figure 2 can be obtained by using various image encryption techniques.

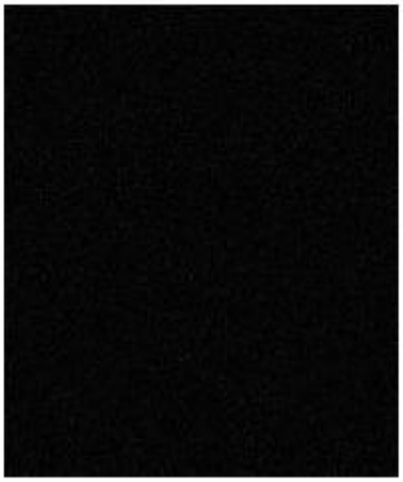

Figure 2: Encryption of an image

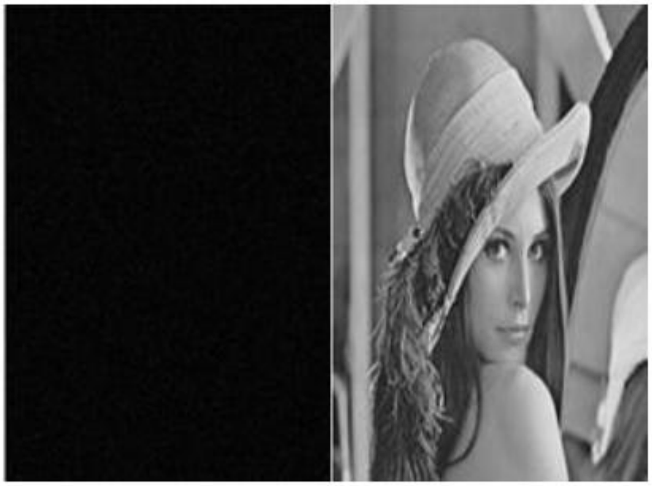

Figure 3: Decryption of an image

IMAGE COMPRESSION

Image compression addresses the problem of reducing the amount of data required to represent a digital image. This process intended to yield a compact representation of an image; thereby reducing the image storage/transmission requirements [3].

Compression is achieved by the removal of one or more of the three basic data redundancies:

- Coding Redundancy
- Inter pixel Redundancy
- Psychovisual Redundancy

Coding redundancy is present when less than optimal code words are used. Thus the inter pixel redundancy results from correlations between the pixels of an image. And Psychovisual redundancy is because of data that is ignored by the human visual system (i.e. visually non essential information). Figure compression methodologies reduce the number of bits required to represent an image by taking advantage of these redundancies. And the inverse process called decompression (decoding) is applied to the compressed data to get the reconstructed

Therefore the main aim of compression is to reduce the number of bits as much as possible; while keeping the resolution and the visual quality of the reconstructed image as close to the original image as possible. And image compression systems are mixed of two distinct structural blocks: an encoder and a decoder.

In first stage, the mapper transforms the input image into a format designed to reduce inter pixel redundancies. Therefore second stage; qunatizer block reduces the accuracy of mapper's output in accordance with a predefined criterion.

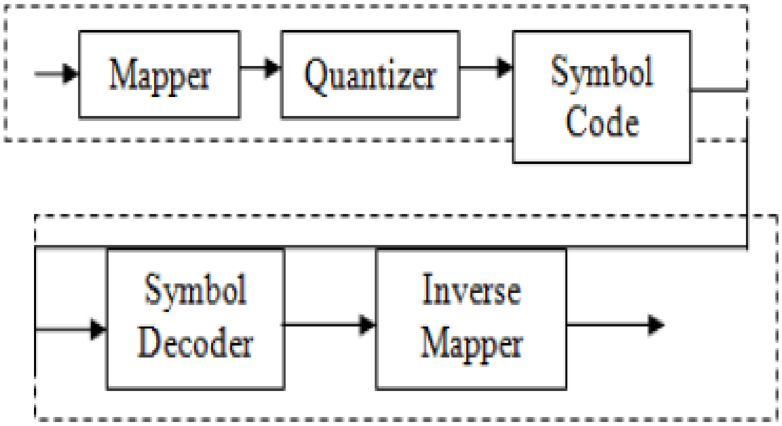

Figure 4: Block diagram of image compression

The third and final stage; a symbol decoder creates a code for quantizer output and maps the output in accordance with the code. All blocks perform; in reverse order the inverse operations of the encoder's symbol coder and mapper block. Therefore the quantization is irreversible; an inverse quantization is not included. The figure 5 shows the output of image compression after one iteration and last one.

PROPOSED METHOD

In this section, we present the details of the three keycomponents in our proposed ETC system. 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. Fig 5 shows the Schematic diagram of the proposed method.

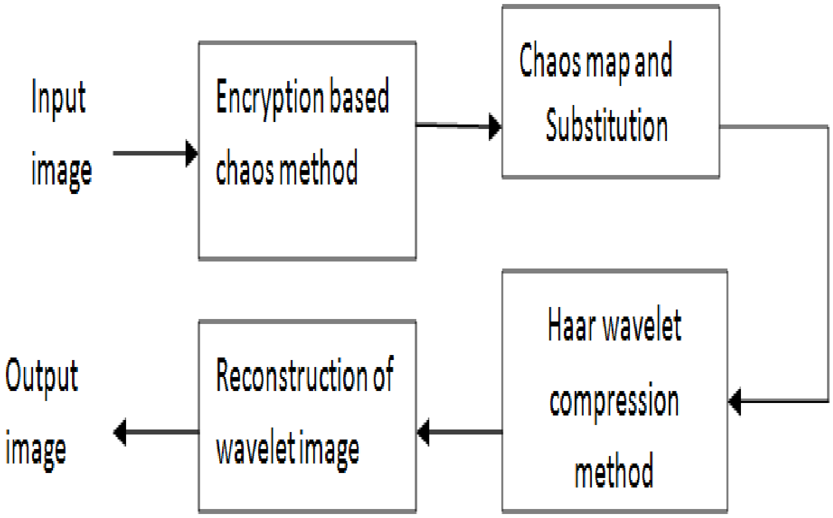
Input image
Encryption based chaos method
Chaos map and Substitution
Haar wavelet compression method
Reconstruction of wavelet image
Output image

Figure5. Schematic diagram of the proposed method

The algorithm for chaos based image encryption is given below.

Algorithm for image encryption by chaos method

The algorithm developed provides a method for purpose of encrypting and decrypting the image of any size and shape. It allows the user to select an image of his choice from a specified location on the computer, external hard drive or any other hardware devices connected to the computer. The system is able to support all standard image formats (e.g.:-TIFF, JPEG,BMP…..).The image selected by the user could be a Square image or a rectangular image of any dimension. The user is able to apply encryption to images captured via the camera and Personal pictures. The image selected should be a color image where the pixels are represented in the RGB model. Each pixel should be represented using minimum 24 pixels. Once the keys have been entered by the user in any form; a standard chaotic map is generated. The chaotic map generated using Mathematical equations and theory is completely reversible, efficient enough to produce diffusion on the entire image pixels.

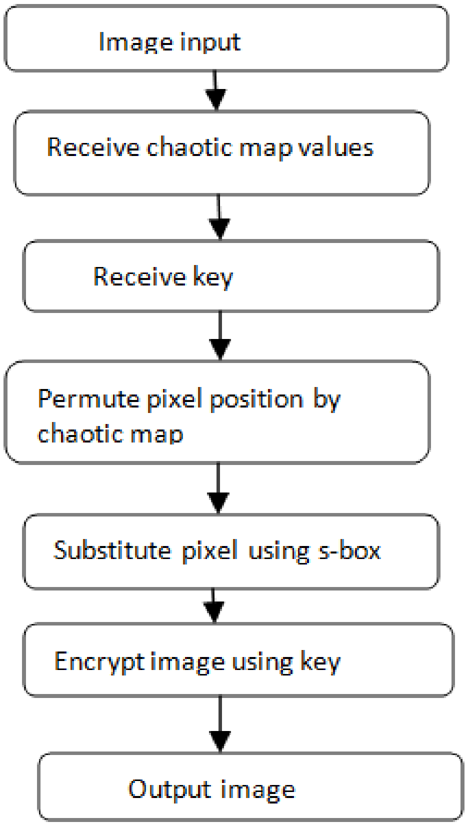
Image input
Receive chaotic map values
Receive key
Permute pixel position by chaotic map
Substitute pixel using s-box
Encrypt image using key
Output image

Approach 1: Sliding Window In order to provide chaos to rectangular images a sliding window approach is used where a fixed square window should run on the image and all the pixels within the range of the window is shuffled. The window is then shifted by one column to produce diffusion on further part of the image.

Approach 2: Perfect Square
Another approach that has been used is that the rectangular image is converted into square image and then diffusion through chaotic map is applied on its pixels. The size of the original image is retained during the process of decryption.

The Chaotic map used will be Arnold cat method which is a 2Dchaotic map used for Cartesian coordinate system.

Equation of Arnold cat map is:
x=mod (2*i+j, m) +1;
y=mod (i+j, m) +1;

Where
x,y are new coordinated of pixels i,j are original coordinated m is size of square image Then, the substitution phase will be basically where key is x is stored with the image pixel value. Thus x or operation occurs on pixels-RGB values, so this will cause change in colour. Hence continuous colour of image is hidden.

GENERATION OF KEYS

The image can be encrypted using two types of keys.

A. Strict Key

In the strict key encryption algorithm the user is asked to enter a 32 digit hexadecimal number. This 32 digit hexadecimal number is then converted into a 128 bit binary key. Each hexadecimal key is represented by four bits. Since a 32-bit long key is entered by the user it corresponds to 128 bit binary key (32 X 4=128).This128 bit key is then used for encrypting the pixels. Each 128 bit key has the potential to encrypt approximately 5 pixels. The image pixels are represented using RGB model. Each colour in the RGB model is represented using 8-bits.So a total of 24-bits are used to represent each pixel. So the 128 bit key can encrypt 128/24~5pixels. The pixel encryption always starts from topmost first pixel and the encryption is performed from left to right. The encryption is performed using Bit-XOR operation:-The XOR gate with inputs *A* and *B* implements the logical expression After performing the encryption on neighbouring 5 pixels the128 bit key is right-round rotated by one. The new key obtained is also 128 bit in size and is then used to encrypt the next 5 pixels.

This process is continued and at each step the key is round rotated by one and then used to encrypt neighbouring pixels.

B. QUICK KEY

In this algorithm the user is asked to enter four decimal keys, say w, x, y, z. The four decimal keys entered should be less than256.Since the maximum decimal number that can be entered is255 its binary representation should consist of 8 bit binary digits. Each decimal key entered by the user is represented by 8 bits and the user enters four keys so we get a total of 32 bit key (8X4=32bit). Now we perform rotate left operation on each (w, x, y and z separately) 8 bit key to obtain a four new 8 bit binary key.

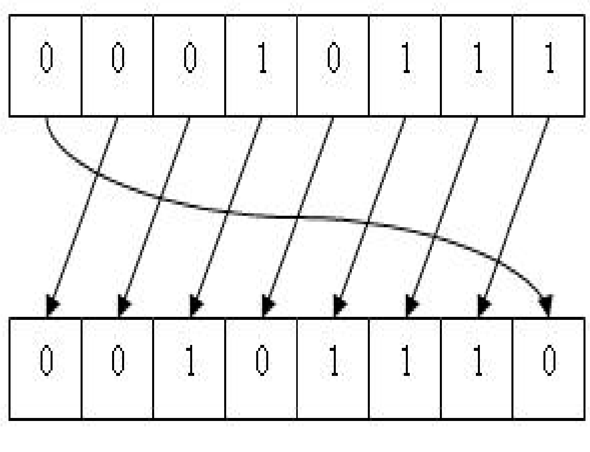

Fig 3. Key left rotate in CBCS(Chaos-Based Cryptosystem)

Now we perform rotate right operation on original four 8 bitbinary key (w, x, y and z combined together)

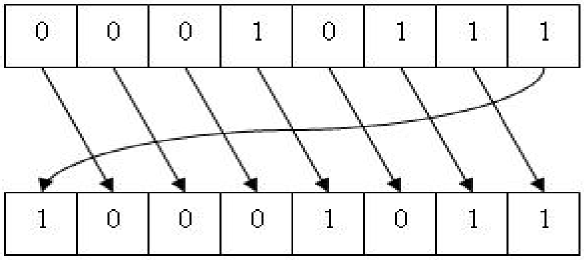

Fig 4. Key right rotate in CBCS(Chaos-Based Cryptosystem)

Next we perform XOR operation using this left shifted key andthe right shifted key to obtain a new 32-bit binary key.

Example:
0101 (decimal 5) XOR 0011 (decimal 3) = 0110 (decimal 6) We combine this four 32 bit key to obtain a 128 bit binary key. This 128 bit key is then used for encrypting the pixels. Each 128bit key has the potential to encrypt approximately 5 pixels. The
image pixels are represented using RGB model. Each color in the RGB model is represented using 8-bits.So a total of 24-bits are used to represent each pixel. So the 128 bit key can encrypt128/24~5 pixels. The pixel encryption always starts from topmost first pixel and the encryption is performed from left to right. After performing the encryption on neighbouring 5 pixels the128 bit key is right-round rotated by one. The new key obtained is also 128 bit in size and is then used to encrypt the next 5 pixels. This process is continued and at each step the key is round rotated by one and then used to encrypt neighbouring pixels.

DECRYPTION

The decryption process will be the reverse of encryption. First reverse substitution using the same key, so that colour is again readjusted and we get original colour. Next apply reverse chaotic map.

Equation for reverse Arnold cat map method is
x=mod (i-j-1, m) +1;
y=mod (2*j-i-2, m) +1;
Where
x,y are new coordinated of pixels
i,j are original coordinated
m is size of square image scanned from right to left.

At each step we apply reverse chaoticmap. Finally last stage in decryption process is resizing of image using reverse perfect square approach. In case of perfect square approach the image is converted to original rectangular shape .Whereas in case of Sliding window approach the image is scanned from right to left. At each step we apply reverse chaotic map.

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

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. Multi wavelet decompositions produce two low pass sub bands and two high pass sub bands 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.

HAAR WAVELET

The **Haar wavelet** is a certain sequence of functions. This recognized as the first known wavelet. The technique was in 1909 by invented Alfred Haar. Thus Haar is using these functions to give an example of a countable ortho normal system for the space of square integrable functions on the real line. Therefore study of wavelets; and even the term "wavelet", did not come until much later. The Haar wavelet is simplest wavelet. Therefore the disadvantage of the Haar wavelet is that it is not continuous; and therefore not differentiable. The mathematical prerequesites will be kept to a minimum; indeed, the main concepts can be understood in terms of addition, subtraction and division by two. We also present alinear algebra implementation of the Haar wavelet transform, and mention important recent generalizations. Like all wavelet transforms, the Haar transform decomposes a discrete signal into two subsignals of half its length.

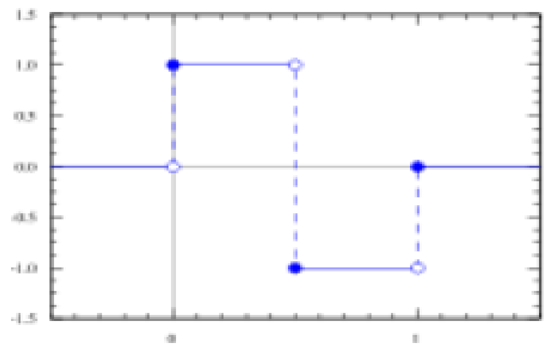

Figure 6: Haar wavelet window

Thus the scaling function φ(t) can be described as:

$$\psi(t) = \begin{cases} 1 & 0 \le t < 1/2, \\ -1 & 1/2 \le t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

$$\phi(t) = \begin{cases} 1 & 0 \le t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Wavelets are mathematical functions that were developed by scientists working in several different fields for the purpose of sorting data by frequency. Then the translated data can then be sorted at a resolution which matches its scale. And studying data at different levels allows for the development of a more complete picture. All small features and large features are discernable because they are studied separately. The discrete cosine transforms; the wavelet transform is not Fourier-based and therefore wavelets do a better job of handling discontinuities in data. Then Haar wavelet operates on data by calculating the sums and differences of adjacent elements. Thus the Haar wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements.

ILLUSTRAION OF THE METHOD INVOLVING COMPRESSION

Consider the image of Gandhiji of size 256x256 which is shown in Figure 4. 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.

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

Level-dependent thresholds are obtained by using a wavelet detail coefficients selection rule based on Birge-Massart strategy. 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

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

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.

We have considered multilevel 2-D Wavelet Transforms, namely, 'haar' image compression and multilevel 2-D Haar wavelet transform for image encryption. We have conducted experiments using the above wavelets for three test images 'Gandhiji' 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.

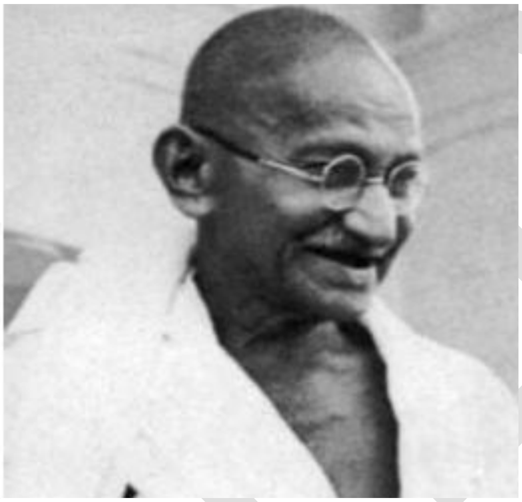

Figure 7. Input image

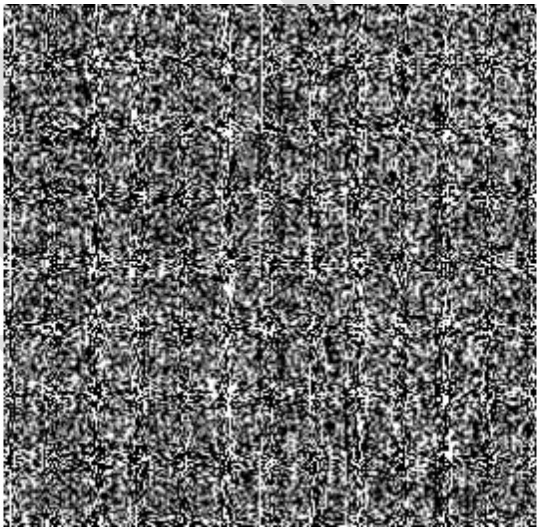

Figure 8. Encrypted image

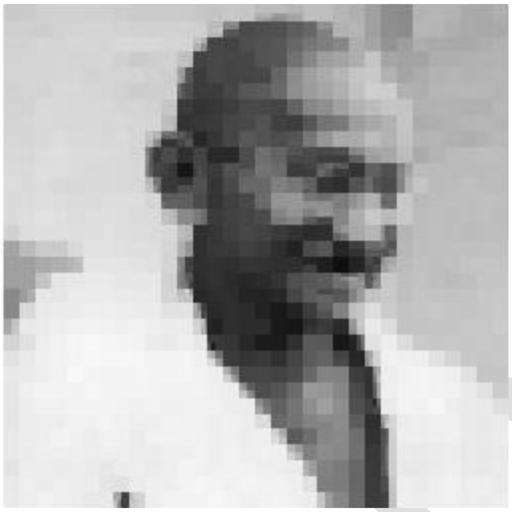

Figure9. Compressed image

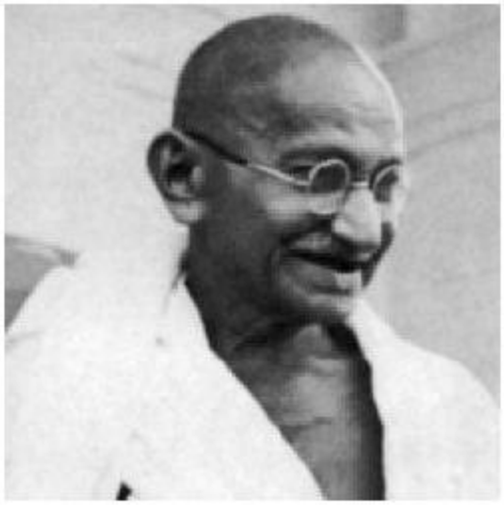

Figure10. Reconstructed image and output image

We have calculated output parameters like encryption and then compression image that determine the efficiency of the proposed system.

CONCLUSIONS

In this research work, we have designed an efficient image Encryption-Compression system. Therefore the proposed framework; the image encryption has been done by chaos based method. and the high efficient compression of encrypted image has been realized by a new image compression algorithm of Haar wavelet transform.

Wavelet transform ‘Haar’ 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. 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] Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, ―Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation‖, IEEE Trans. Inf. Forensics Security, vol. 9, issue 1, January 2014.

[2] R. Mehala and K. Kuppusamy, ―A New Image Compression Algorithm using Haar Wavelet Transformation‖, International Journal of Computer Applications(0975-8887), International Conference on Computing and Information Technology, 2013.

[3] X. Zhang, G. Sun, L. Shen, and C. Qin, ―Compression of encrypted images with multilayer decomposition‖, Multimed. Tools Appl., vol. 78, issue 3, Feb. 2013.

[4] J. Zhou, X. Wu, and L. Zhang, ―l2 restoration of l∞-decoded images via soft-decision estimation‖, IEEE Trans. Imag.Process., vol. 21, issue 12, Dec. 2012.

[5] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, ―On compression of data encrypted with block ciphers‖, IEEE Trans. Inf. Theory, vol. 58, issue 11, Nov. 2012. [6] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, ―Generating private recommendations efficiently using homomorphic encryption and data packing‖, IEEE Trans. Inf. Forensics Security, vol. 7, issue 3, June 2012.

[7] X. Zhang, G. Feng, Y. Ren, and Z. Qian, ―Scalable coding of encrypted images‖, IEEE Trans. Imag. Process, vol. 21, issue 6, June 2012.

[8] NidhiSethi, Ram Krishna, R. P. Arora, ―Image Compression using HAAR Wavelet Transform‖, IISTE Comp. Engg. & Intelligent Systems, ISSN 2222-1719, 2011

[9] X. Zhang, Y. L. Ren, G. R. Feng, and Z. X. Qian, ―Compressing encrypted image using compressive sensing‖, in Proc. IEEE 7th IIH-MSP, Oct. 2011.

[10] M. Barni, P. Failla, R. Lazzeretti, A. R. Sadeghi, and T. Schneider, ―Privacy-preserving ECG classification with branching programs and neural networks‖, IEEE Trans. Inf. Forensics Security, vol. 6, issue 2, June 2011.

[11] X. Zhang, ―Lossy compression and iterative reconstruction for encrypted image‖, IEEE Trans. Inf. Forensics Security, vol. 6, issue 1, Mar. 2011

[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] DebayanGoswami, NaushadRahman, JayantaBiswas, AnshuKoul, 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.

[15] Q. M. Yao, W. J. Zeng, and W. Liu, ―Multi-resolution based hybrid spatiotemporal compression of encrypted videos,‖ IEEE in Proc. ICASSP, Apr. 2009, pp. 725–728.

[16] T. Bianchi, A. Piva, and M. Barni, ―On the implementation of the discrete Fourier transform in the encrypted domain‖, IEEE Trans. Inf. Forensics Security, vol. 4, issue 1, Mar. 2009.

[17] A. Kumar and A. Makur, ―Lossy compression of encrypted image by compressing sensing technique‖, in Proc. IEEE Region 10 Conf. TENCON, Jan. 2009.

[18] T. Bianchi, A. Piva, and M. Barni, ―Encrypted domain DCT based on homomorphic cryptosystems‖, EURASIP J. Inf. Security, 2009, Article ID 716357.

[19] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, ―Toward compression of encrypted images and video sequences‖, IEEE Trans. Inf. Forensics Security, vol. 3, issue 4, Dec. 2008.

[20] R. Lazzeretti and M. Barni, ―Lossless compression of encrypted grey-level and color images‖, in Proc. 16th Eur. Signal Process. Conf., Aug. 2008.
[21] G. Millérioux, J. M. Amigo, J. Daafouz, ―A connection betweenchaotic and conventional cryptography,‖ IEEE Trans. Circuits andSystems, vol. 55, no. 6, pp. 1695-1703, Jul. 2008.
[22] H. Xiao, S. Qiu, C. Deng, ―A Composite Image Encryption SchemeUsing AES and Chaotic Series,‖ First International Symposium onData, Privacy and E-Commerce, pp. 277279 – 277279, 2007.
[23] A. Awad, A. Saadane, ―Efficient Chaotic permutations for imageencryption algorithms‖, IAENG, International Conference of Signaland Image Engineering, pp. 748–753, 30 Jun-3 July , London, UK,2010.
[24] S. Tao, W. Ruli, Y. Yixun, ―Perturbance based algorithm to expandcycle length of chaotic key stream,‖ IEEE, Electronics Letters, vol.34, no. 9, pp. 873-874, 1998.
[25] T. Yang, C. W. Wu, L. O. Chua, ―Cryptography Based on ChaoticSystems,‖ IEEE Trans. Circuits and Systems, vol. 44, no.5, pp. 469–472, Feb. 1997.
[26] G. Jakimoski, L. Kocarev, ―Chaos and Cryptography: BlockEncryption Ciphers Based on Chaotic Maps,‖ IEEE Trans. Circuitsand Systems, vol. 48, no. 2, pp. 163–169, Feb. 2001.
[27] Security in Computing - Charles P. Pfleeger , Pearson Education.
[28] Cryptography and Network Security by Behrouz A. Forouzan, TATAMcGraw hill.