Image Compression using Haar Wavelet Transform and Chaos-Based Encryption

Ranu Gupta[1]

[1] **JUET, ,India**
Guna , Madhya Pradesh 473226/91, India

Abstract

With the increasing growth of technology and the world has entered into the digital image, we have 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. Wavelets provide a mathematical way of encoding information in such a way that it is layered according to level of detail. This layering facilitates approximations at various stages. These approximations can be stored in less memory space than the original data. Here the 2D image is being compressed using Haar wavelet transform and the quality of the picture is presented here. After the compression the image is Encrypted using chaotic logistic map and an external secret key of 256-bit.The initial conditions for the chaotic logistic map are derived using external secret key by providing weighted to its bits corresponding to their position in the key. The quality of the image is evaluated by showing the table and graph of compression factor. While the various experimental results show that the proposed chaos based encryption provides high security level.

Keywords: *Haar Wavelet, Chaos, Chaotic Logistic Map, Cipher.*

1. Introduction

An image is essentially a 2-D signal processed by the human visual system. The signals representing images are usually in analog form. However, for processing, storage and safe transmission by computer applications, they are converted from analog to digital form. A digital image is basically a 2-Dimensional array of pixels. The use of and dependence on information and computers continue to grow, so too does our need for efficient ways of storing and safe transmission of large amounts of data. Nowadays, images are normally transmitted as well as stored in electronic form. The vulnerability of this form of information to be attacked such as modification and fabrication is higher as compared to paper-based image. One of the mechanisms that can be applied to guarantees the storing, privacy, integrity and the authenticity in image transmission and archival applications is compressing and modem cryptography.

Encryption algorithms such as Triple-DES, IDEA and RC5 are considered secured but their computation is complex. On the other hand, chaotic encryption that requires a simple computational procedure offers an alternative for implementing a stream or block cryptosystem.

2. Image Compression

In a raw state, images can occupy a large amount of memory both in RAM and in storage. Image compression reduces the storage space required by an Image and the bandwidth needed when streaming that image across a network. From the Table 1. [1], the examples show clearly the need for sufficient storage space, large transmission bandwidth and long transmission time for image. At the present state of art in technology, the only solution is to compress image.

2.1 Principle of Compression

A common characteristic of most of the images is that the neighboring pixels are correlated and therefore contain redundant information. The foremost task is to find less correlated representation of the image. Two fundamental components of compression are redundancy and irrelevancy reduction [3]. Redundancy reduction aims at removing duplication from the signal source (image). Irrelevancy reduction omits parts of the signal that will not be noticed by the signal receiver, namely the Human Visual System (HVS).
In general, three types of redundancy can be identified

- Spatial Redundancy or correlation between neighboring pixel values.
- Spectral Redundancy or correlation between different color planes or spectral bands.
- Temporal Redundancy or correlation between adjacent frames in a sequence of images (in video applications).

Table1: Describe type of Image, its size, bits-pixel; uncompress size, transmission bandwidth and time.

Types Of Image	Size	Bits/Pixel /or bits/sample	Uncompressed Size	Transmission Bandwidth	Transmission Time (using a 28.8K Modem)
Grayscale Image	512x512	8bpp	262KB	2.1Mb	1.`13min
Color Image	512x512	24bpp	786KB	6.24Mb	3.34min
Medical Image	2048x1680	12bpp	5.16MB	41.3Mb	23.54min
SHD Image	2048x2048	24bpp	12.58MB	100Mb	58.15min

We focus only on still images. For image compression there are three types of redundancies. Coding redundancy is present when less than optimal code words are used. Inter-pixel redundancy results from correlations between the pixels of an image. Psycho visual redundancy is due to data that is ignored by the human visual system (i.e. visually non essential information). The objective of image compression is to reduce the number of bits, while keeping the resolution and visual quality of the reconstructed image as close to the original image.

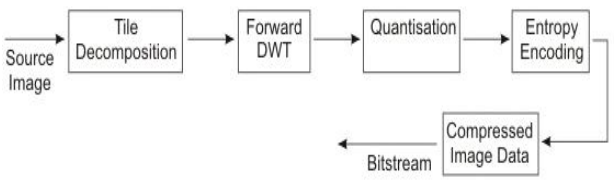


Fig.2.1 General Block diagram of Image Compression.

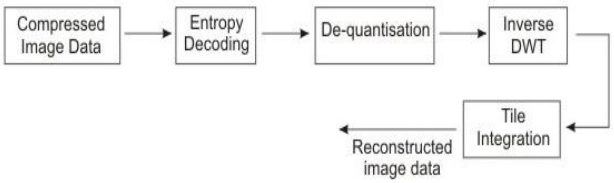


Fig. 2.2 General block diagram of Image Decompression

Fig. 2.1 and Fig. 2.2 show the block diagram of image compression and image decompression techniques. Before applying the DWT, the source image is divided into components (colors) and each component is divided into tiles which are compressed independently. This paper is concentrated on wavelet-based lossy compression of grey-level still images. When there are 256 levels of possible intensity for each pixel, then we shall call these images 8 bpp (bits per pixel) images. Images with 4046 grey-levels are referred to as 12 bpp.

2.2 Haar Wavelet Transform

Haar Wavelet Transform exploits both the spatial and frequency correlation of data by dilations (or contractions) and translations of mother wavelet on the input data. Another encouraging feature of wavelet transform is its symmetric nature that is both the forward and the inverse transform has the same complexity,
Building fast compression and decompression routines. The output of the filter banks is down-sampled, quantized, and encoded.
The wavelet transform is computed by recursively averaging and differencing coefficients, filter bank. We can reconstruct the image to any resolution by recursively adding and subtracting the detail coefficients from the lower resolution versions. The basis functions for the spaces Vj are called scaling functions, and are usually denoted by the symbolΦ.A simple basis for Vj given by the set of scaled and translated box functions [14]:

$$\Phi ij\,(x) := \Phi(2jx - i)\ i = 0, 1, 2\ldots..2j - 1 \text{ where}$$

$$\Phi(x) := \begin{cases} 1 & \text{for } 0 \le x < 1 \\ 0 & \text{otherwise} \end{cases}$$

The wavelets corresponding to the box basis are known as the Haar wavelets Fig. 2.5, given by

$$\Psi ji\,(x) := \Psi(2jx - i) \quad i = 0, 1, 2, \ldots\ldots..2j - 1 \text{ where}$$

$$\Psi\,(x) := \begin{cases} 1 & \text{for } 0 \le x < \tfrac{1}{2} \\ -1 & \text{for } \tfrac{1}{2} \le x < 1 \\ 0 & \text{otherwise} \end{cases}$$

By using HPF or LPF filters in one stage, an image is decomposed into four bands. There exist three types of detail images for each resolution: horizontal (HL), vertical (LH), and diagonal (HH). The operations can be repeated on the low low (LL) band using the second stage of identical filter bank. Thus, a typical 2D DWT, used in image compression, generates the hierarchical structure shown in Fig.2.3

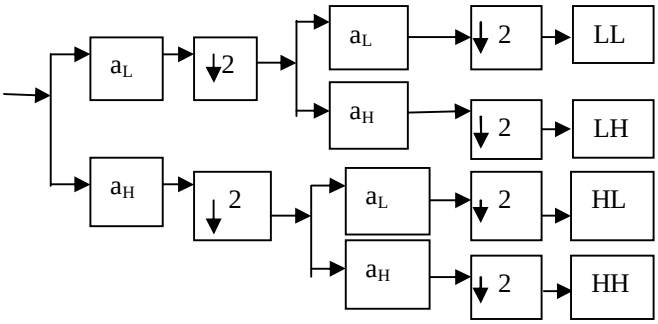


Fig. 2.3 One Filter Stage in 2D DWT

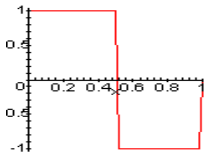


Fig. 2.4 Haar Wavelet

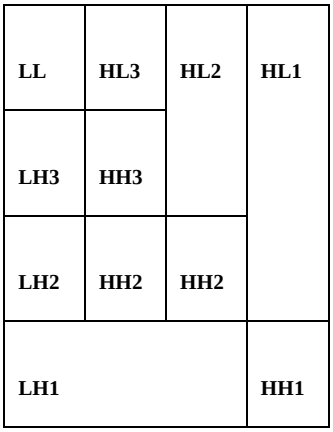


Fig. 2.5 Structure of wavelet decomposition

3. Image Encryption

Encryption is the process of transforming the information to insure its security. For confidential or private information different security techniques have been used to provide the required protection [14]. Image encryption techniques try to convert an image to another one that is hard to understand [4]. There are two major groups of image encryption algorithms: (a) non-chaos selective methods and (b) Chaos-based selective or non-selective methods.

Chaos theory is a scientific discipline that focuses on the study of nonlinear systems. The properties of chaotic systems are [2]:

i. Deterministic, this means that they have some determining mathematical equations ruling their behavior.
ii. Unpredictable and non-linear, this means they are sensitive to initial conditions. Even a very slight change in the starting point can lead to a significant different outcome.
iii. Appear to be random and disorderly hut in actual fact they are not. Beneath the random behavior there is a sense of order and patted.

Several papers regarding this have been published, most of which discussed about application of chaos encryption in secure communication for text-based messages as well as optical data [3, 4].

4. Related Work Done

Mitra A et al. [5] have proposed a random combinational image encryption approach with bit, pixel and block permutations.

Zhi-Hong Guan et al. [6] have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the compress image.

Sinha A. and Singh K. [7] proposed an image encryption by using Fractional Fourier Transform (FRFT) and Jigsaw Transform (JST) in image bit planes.

Shujun Li et al. [8] have pointed out that all permutation-only image ciphers were insecure against known/chosen-compress text attacks. In conclusion, they suggested that secret permutations have to be combined with other encryption techniques to design highly secured images.

Maniccam S.S. and Bourbakis N G. [9] proposed image and video encryption using SCAN patterns. The image encryption is performed by SCAN-based permutation of pixels and a substitution rule which together form an iterated product cipher.

Ozturk I. and Sogukpinar I. [10] proposed new schemes which add compression capability to the mirror-like image encryption MIE and Visual Cryptography VC algorithms to improve these algorithms.

Sinha A. and Singh K. [11] proposed a technique to encrypt an image for secure transmission using the digital signature of the image. Digital signatures enable the recipient of a message to authenticate the sender of a message and verify that the message is intact.

Droogenbroeck M.V. and Benedett R. [12] have proposed two methods for the encryption of an image; selective encryption and multiple selective encryptions.

Maniccam S.S., Nikolaos G. and Bourbakis. [13] have presented a new methodology, which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology.

5. The Proposed Technique

In the proposed technique the image is first converted into matrix form in which the color of each pixel is represented by a component of a matrix .The minimum of this matrix representing black ,and the maximum representing white. We will then use a process called averaging and differencing to develop a new matrix representing the same image in a more concise manner. To compress the image we will eliminate some of the unnecessary information, and arrive at an approximation of our original image. Now the compressed image is encrypted by a chaos function. It is a simple block cipher with block size of 8-bit and 256-bit secret key. The key is used to generate a pad that is then merged with the compressed text a byte at a time.

5.1 Procedure for Compression and Encryption

1. The image is converted into matrix.

2. Then we apply the averaging and differencing using linear algebra we can use three matrices (A1, A2, A3) that perform each of the three steps of averaging and differencing.

Step1: When multiplying the string by the first matrix (A1) the first four columns are taking the average of each pair, and the last four columns take the corresponding differences.

Step 2: The second matrix (A2) works much in the same way; the first four columns now perform the averaging and differencing to the remaining pairs and the identity matrix in the last four columns carry down the detail coefficients from step 1.

Step 3: Similarly in the final step, the averaging and differencing is done by the first two columns of the matrix (*A3*), and the identity matrix carries down the detail coefficients from step 2.

To simplify this process we can multiply these three matrices together to obtain a single transform matrix (*W=A1A2A3*).We can now multiply our original string by just one transform matrix to go directly from the original string to the final result of step 3.

In the following equations we simplify this process of matrix multiplication, first the averaging and differencing.

$$T = \left[(AW)^T\right] W$$
$$T = \left[W^T A^T W \right)^T$$
$$T = W^T (A^T)^T (W^T)^T$$
$$T = W^T AW \quad (1)$$

3. The compressed image is then encrypted using chaos function. For the encryption/decryption, we divide compress-text/cipher-text into blocks of 8-bits. Compress-text and cipher-text of i blocks can be represented as

$$P = P_1P_2P_3P_4 \ldots\ldots\ldots P_i \quad (2)$$
$$C = C_1C_2C_3C_4 \ldots\ldots\ldots C_i \quad (3)$$

4. The proposed image encryption process utilizes an external secret key of 256-bit long. Further, the secret key is divided into blocks of 8-bit each, referred as session keys.

$$K = K_1K_2K_3K_4 \ldots\ldots\ldots K_{64} \quad \text{(in hexadecimal)} \quad (4)$$

here, Ki's are the alphanumeric characters (0–4 and A–F) and each group of two alphanumeric characters represents a session key. Alternatively, the secret key can be represented in ASCII mode as

$$K = K_1K_2K_3K_4 \ldots\ldots\ldots K_{32} \quad \text{(in ASCII)} \quad (5)$$

here, each K_i represents one 8-bit block of the secret key i.e. session key.

5. The initial condition (X_0) for the chaotic map and the initial code C_0 are generated from the session keys as

$$R = \sum_{i=1}^{32} M1[Ki] \quad (6)$$
$$X_0 = R - \lfloor R \rfloor \quad (7)$$
$$C_0 = \left[\sum_{i=1}^{32} (Ki)\right] \bmod 256 \quad (8)$$

here *Ki* , $\lfloor\rfloor$, and *M1* are, respectively, the decimal equivalent of the ith session key, the floor function, and mapping from the session, key space, all integers between 0 and 255, into the domain of the logistic map, all real numbers in the interval [0,1].

6. Read a byte from the image file (that represent a block of 8-bits) and load it as compressed-image pixel P_i.

7. Encryption of each compressed-image pixel P_i to produce its corresponding cipher-image pixel C_i can be expressed mathematically as:

$$C_i = \left[Pi + M2\left\{ \sum_{r=1}^{\#i} rXi\,(1 - Xi) \right\} \right] \bmod 256$$

Where X_i represents the current input for logistic map and computed as:

$$X_i = M_1 [X_{i-1} + C_{i-1} + K_i] \quad (10)$$

$\#_i$ is the number of iteration of logistic map for its current input X_i and calculated as:

$$\#_i = K_{i+1} + C_{i-1} \quad (11)$$

And M_2 maps the domain of the logistic map, [0, 1], back into the interval [0,255].

8. Repeat steps 6-7 until the entire image file is exhausted.

5.2 Procedure for Decryption and Decompression

Decryption is very simple; the same pad is generated but this time un-merged with the cipher-text to retrieve the compressed-text. The decryption module receives an encrypted image (cipher-image) and the 256-bit secret key and returns to the compressed image. The compressed image is then decompressed by inverse haar wavelet transform to receive the original image. In particular, the decryption module works in the same way as the encryption module but now the output of the logistic map is subtracted from the corresponding cipher image pixel C_i providing the compressed image pixel Pi .Decryption of each cipher image pixel C_i to produce its corresponding compressed image pixel P_i can be expressed mathematically as:

$$Pi = \left[C_i + M_2 \left\{ \sum_{r=1}^{i} rXi(1 - Xi) \right\} \right] \mod 256$$

The compressed image is then decompressed by taking the inverse of the transform matrix and multiplying by the matrix T as in equation (1)

$$(W')^{-1} TW^{-1} = A$$
$$(W^{-1})' TW^{-1} = A$$

where, A is the original image matrix and W is the transform matrix.

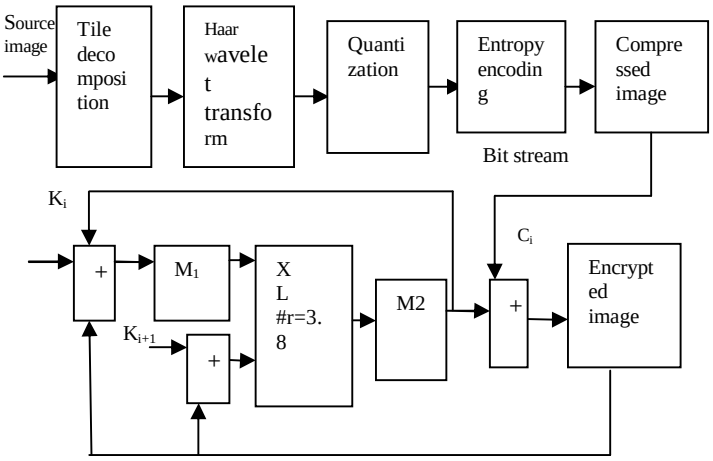
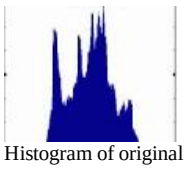


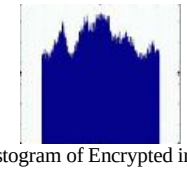
Fig. 3 Block diagram showing compression and encryption of image.

6. Results of Compression and Encryption

Original image compressed image Encrypted image



Histogram of original image



Histogram of Encrypted image

Table 2. Showing the compression factor

Name of the Image	Wavelet Transform
Lena	
Total No. of coefficients	**262144**
No. of coefficients used	**3586**
No. of coefficients discarded	**258558**
Compression Factor	**73.1020**

Table 3. Correlation coefficients in compress image/cipher image

Direction of adjacent pixels	Compress image	Cipher image
Horizontal	0.4405	0.0308
Vertical	0.4787	0.0304
Diagonal	0.4645	0-0317

Table 4: Enciphering speed test results of the Proposed Encryption algorithm

Image size (in pixels)	Colors	Encryption in Sec.
256 x 256	16	0.0010
256 x 256	256	0.0030
256 x 256	16777216	0.0267
512 x 512	16	0.0108
512 x 512	26	0.0358
512 x 512	16777216	0.1306

7. Conclusion and Future Work

A picture can say more than a thousand words. However, storing an image can cost more than a million words. This is not always a problem because now computers are capable enough to handle large amounts of data. However, it is often desirable to use the limited resources more efficiently. The rapid increase in the range and use of electronic imaging justifies attention for systematic design of an image compression system and for providing the image quality needed in different applications. Wavelet can be effectively used for this purpose. A low complex 2D image compression method using Haar wavelets as the basis functions along with the quality measurement of the compressed images have been presented here. Furthermore, finding out the exact number of transformation level required in case of application specific image compression can be studied. Also, thorough comparison of various still image quality measurement algorithms may be conducted. A new way of image encryption scheme also have been proposed which utilizes a chaos-based encryption scheme using the logistic map and an external secret key of 256 bit. The computation time was reduced rapidly because of encrypting only the most important coefficients and the security of encrypted image is still high enough. However, there is a loss of information when reconstructing the image because of omitting some details. Nevertheless, this encryption scheme can be applied to the real-time processes, such as encrypted videoconferences, R&D, security force, investigation bureau where the requirements to quality of reconstructed images are inferior.

References

[1] Jeffrey M. Gilbert, Robert W. Brodersen; “A Lossless 2-D Image Compression Technique for Synthetic Discrete- Tone Images”. University of California at Berkeley, Electrical Engineering & Computer Sciences Berkeley, CA 44720-1770.

[2] Chaos Mathematics.December2001.Citing Internet sources.

[3] Habutsu T., Nishio Y., Sasase I., and Mori S. A Secret Key Cryptosystem by Iterating a Chaotic Map, Proceedings of Eurocrypt'4: 127-140, 1441.

[4] Focus Systems. JAVA-Compatible Chaos Encryption A new Standard for IT Security. Financial Times 2001.

[5] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, p.127, 2006.

[6]G. Zhi-Hong, H. Fangjun, and G.Wenjie, "Chaos - based image encryption algorithm," Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2005, pp. 153-157.

[7] A. Sinha, K. Singh, "Image encrypt ion by us ing f r a c t iona l Fo ur i e r t r ans fo rm and J igs aw transform in image bit planes," Source: optical engineering, spie-int society optical engineering, vol. 44, no. 5, 2005, pp.15-18.

[8]Li. Shujun, Li. Chengqing, C. Guanrong, Fellow., IEEE., Dan Zhang., and Nikolaos,G., Bourbakis Fellow., IEEE. "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004,

[9]S.S. Maniccam, N.G. Bourbakis, "Image and video encryption using SCAN patterns," Journal of Pattern Recognition Society, vol. 37, no. 4, pp.725– 737, 2004.

[10] I. Ozturk, I. Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, 2004, p.38.

[11] A. Sinha, K. Singh, "A technique for image encryption using digital signature," Source: Optics Communications, vol.218, no. 4, 2003, pp.224-234.

[12] M. V. Droogenbroeck, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS’02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002.

[13] S .S .Ma n i c c am. , G.Nikolaos, and Bourbakis, "Lossless image compression and encryption using SCAN," Journal of: Pattern Recognition, vol. 34, no. 6:, 2001, pp.1224– 1245.

[14] H. El-din. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," enoufia University, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menouf-32952, Egypt, 2006.

Ranu Gupta has done B.Tech. , MBA (HRA), M.Tech. and pursuing Ph.D. Presently working as Assistant Professor in JUET, Guna (M.P), India.

Third Author is a member of Indian Science Congress