ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 5, May 2015*

# Secured Color Image Compression and Efficient Reconstruction Using Arnold Transform with Chaos Encoding Technique

**D. Venugopal [1], M.Gunasekaran [2], A.Sivanatharaja [3]**

Associate Professor, ECE Department, KLN College of IT, Madurai, Tamilnadu, India[1]

M.E. Student, Department of CN, KLN College of IT, Madurai, Tamilnadu, India[2]

Associate Professor, Department of ECE, A.C.Technology, Karaikkudi, Tamilnadu, India[3]

**Abstract**: Secured image compression is the key issue in image transmission applications. This paper proposes the idea of combining both compression and security of an image. In the existing methods to encrypt images, the key size is too large since the whole matrix is considered as the key. To solve this problem, encryption through key controlled matrix is constructed using the logistic map in this proposed method. Then Arnold transform is used for image location scrambling. First the input image is decomposed into bands and compressed by level dependent hard threshold method and then combined with above encryption algorithms to get compressed-encrypted image. This algorithm produces a cipher for test images that have good diffusion and confusion properties. Simulation results of histogram analysis, key sensitivity analysis of adjacent pixels and PSNR shows the enhanced security and effectiveness of the proposed algorithm and reasonable increase in compression performance.

**Keywords**: Arnold transforms chaos system, encryption, and Image compression.

## I. INTRODUCTION

During the last decade, the use of computer networks has grown enormously and this growth continues unabated. Hence the problems of digital multimedia information storage, security, intellectual property protection and authentication issues become increasingly prominent. Among them compressed image security finds an inevitable place due to the increased number of computer crimes. For example, it is important to protect the diagrams of army emplacements, the diagrams of bank building construction and the important data captured by military satellites, etc. This paper puts forward an encryption algorithm combining Logistic chaos system and position scrambling system (Arnold transform) and can enhance the robustness of image encryption.

## II. LITERATURE REVIEW

With the recent development of multimedia technology, lot of information comes from images. The security of images becomes a serious issue and there are number of image encryption algorithms were proposed. For example, Chen et al. proposed a novel image compression–encryption algorithm which is based on key-controlled measurement matrix using choas system in compressive sensing [1], where the input image is divided into bands and compressed – encrypted combinedly using random pixel exchange in compressive sensing. Here in this paper the DWT is chosen based on the comparison performed by Anitha S [3]. Karl Martin et al. proposed [5] an efficient method for encrypting still color images based on the principle of partial or selective encryption, this scheme based on the color set partitioning in hierarchical trees (C-SPIHT) compression algorithm and a stream cipher to produce a secure, coded image. Hilton et al. [6] proposed method shows effectiveness of a new Partial Discharge denoising approach based on spatial correlations of Wavelet Transform coefficients along decomposition levels. Fang et al.[8] employed both Aronld transform and chaotic map system for encryption. Several image encryption algorithms based on CS have been proposed. For example, compressive sensing was introduced in an image encryption method based on double random-phase encoding to lower the encryption data volume due to the dimensional decrease properties of CS [9]. Based on the method in [9], the Arnold transforming was introduced later to enhance the security [10]. Huang and Sakurai divided the original image to blocks and vectorized each block to one-dimensional vectors, and then encrypted and compressed these vectors with CS and block Arnold scrambling [11].

## III. TECNICAL BACKGROUND

### *A. DWT Technique*

Wavelet analysis [2] can be used to divide the information of an image into approximation and detailed sub signal [4]. The approximation sub signal shows the general trend of pixel value and three detailed sub 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 significantly changing the image. If the number of zeroes is greater, then the compression ratio is also greater. Recommended font sizes are shown in Table 1.

So signal is effectively decomposed into two parts, a detailed part (high frequency) and approximation part (low frequency). LL1 is approximation, HL1, LH1 & HH1 are

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 5, May 2015*

respectively horizontal, vertical and diagonal of the image signal. Figure.1. shows 2 level dwt.

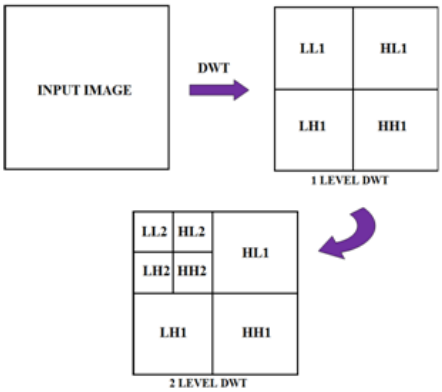


Fig. 1. Two-level wavelet analysis

*B. Threshold coding Method*

In level dependent threshold coding [6 & 7] 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 below this threshold level are zeroed, and the output after a hard threshold is applied and defined [13] by this equation:

$$y_{hard}(t) = \begin{cases} x(t), |x(t)| > T \\ 0, \text{other wise} \end{cases} \quad (1)$$

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

*C. Logistic map*

Chaos system [1 & 8] is often used in cryptography due to its pseudo randomness and sensibility to the initial condition, the definition of Logistic map is

$$X_{n+1} = \mu X_n (1 - X_n),\ X_n \in (0,1). \quad (2)$$

It becomes chaotic when the parameter μ lies in the interval [3.57,4].

*D. Arnold transformation*

Arnold's Cat Map transformation [5, 8, & 10] applied to an image to randomly rearrange the pixels of the image. Arnold transformation is defined as follows. Let (x, y) is pointing in the unit square and it moves to (x', y') by the following equation where n is the order of the image.

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

Figure.2. shows how the linear map stretches the unit square and how its pieces are rearranged when modulo operation is performed. The lines with the arrows show the direction of the contracting and expanding Eigen spaces.

## IV. PROPOSED SYSTEM

*A. Key matrix generation*

The key is generated as a circulant matrix in which the original row vector is controlled by the logistic chaos map. The process is given as steps:

- A sequence with length 2N by logistic map with initial condition K1 is generated; to obtain the initial row vector of the circulant matrices abandon the preceding N elements.
- With the initial row vectors the circulant matrix $\Phi$ is constructed. The relevance among the column vectors are reduced by multiplying $\Phi(i-1, N)$ by Λ, which gives the first element of vector $\Phi(i, N)$, where 2 < i < M and Λ > 1, and the iteration:

$$\Phi(i, 1) = \Lambda * \Phi(i-1, N) \quad (4.1)$$

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

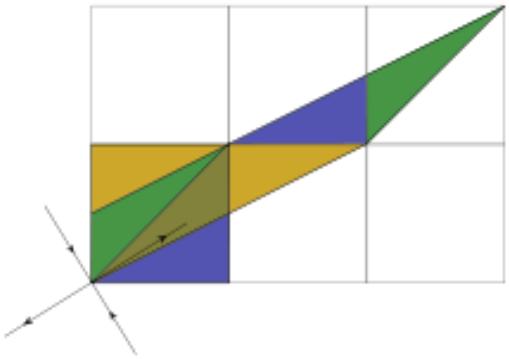

Fig. 2. The linear map stretches the unit square and its pieces rearrangement.

*B. Image compression–encryption algorithm*

The proposed algorithm is fit for the image whose width equals to height as N × N. Encryption and decryption process are interpreted diagrammatically in Fig.3 & 4 and the image compression – encryption procedure is given as follows:

1) Decompose the input image using DWT into 4 bands, band 1 (lower), band 2, 3 and 4(higher) and thus each band will have the size (N/2, N/2).
2) Generate the compressed image by applying level dependent hard threshold method.
3) Separate the RGB coordinate from the compressed image.
4) Construct two (N/2 × N/2) key matrices $\Phi_1$ and $\Phi_2$, with keys K1, K2 and K3 and multiply them with bands. C1, C2, C3 and C4 are the encrypted matrices corresponding to band1, 2, 3 and 4 respectively and RK, GK and BK are the encrypted image of RGB coordinates respectively.
5) Scramble the bands by Arnold transform with two iterations resulting in scrambled matrices A1, A2, A3 and A4 and RA, GA and BA are the Arnold transformed image of the RGB coordinates.
6) RA, GA and BA are combined to get the compressed−encrypted image A.

## V. EXPERIMENTAL ANALYSIS AND RESULTS

The standard gray image 'Lena' with resolution 256 × 256 is taken as the sample input image. After DWT, the size of each block becomes128 × 128.The simulation parameters are T = 3.5, Λ = 2, K1= 0.11, K2 = 0.33, K3 = 0.51, μ = 3.99, I1= 3, I2 = 9, I3 = 24 and the compression ratio is 4/3 (N = (3/4 × N/2) = 96). The encrypted and the decrypted images are shown in Fig. 5. If the whole key matrices are considered as the key, then the key length would be N × N. For example, for same test image, the size of key matrix will be 3 × 256 × 256, but here the key

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 5, May 2015*

length is reduced to 6. Thus this proposed method shortens the key length greatly without much increase in computational complexity when compared with similar methods. There are 3 × 192 times float number add operations, 96 × 96 × 2 times shift operation and 3 × 96 × 96 × 5 times float number multiplication operations in generating encryption matrix 3 × 96 × 96 × 5 times scrambling operations and 3 × 96 × 96 × 5 times mod operation in the Arnold transform.

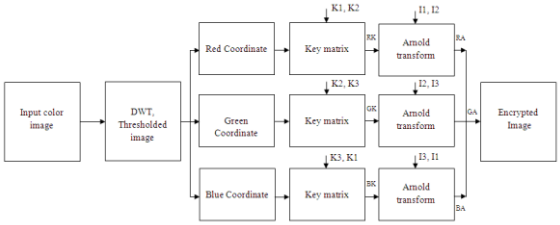


Fig. 3: Process flow of the proposed encryption algorithm

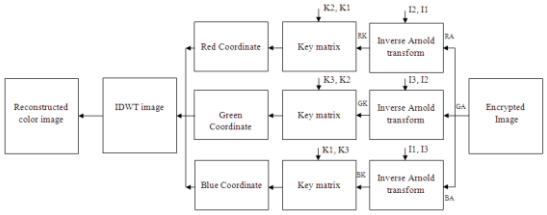


Fig. 4: Process flow of the proposed decryption algorithm

### *A. Histogram Analysis*

The histogram representation for input images and encrypted images are shown in Fig.6. Figure.6. (a1), (a2) and (a3) are the histograms of Lena, Peppers and Mandrill, respectively and Fig. 6(b1), (b2) and (b3) are the histograms of their encrypted images, correspondingly. It is inferred that the histogram of the input images are varying but the encrypted images are similar. Other than the samples given here, the experimentation is performed with many numbers of different images with different parameters. Then it is observed that this algorithm would produce similar histogram values such that the attacker cannot predict the input image which ultimately increases the security. The uniqueness of this proposed method is it reduces the histogram values of encrypted images significantly which implies that it contains low intensity values that intruders won't easily hack it.

### *B. Computation of correlation coefficient*

The correlation coefficient is

$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{D(x)}\sqrt{D(y)}}. \quad (5)$$

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 correlation coefficients are computed and represented graphically in Fig.7. The values are tabulated in Table 1. Correlation between adjacent pixels should be zero or minimum for the encrypted images to ensure the security. By random selection of adjacent pixels from original image and encrypted image, the correlation coefficient is computed in horizontal, vertical and diagonal directions. The high correlation in original images and the low correlation in encrypted images are observed by the distribution obtained in Fig.7. a1, a2, b1, b2, c1 & c2.

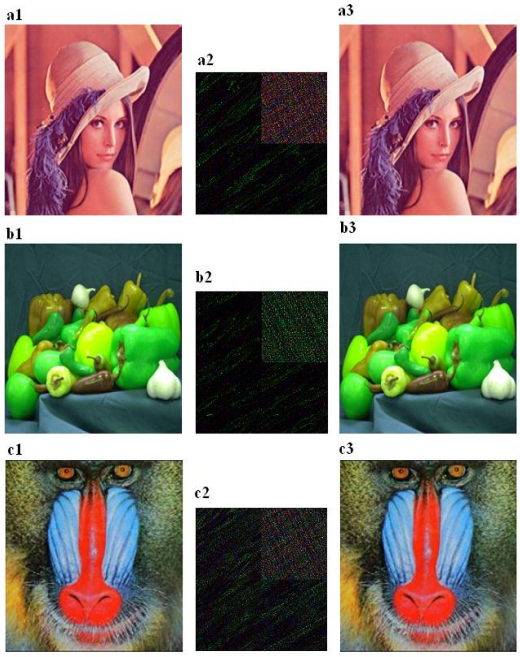


Fig. 5: (a)input images;(b)encrypted images; and(c)correct decrypted images.

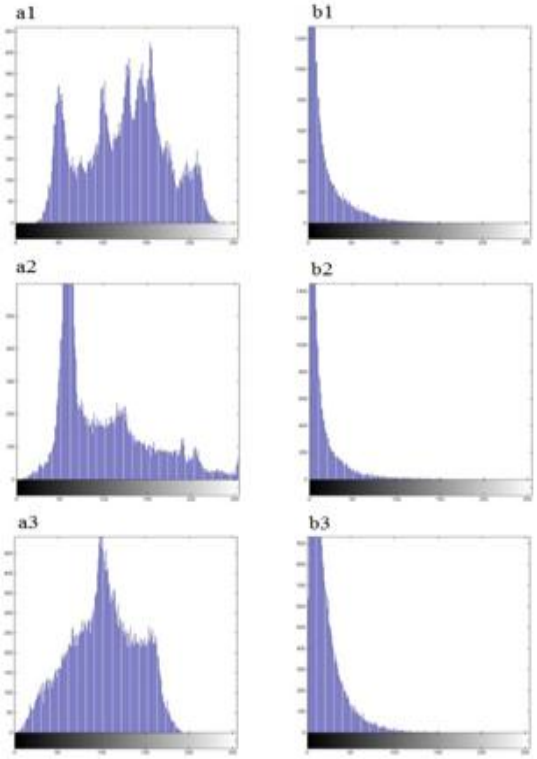


Fig. 6: Histogram: (a1) Lena; (b1) encrypted Lena; (a2) Peppers; (b2) encrypted Peppers; (a3) Mandrill; and (b3) encrypted Mandrill.

Compared with the similar work in [1] the correlation coefficient values are reduced and approaching zero as in Table 1 and similarly for medical images are shown in

Table 2. The results imply that the attackers cannot predict the present values from statistics.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 5, May 2015*

TABLE:I CORRELATION COEFFICIENTS OF ADJACENT PIXELS FOR STANDARD IMAGES.

| Sl. No | Correlation coefficient for | Horizontal | Vertical | Diagonal |
|---|---|---|---|---|
| 1 | Lena image | 0.9590 | 0.9217 | 0.9071 |
| | **Proposed method** | **0.0514** | **0.0308** | **-0.0495** |
| 2 | Peppers image | 0.9585 | 0.9529 | 0.9064 |
| | **Proposed method** | **-0.0585** | **0.0303** | **-0.0144** |
| 3 | Mandrill image | 0.9528 | 0.9278 | 0.9126 |
| | **Proposed method** | **0.0576** | **-0.0432** | **-0.0351** |
| 4 | Splash image | 0.9871 | 0.9899 | 0.9829 |
| | **Proposed method** | **-0.0488** | **0.0529** | **-0.0476** |
| 5 | Tiffany image | 0.9545 | 0.9738 | 0.9147 |
| | **Proposed method** | **0.0580** | **0.0463** | **-0.0730** |
| 6 | Bandon image | 0.9942 | 0.9833 | 0.9781 |
| | **Proposed method** | **-0.0507** | **0.0396** | **0.0087** |
| 7 | F16 image | 0.9506 | 0.9364 | 0.8866 |
| | **Proposed method** | **0.0619** | **0.0354** | **-0.0702** |
| 8 | House image | 0.9671 | 0.9597 | 0.9126 |
| | **Proposed method** | **0.0577** | **0.0448** | **-0.0670** |
| 9 | Jelly beans image | 0.9734 | 0.9801 | 0.9478 |
| | **Proposed method** | **0.0579** | **0.0341** | **-0.0502** |
| 10 | Girl image | 0.9729 | 0.9635 | 0.9482 |
| | **Proposed method** | **0.0480** | **-0.0295** | **-0.0607** |
| 11 | Pills image | 0.9292 | 0.9426 | 0.8991 |
| | **Proposed method** | **0.0564** | **-0.0448** | **-0.0651** |
| 12 | Watch image | 0.9361 | .9440 | 0.9141 |
| | **Proposed method** | **-0.0440** | **-0.0327** | **-0.0340** |
| 13 | Terraux image | 0.9515 | 0.9640 | 0.9340 |
| | **Proposed method** | **-0.0668** | **-0.0475** | **-0.0392** |
| 14 | Water image | 0.9306 | 0.9256 | 0.8950 |
| | **Proposed method** | **-0.0122** | **0.0077** | **-0.0432** |
| 15 | Tree image | 0.9590 | 0.9425 | 0.9159 |
| | **Proposed method** | **0.0416** | **0.0368** | **-0.0482** |

*C. Key space*

The key space is calculated for K1 as generate two different sequences $\delta$ and $\bar{\delta}$ by using K1 and K1 + $\chi$ as initial values and both sequences are of length N, and define mean absolute error between the two sequences as [12]

$$\mathrm{MAE}(\delta, \bar{\delta}) = \frac{1}{N}\sum |\delta - \bar{\delta}|. \qquad (6)$$

The key space for K1 is equal to $(1/\chi_0)$, where $\chi_0$ is the value of $\chi$ for MAE = 0. The simulation results show that $\chi_0$ comes out to be $1 \times 10^{17}$, i.e., the key space of K1 is $1 \times 10^{17}$. Similarly, the key space of K2 is $1 \times 10^{17}$. Thus, the key space is $10^{34}$ for Low-Low band and $1 \times 10^{17}$ for the other three Low-High, High-Low and High-High bands. It will be $10^{51}$ for these three bands and a total of $10^{85}$ .This large key space will prevent brute-force attack. Most importantly the key space is $10^{51}$ expanded when compared with existing work.

*D. Key sensitivity analysis*

The proposed method is key sensitive since the original row vectors of circulant matrices are controlled by the logistic map and the interaction of the Arnold transform. It is tested by comparing two encrypted images obtained by using neighbor keys. Figure.8(a) and (b) shows the encrypted images with K1 = 0.11, K2 = 0.33 and K3 = 0.51 and its neighbor keys K1 = 0.11 + $1 \times 10^{-16}$, K2 = 0.33 and K3 = 0.51, respectively and the difference between these two encrypted images is shown in Fig. 8(c). It is clearly seen there is much difference visually in the appearance.

TABLE II CORRELATION COEFFICIENTS OF ADJACENT PIXELS FOR MEDICAL IMAGES.

| Sl.no | Correlation coefficient | Horizontal | Vertical | Diagonal |
|---|---|---|---|---|
| 1 | Image 1 | 0.9559 | 0.9369 | 0.9336 |
| | **Proposed method** | **0.0541** | **-0.0092** | **0.0127** |
| 2 | Image 2 | 0.9631 | 0.9367 | 0.9242 |
| | **Proposed method** | **0.0579** | **0.0024** | **0.0299** |
| 3 | Image 3 | 0.9551 | 0.9335 | 0.929 |
| | **Proposed method** | **0.0632** | **-0.0155** | **0.0147** |
| 4 | Image 4 | 0.9785 | 0.9798 | 0.9669 |
| | **Proposed method** | **0.1064** | **-0.033** | **0.0402** |
| 5 | Image 5 | 0.9809 | 0.9821 | 0.9703 |
| | **Proposed method** | **0.01** | **0.0069** | **-0.0142** |
| 6 | Image 6 | 0.9441 | 0.9508 | 0.9179 |
| | **Proposed method** | **0.0908** | **0.0541** | **0.0789** |
| 7 | Image 7 | 0.9552 | 0.9508 | 0.9219 |
| | **Proposed method** | **0.0884** | **0.0531** | **0.0706** |
| 8 | Image 8 | 0.9549 | 0.9604 | 0.9301 |
| | **Proposed method** | **0.0466** | **0.0281** | **0.0126** |
| 9 | Image 9 | 0.9176 | 0.9085 | 0.8622 |
| | **Proposed method** | **0.0776** | **0.0647** | **0.0385** |
| 10 | Image 10 | 0.9658 | 0.9636 | 0.9387 |
| | **Proposed method** | **0.016** | **0.0201** | **0.0176** |
| 11 | Image 11 | 0.9640 | 0.9652 | 0.9377 |
| | **Proposed method** | **0.0154** | **0.0022** | **-0.0046** |
| 12 | Image 12 | 0.9664 | 0.9792 | 0.9565 |
| | **Proposed method** | **0.0776** | **0.0538** | **0.066** |
| 13 | Image 13 | 0.8669 | 0.9526 | 0.7057 |
| | **Proposed method** | **0.2233** | **0.2179** | **0.1746** |

*E. Reconstruction:*

Decryption and reconstruction process are interpreted diagrammatically in Fig.3b and the image reconstruction procedure is given as follows:

[1]. Compressed−encrypted image A is split into RA, GA and BA images.

[2]. Inverse Arnold transform is applied with I1, I2 and I3 to A1, A2, A3 and A4 images of RA, GA and BA to get the unscrambled encrypted images C1, C2, C3, and C4 respectively of RGB.

[3]. Key matrices $\Phi_1$ and $\Phi_2$ of size (N/2 × N/2) is constructed, with keys K1, K2 and K3 and divide them with C1, C2, C3 and C4 to get the low-low, low-

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 5, May 2015*

high, high-low and high-high bands respectively of RGB.

[4]. Inverse DWT is applied to 4 bands; band 1 (lower), band 2, 3 and 4(higher) to reconstruct the input image.

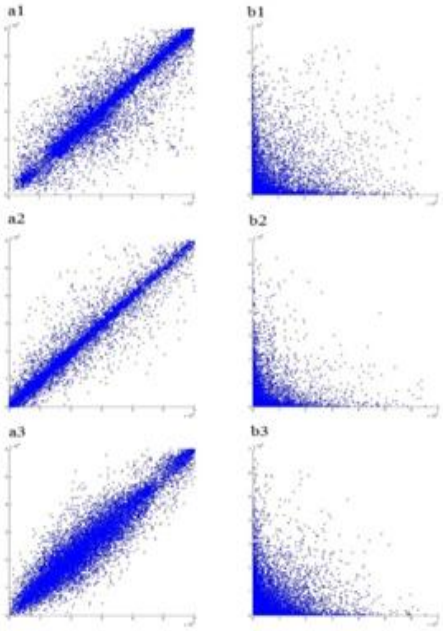


Fig. 7 Correlation distribution of two horizontally adjacent pixels in (a1) original Lena; (a2) encrypted Lena; (b1) original Cameraman; (b2) encrypted Peppers; (c1) original Mandrill; and (c2) encrypted Mandrill.

TABLE III THE PSNR FOR DIFFERENT COMPRESSION RATIO IN DB FOR STANDARD IMAGES.

| Sl. No | Compression Ratio | 4:3 | 2:1 | 4:1 |
|---|---|---|---|---|
| 1 | Lena image | 10.8263 | 9.5439 | 8.8542 |
| 2 | Peppers image | 9.8588 | 9.4930 | 9.0739 |
| 3 | Mandrill image | 6.3531 | 6.2927 | 6.4046 |
| 4 | Splash image | 14.9052 | 14.8071 | 13.0534 |
| 5 | Tiffany image | 16.796 | 15.9851 | 13.7207 |
| 6 | Bandon image | 26.8989 | 27.3234 | 24.7396 |
| 7 | F16 image | 18.4507 | 11.5336 | 9.1227 |
| 8 | House image | 11.2712 | 9.8368 | 9.6517 |
| 9 | Jelly beans image | 10.3389 | 12.8743 | 14.1683 |
| 10 | Girl image | 18.3621 | 20.5851 | 17.6595 |
| 11 | Pills image | 9.7087 | 7.5928 | 6.4697 |
| 12 | Watch image | 8.6625 | 16.6097 | 17.0492 |
| 13 | Terraux image | 18.4507 | 10.4838 | 9.1471 |
| 14 | Water image | 6.5493 | 14.7115 | 9.7331 |
| 15 | Tree image | 9.1914 | 6.1869 | 5.7292 |

*F. Estimation of PSNR for Different Compression Ratio*

The degree of compression and the quality of reconstructed image are assessed by the formulae [7]:

$$CR = \frac{\text{compressed file size}}{\text{input file size}} \quad (7)$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} [R(i,j) - I(i,j)]^2 \quad (8)$$

$$PSNR = 10 \log \frac{255^2}{MSE} \quad (9)$$

Where, R(i, j) and I(i, j) are the reconstructed image and the input image, respectively.

Table 3 & 4 lists the PSNR for different compression ratios for standard and medical images respectively and Fig.9 shows visually the reconstructed images. The values show that there is no reduction in PSNR and even a little increment in it. Hence reconstruction quality is ensured without degradation in existing value.

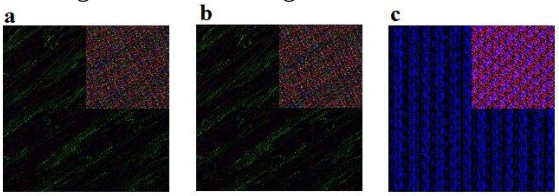


Fig. 8. a) Encrypted Lena using K1 = 0.11, K2 = 0.33 and K3 = 0.51; (b) encrypted Lena using K1 + Δ = 0.11 + 1×10-16, K2 = 0.33 and K3 = 0.51; and (c) difference between two encrypted images (a) and (b).

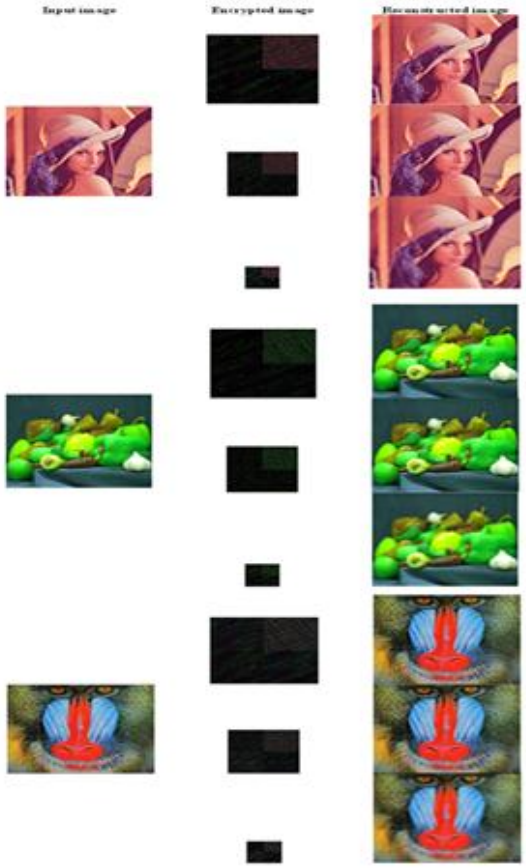

Fig. 9. Reconstructed image for different compression ratio

## VI. CONCLUSION

In this paper a hybrid algorithm for compression-encryption has been proposed which is based on key matrix and chaos system with Arnold transform. From the results, it is inferred that the histogram is same for encrypted images for varying input images, correlation coefficient is close to zero, key space has been increased from $10^{34}$ to $10^{85}$, and key sensitiveness is enhanced and appears visually, PSNR is optimum for better CR values. Finally it is concluded that the proposed algorithm offers

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 5, May 2015*

improved security. It will be useful for secured image transfer applications. Further work may be done with standard color images and also with medical images.

## REFERENCES

[1]. Nanrun Zhou, Aidi Zhang, Fen Zheng, and Lihua Gong, "Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," Optics & Laser Technology. 62, 152–160, 2014.
[2]. C. Rafael Gonzalez, E. Richard Woods, "Digital Image Processing (2nd edition)," NJ, Prentice Hall, 1992.
[3]. S.Anitha, "Image Compression using Discrete Cosine Transform and Discrete Wavelet Transform," International Journal of Scientific & Engineering Research. 2(8), 1-6, 2011.
[4]. Pavan Kumar, Goswami, Namita Tiwari, and Meenu Chawla, "Block Based Image Encryption Using Iterative Arnold Transformation," International Journal of Advanced Research in Computer Science and Software Engineering. 3(8), 273-278, 2013.
[5]. Karl Martin, Rastislav Lukac, and Konstantinos N. Plataniotis, "Efficient Encryption of Compressed Color Images," IEEE ISIE 2005, Dubrovnik, Croatia, 1245-1250, 2005.
[6]. Hilton de Oliveira Motaa, Leonardo Chaves Dutra da Rochaa, Thiago Cunha de Moura Salles, and Flávio Henrique Vasconcelos, "Partial discharge signal denoising with spatially adaptive wavelet thresholding and support vector machines," Elsevier.81, 644–659, 2011.
[7]. Fei Xiaoa, Yungang Zhang, "A Comparative Study on Thresholding Methods in Wavelet based Image Denoising," Elsevier.15, 1877-7058, 2011.
[8]. Wang Sheng Fang, Lu Lu Wu, and Rong Zhang, "A Watermark Preprocessing Algorithm Based on Arnold Transformation and Logistic Chaotic Map," Advanced Materials Research. 341-342, 720-724, 2012.
[9]. Lu P, Xu ZY, Lu X, and Liu XY, "Digital image information encryption based on compressive sensing and double random-phase encoding technique," Optik-International Journal for Light and Electron Optics. 124(16), 2514–2518, 2013.
[10]. Liu XY, Cao YP, Lu P, Lu X, and Li Y, "Optical image encryption technique based on compressed sensing and Arnold transformation," Optik-International Journal for Light and Electron Optics.124, 6590–3, 2013.
[11]. R. Huang, K.Sakurai, "A robust and compression-combined digital image encryption method based on compressive sensing," In: Proceedings of the 7th international conference on intelligent information hiding and multimedia signal processing (IIHMSP). 105–8, 2011.
[12]. BM. Hennelly, JT. Sheridan, "Image encryption and the fractional Fourier trans-form," Proc SPIE –Int Soc Opt Eng, 5202: 76-8, 2003.