International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 638 - 643

An Image Compression– Encryption Hybrid Algorithm Using DWT and Chaos System

A. Ilakkiya[1]
M.PHIL Scholar Dept. of Computer Science [1]
Mother Teresa Women's University, Madurai
ilak.jcd@gmail.com

Dr. M. Pushparani[2]
Head Department of Computer Science
Mother Teresa Women's University,
Madurai

***Abstract*—** Recent developments of digital image production and applications have increases importance of digital image compression and security in today's world. The proposed method is developed to combine both compression and security of image. Compression is achieved by the deletion of redundant data. Discrete Wavelet Transform (DWT) is a in recent times developed compression technique in image compression. The existing methods to encrypt images usually treat the whole matrix as the key which makes the key too large to distribute and memorize or store. To solve this problem, in this proposed method key matrix is constructed using the logistic diagram and the Arnold transform is used for image position scrambling. Initially the original image is decomposed into bands and compressed by level dependent hard threshold technique and then combined with above encryption algorithms to get compressed-encrypted image. This algorithm produces a cipher for the test image that has good diffusion and confusion properties. Simulation results of the histogram analysis, key sensitivity analysis of adjacent pixels, PSNR, are representing the scrambling effect, security of the proposed algorithm and considerable compression performance.

Keywords- *image compression, encryption, Arnold transform, chaos system.*

*****

Introduction

During the last decade, the use of computer networks has grown-up enormously, and this growth continues unabated. Almost all networks are being installed, interconnected, and connected to the universal internet. Through internet more and more information has been transmitted. The information is not only text also audio, image, and other multimedia. As the developing of networks and multimedia communications technology, the problems of digital multimedia information security and intellectual property protection and authentication issues become increasingly prominent. For example, it is vital to protect the diagrams of army emplacements, the diagrams of bank building construction, and the important data captured by military satellites. In addition, the number of computer crimes has improved recently. Image security has become an important topic in the modern computer world. To solve those problems, the common method is image scrambling technology. In recent years, many researches of watermark preprocessing only confined to the location scrambling, and didn't guarantee the security. This paper puts forward an encryption algorithm combing Logistic chaos system and position scrambling system (Arnold transform), and reach a better effect. It can enhance the robustness of image encryption.

A. Compression

In modern day, many applications need large number of images for solving problems. Digital image [2] can be store on disk. This storing space of image is also important. Because less memory space means less time required to processing for image. Here the concept of image compression comes. "Image compression [2] means reduced the amount of data essential to represent a digital image". There are lot of applications [3] where the image compression is used to effectively increased efficiency and performance. Applications are like Health Industries, Retail Stores, Federal Government Agencies, Security Industries, Museums and Galleries etc.

The goal of image compression is to decrease the amount of data required to represent a digital image to decrease the large storage ability and transmission bandwidth. The Discrete wavelet transform (DWT) has gained well-known recognition in signal processing and image compression. The presentation of DWT based coding depends on the wavelet decomposition level and threshold value.

B. DWT Technique Arnold transformation

Wavelet analysis [2, 4, 6] can be used divided the information of an image into approximation and detailed subordinate signal [4]. The approximation subordinate signal shows the general trend of pixel value, and three detailed subordinate signal show vertical, horizontal and diagonal details or changes in image. If these detail is very small than they can be set to zero without considerably changing the image. If the number of zeroes is larger than the compression ratio is also greater. There is two types of wavelet is used. First one is Continues wavelet transform[2] and second one is Discrete wavelet transform.[2] Wavelet analysis is computed by filter bank. There is two type of filter

1) High pass filter: high frequency information is kept, low frequency information is lost.

2) Low pass filter: low frequency information is kept, high frequency information is lost.

So signal is successfully decomposed into two parts, a detailed part (high frequency) and approximation part(low frequency). Level 1 is approximation, Level2, 3, &4 are correspondingly horizontal, vertical and diagonal of the image signal.

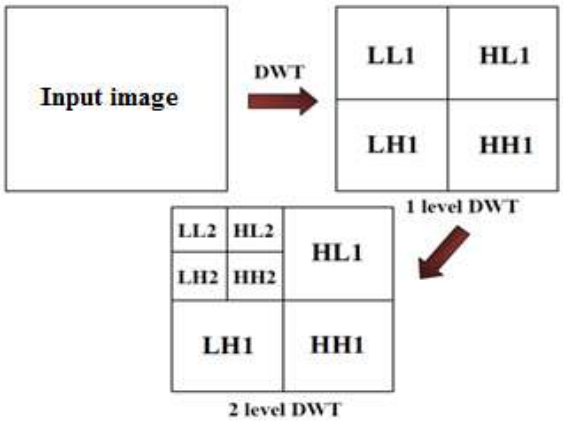

Fig.1.Two-level wavelet analysis

C. *Threshold coding Method*

In level dependent threshold coding method, each transform coefficient is compared with a threshold. If it is smaller than the threshold then it is set to zero. If it is larger then it will be retained. Different threshold values for different decomposition level are used. By applying hard threshold the coefficients lower this threshold level are zero, and the output after a hard threshold is functional and defined by this equation:

$$y_{hard}(t) = \{ \quad (1)$$

Where x(t), the input signal and T is the threshold.

D. *Logistic map*

Chaos system is often used in cryptography due to its pseudo randomness and sensibility to the initial condition, the definition of Logistic map is

$$X_{n+1} = \mu X_n (1 - X_n \quad (2)$$

It becomes chaotic when the parameter .

E. *Arnold transformation*

Arnold's Cat Map transformation applied to an image to randomly rearrange the pixels of the image. We can define Arnold transformation as follows. Let (x,y) is pointing in the unit square. Its move to (x',y') by the following equation and n is the order of the image.

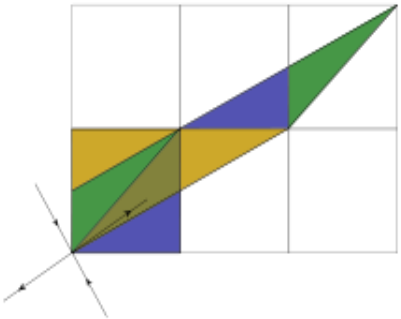

Fig.2. The linear map stretches the unit square and its pieces rearrangement

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \quad (3)$$

Fig.2. showing how the linear diagram stretches the unit square and how its pieces are rearranged when the modulo action is performed. The lines with the arrows show the direction of the toning and increasing eigen spaces.

II. THE PROPOSED IMAGE COMPRESSION–ENCRYPTION ALGORITHM

A. *Key matrix generation*

The Key matrix is constructed as a circulate matrix. The original row vector of the circulate matrix is controlled by the logistic chaos map. The steps are as follows [1]:

1. A sequence with length 2N by logistic map with initial condition X_{01} is generated; abandon the preceding N elements to obtain the sequence, which are used as the initial row vectors of the circulate matrices.
2. The circulate matrix is constructed with the initial row vectors. To reduce the relevance among the column vectors, the first element of vector will be the result of multiplying by , where 2 < i < M and > 1, and the iteration:

$$\Phi(i,1) \quad (4.1)$$
$$\Phi(i,2{:}N) = \Lambda * \Phi(i - \quad (4.2)$$

Image compression – encryption algorithm

The proposed algorithm is suitable for the image whose width equals to height like the size of input image is N N. The proposed method is shown in Fig.3a and b, and the image compression – encryption steps are as follows:

1 Decompose the original image into 4 bands, band 1 (lower), band 2, 3 and 4(higher), as shown in Fig.3a, thus each band is of the size (N/2, N/2) using DWT.
2 Generate the compressed image by applying level dependent hard threshold technique.
3 Construct two (N/2 N/2) key matrices, and , with keys X_{01} and X_{02}, and multiple with the bands as shown in Fig.3. C1, C2, C3 and C4 are the encrypted matrices corresponding to band1, band2, band3 and band4.
4 Scramble the bands by the Arnold transform with iteration1 and iteration 2 as show in Fig.3a. A1, A2, A3 and A4 are the scrambled matrices corresponding to band1, band2, band3 and band4. Image A is the compressed encrypted image

The decryption and reconstruction process are shown in Fig.3b. First the inverse Arnold transform performed and then the key removed to produce the image bands. Next Inverse DWT is applied to produce the reconstructed image.

III. SYSTEM MODELS

The system model contains 4 main modules.They are Input, DWT, Key Matrix Generation,Arnold transform,Encrypted Image.

A. INPUT IMAGE

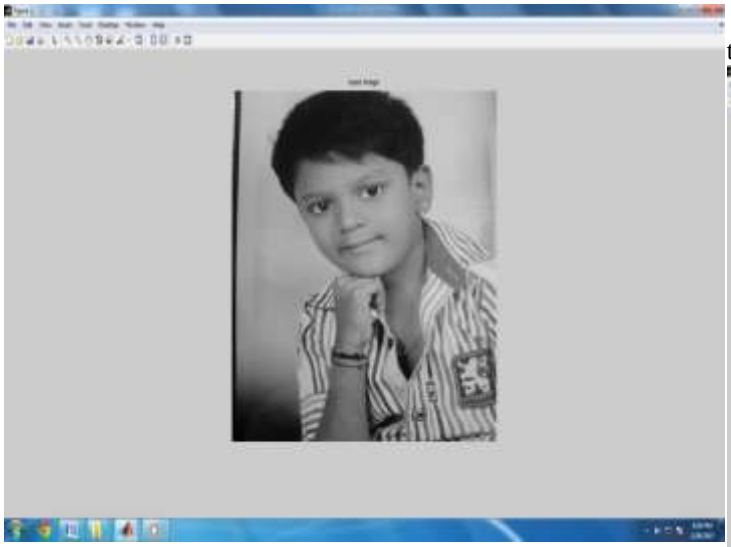

Fig.4.1. INPUT IMAGE

B. DWT

A **discrete wavelet transform** is used to decompose the image.

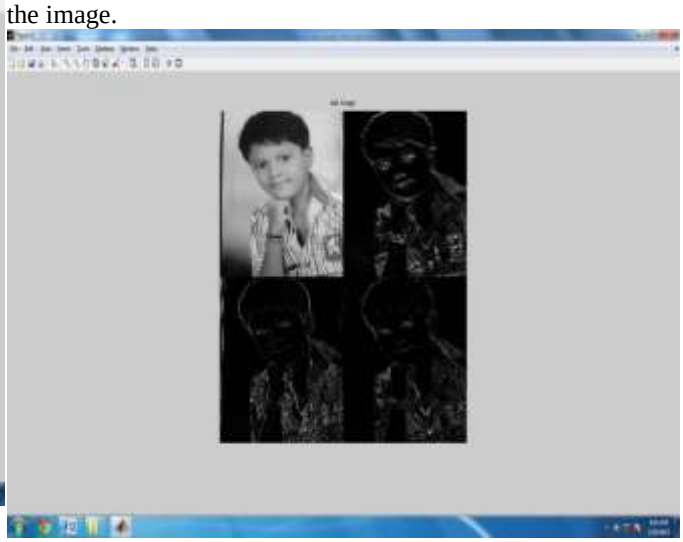

Fig.4.2. DWT IMAGE

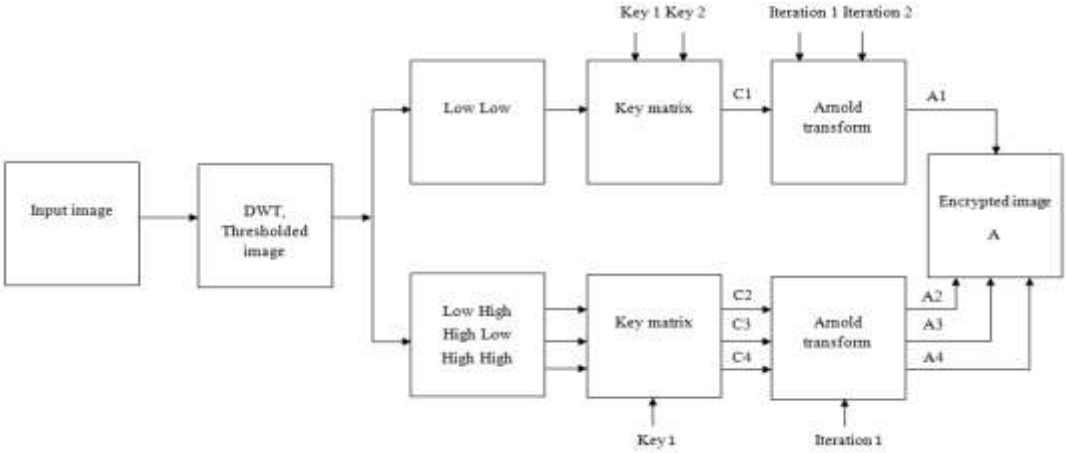

Fig.3.a. Process flow of the encryption algorithm

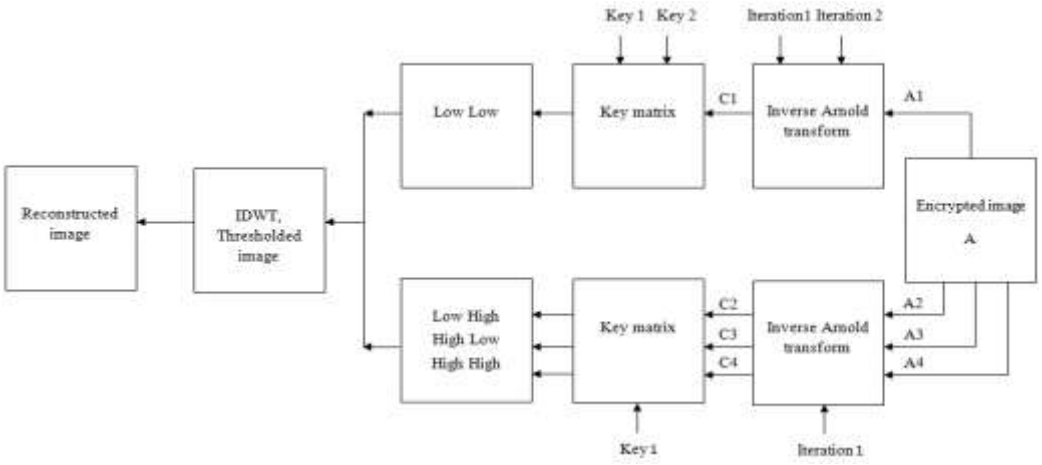

Fig.3.b. Process flow of the decryption algorithm

C.

D. *KEY MATRIX GENERATION*

Chaos system is used to create key matrix for encryption.

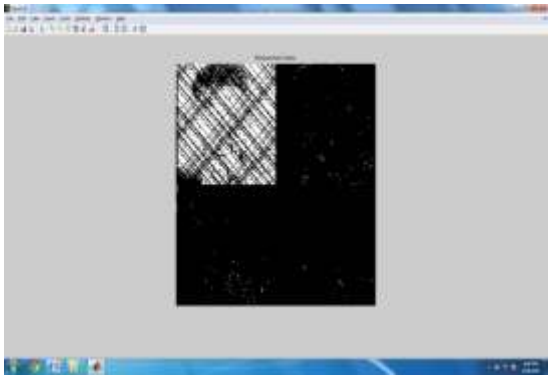

Fig.4.3. MEASUREMENT MATRIX

E. *ARNOLD TRANSFORM*

The pixels of the blocks are scrambled by **Arnold transform**.

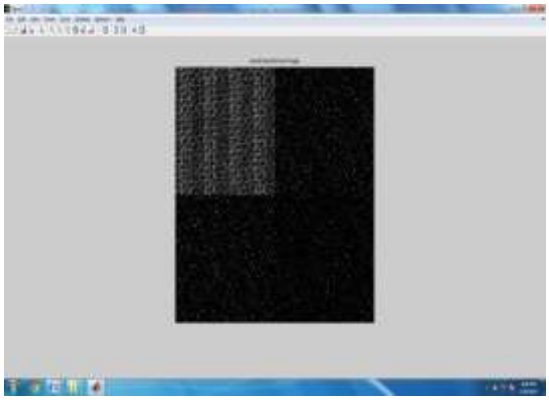

Fig.4.4. ARNOLD TRANSFORM IMAGE

F. *OUTPUT IMAGE*

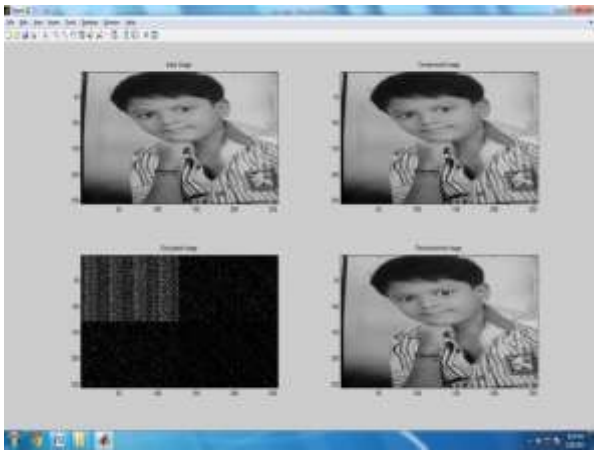

Fig.4.5.(a). Input Image Fig. (b). Compressed Image

Fig.(c). Encrypted Image Fig.(d). Reconstructed Image

IV. EXPERIMENTAL ANALYSIS AND RESULTS

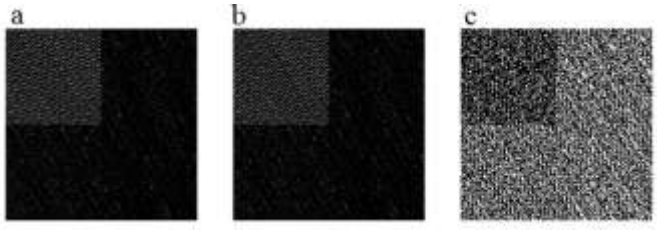

Fig.6. (a) Encrypted Image using X_{01} = 0.11 and X_{02} = 0.23; (b) encrypted Image using X_{01} + = 0.11 + 1 10^{16} and X_{02} = 0.23; and (c) difference between two encrypted images (a) and (b).

Table 1
Correlation coefficients of adjacent pixels.

[1]	***Correlation coefficient***	[2]	***Horizontal***	[3]	***Vertical***	[4]	***Diagonal***
[5]	Input image	[6]	0.9590	[7]	0.9217	[8]	0.9071
[9]	Existing method	[10]	0.0846	[11]	0.0583	[12]	0.0931
[13]	Proposed method	[14]	**0.0624**	[15]	**0.0108**	[16]	**0.0608**
[17]	Input image	[18]	0.9585	[19]	0.9529	[20]	0.9064
[21]	Existing method	[22]	0.0639	[23]	0.0539	[24]	0.0848
[25]	Proposed method	[26]	**0.0323**	[27]	**0.0274**	[28]	**0.0527**

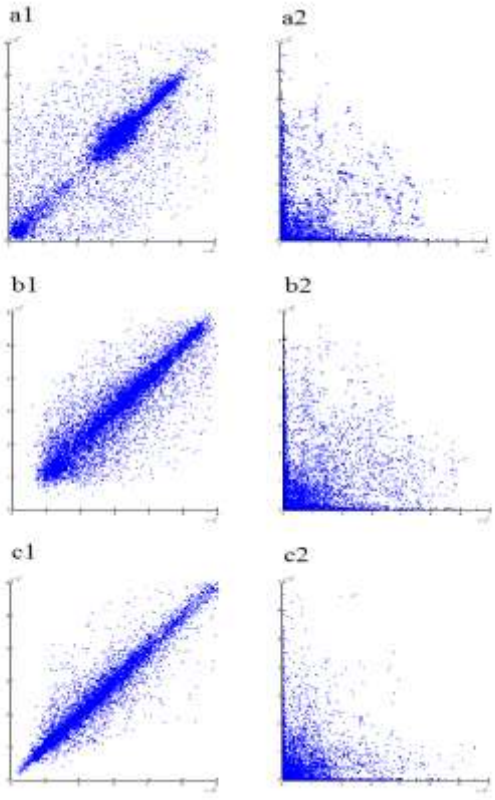

Fig.7. Correlation distribution of two horizontally adjacent pixels in (a1) original Lena; (a2) encrypted Lena; (b1) original Cameraman; (b2) encrypted Cameraman; (c1) original Peppers; and (c2) encrypted Peppers.

A. *Histogram*

The image histogram is often used to analyze the performance of the image encryption algorithm. It is the best when the values in the histogram of the encrypted image are fairly uniform in distribution or the second best when the histograms of different encrypted images are similar to each other. Fig. 5(a1), (b1) and (c1) are the histograms of Lena, Cameraman and Peppers, respectively. And Fig. 5(a2), (b2) and (c2) are the histograms of their encrypted images, correspondingly.

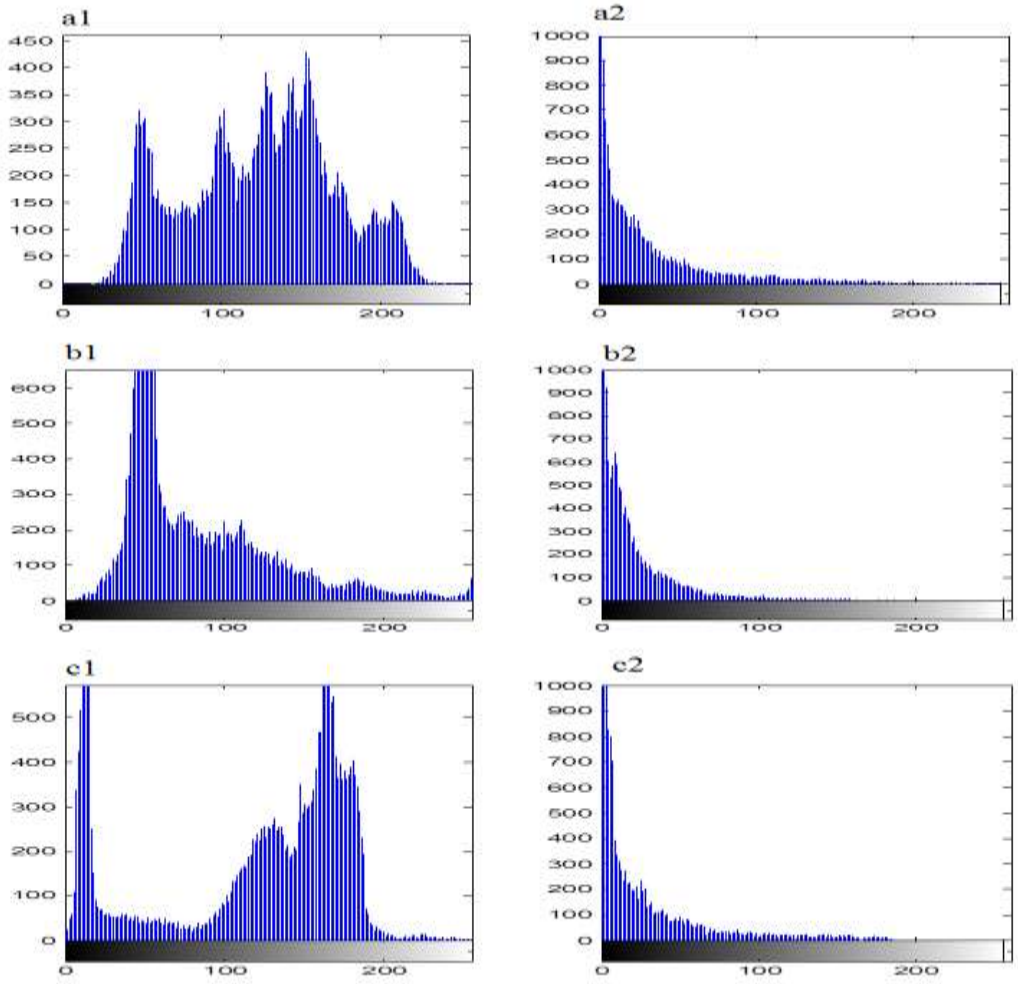

Fig.5. Histogram: (a1) Lena; (a2) encrypted Lena; (b1) Cameraman; (b2) encrypted Cameraman; (c1) Peppers; and (c2) encrypted Peppers.

The histograms of the two original images are obviously different from each other, while their encrypted images have similar histograms. After a large number of parallel experiments, shows that the histograms of the cipher texts of different original images are similar to Fig. 5(a2), (b2) and (c2). That is to say, the proposed algorithm can frustrate the statistical analysis attack.

B. *Key space*

An image encryption algorithm should be secure even though everything is known except for the key. Thus a good encryption algorithm should have a large enough key space. In the proposed algorithm, X_{01} and X_{02} are used as keys. Here, the key space is calculated for X_{01} as generate two different sequences and by using X_{01} and X_{01} + as initial values and both sequences are of length N, and define mean absolute error between the two sequences as [14]

$$MAE\left(\delta, \bar{\delta}\right) \quad (5)$$

The key space for X_{01} is equal to $(1/\chi_0)$, where χ_0 is the value of χ for MAE = 0. The simulation results show that χ_0 comes out to be 1×10^{17}, i.e., the key space of X_{01} is 1×10^{17}. Similarly, the key space of X_{02} is 1×10^{17}. Thus, the total key space is as large as 10^{85}. If one wants to construct the correct measurement matrix by exhausting the keys, she must

calculate 10^{85} times which would take much time. Thus the proposed algorithm is secure against brute-force attack.

C. *Correlation of two adjacent pixels*

The correlation of two adjacent pixels in a meaningful image is usually close to 1, while that of the encrypted image should be close to 0. To measure the correlations between two adjacent pixels in the horizontal, vertical and diagonal directions, 16,000 adjacent pixel pairs are selected randomly from original image and encrypted image, correspondingly. original image and the disordered distribution reflects the

weak correlation between two adjacent pixels in the encrypted image. And the distributions of vertical and diagonal directions share the similar modality. The correlation coefficient is

$$r_{xy} = \frac{\sum_i^l}{} \quad (6)$$

Where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$. The quantitative evaluation on correlation is compiled in Table 1. That shows that the proposed algorithm removes the tight relationship between adjacent pixels of the original image successfully. The results demonstrate that the attackers cannot obtain useful information by statistical analysis and the proposed algorithm can resist statistical analysis.
analysis the mean square error (MSE) [13] between decrypted image and original image is calculated as

$$MSE = \frac{1}{M \times N}\sum_{x,y}[I(x,y) \quad (7)$$

where M × N represents the total number of image pixels, *I*(*x*, *y*) and *D(x, y)* denote the values of input image and output image at the pixel *(x , y)*, respectively. The sensitivity can also be tested by comparing two encrypted images obtained by using neighbor keys. Fig. 7(a) and (b) shows the encrypted its neighbor keys $X_{01} = 0.21 + 1 \quad 10^{16}$, $X_{02} = 0.35$, respectively. And the difference between these two encrypted images is shown in Fig. 7(c). The tiny change in the keys results in great changes in the encrypted image. From the above two cases, the proposed algorithm is sensitive enough to the keys.

V. CONCLUSION

In this paper a hybrid algorithm for compression-encryption has been proposed which based on key matrix and chaos system with Arnold transform. The image is decomposed into 4 bands to compress and encrypt. Then the compressed image is encrypted by chaos system with Arnold transform. By using the chaos system the original key circulant matrix is constructed and controlled, the proposed method is secure. By using Arnold transform the compressed and encrypted image is scrambled, the security is enhanced further. The encrypted image is analysised from histogram, key sensitivity, PSNR and correlation of adjacent pixels, which shows that the proposed method resists to different attacks. Since this algorithm uses the number of Arnold transformation and the initial value of Logistic chaos system as the key, the key space is big, and has a strong sensitivity. From the simulation results the proposed algorithm is secure and can provide good compression.

VI. REFERENCES

[1] Nanrun Zhou, Aidi Zhang, Fen Zheng, Lihua Gong "Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," Optics & Laser Technology 62 (2014)152–160 .

[2] Rafael C. Gonzalez, Richard E. Woods. (1992), Digital Image Processing(2nd edition), NJ:Prentice Hall

[3] Locker Gnome (2011), "Real World Application Of Image Compression," http://www.lockergnome.com/nexus/windows/2006/12/25/real-world-applications-of- image compression/ [accesed 11 Dec 2011].

[4] Swastik Das and Rashmi Ranjan Sethy, "A Thesis on Image Compression using Discrete Cosine Transform and Discrete Wavelet Transform," Guided By: Prof. R. Baliarsingh, dept of Computer Science & Engineering, National Institute of Rourkela.

[5] Pavan Kumar Goswami, Namita Tiwari, Meenu Chawla, "Block Based Image Encryption Using Iterative Arnold Transformation," International Journal of Advanced Research in Computer Science and Software Engineering 3(8), August - 2013, pp. 273-278

[6] Karen Lees "Image compression using Wavelets," Report of M.S. 2002.

[7] B. Bhargava, C. Shi, and S. Y.Wang, "MPEG video encryption algorithms," Multimedia Tools and Applications, vol. 24, no. 1, pp. 57–79, 2004.

[8] A. Cohen and J. Kovacevic, "Wavelets: the mathematical background," Proceedings of the IEEE, vol. 84, no. 4, pp. 514–522, 1996.

[9] Wangsheng Fang1, Lulu Wu1,Rong Zhang1, "A Watermark Preprocessing Algorithm Based on Arnold Transformation and Logistic Chaotic Map," Advanced Materials Research Vols. 341-342 (2012) pp 720-724

[10] Pavan Kumar Goswami, Namita Tiwari, Meenu Chawla, "Block Based Image Encryption Using Iterative Arnold Transformation", International Journal of Advanced Research in Computer Science and Software Engineering 3(8), August - 2013, pp. 273-278

[11] Lu P, Xu ZY, Lu X, Liu XY. "Digital image information encryption based on compressive sensing and double random-phase encoding technique." Optik-Int J Light Electron Opt 2013;124:2514–8.

[12] Takanori N, Bahram J. Optical encryption system with a binary key code. Appl Opt 2000;39:4783–7.

[13] Chu Hui Lee and Zheng Wei Zhou, "Comparison of Image Fusion based on DCT-STD and DWT-STD," IMECS Vol I, March 14-15, 2012, Kong Kong.

[14] Hennelly BM, Sheridan JT. Image encryption and the fractional Fourier trans-form. Proc SPIE – Int Soc Opt Eng 2003;5202:76–87