Reason - A Technical Journal
ISSN 2277–1654
Volume - XIV ● 2015

A NOVEL APPROACH IN SYMMETRIC KEY IMAGE ENCRYPTION USING GENETIC ALGORITHM

Subhajit Das[1] and Satyendra Nath Mandal[2]

[1]Nayagram Bani Bidyapith, Nayagram, India. Email: subhajit.batom@gmail.com.
[2]Kalyani Govt. Engg College, Dept.of Information Tech., Kalyani, Nadia, India
Email: satyen_kgec@rediffmail.com

Paper received on: March 04, 2016, accepted after revision on: March 19, 2016

Abstract: In this paper, a symmetric key image encryption algorithm has been proposed based on genetic algorithm. The algorithm has three steps, generation of random sequence, diffused image and image encryption. Key generation is based on a new integer sequence generation and a mixing process. The random integer sequence has been generated from 64 bits key and mixing. The input image has been diffused by genetic algorithm and parents have been selected from image folding. The encrypted image is formed after performing logical operation between diffused image and random sequenence. The effectiveness of the algorithm has been measured by applying number of statistical tests between plain and encrypted image.It has been observed that the proposed algorithm is giving satisfactory result in all cases.

Keywords: Symmetric key; Genetic algorithm; Horizontal and vertical folding; Remainder set and Security level.

1. INTRODUCTION

Cryptography the art of protecting data from auautharized user. The traditional encryption algorithms such as DES, AES, RSA etc. are not very suitable for the encryption as every digital image contains huge redundancy. In recent years, some researchers are started to work in this field and their works are mentained here. Seyyed Mohammad, Reza Farshchi and Iman Dehghan Ebrahimi [2] have developed a new color image encryption algorithm based on chaos genetic algorithm and control parameter chaotic map. Mohammed A.F. and Al-Husainy [3] have demonstrated a symmetric key image encryption using genetic algorithm. The authors have converted the input (W × H) into n vectors of length L (64 bits). The crossover and mutation have been applied on two consecutive vectors to produce encrypted image. Aarti Soni et al. [4] have described a key generation algorithm based on genetic algorithm. The key has been generated from pseudo random binary sequence and genetic operations.V Srikanth et al. [5] have proposed a bit level encryption using genetic algorithm into two steps. In first step, the input images has been splited into blocks. The single point crossover and mutation have been applied on blocks to obtain the cipher image. Kumar and Nirmala [6] have used linear congruential generator to generate pseudorandom key sequence. The crossove and mutation have been applied on sequence to generate encrypted image.From the study [1-13], it has been observed that most of the papers have been written on key generation using genetic algorithm and some researchers also used chaos theory to generate effective encryption algorithm. This paper is divided into the following parts. The first part consists of the abstract and introduction.The proposed algorithm is giving at part 2. The part 3 and part 4 are the experimental set up, the result and security level testing. The conclusion is in part 5 and the references are giving at the end.

2. PROPOSED ALGORITHM

The algorithmis known as Symmetric Key Image Encryption Using Genetic Algorithm (SKIEG) is follows:

Input : Gray level Image, Key value

Output: Encrypted Image

Method:

Begin

Step 2.1. Random sequence generation

Step 2.2. Image diffusion

Step 2.3. Image Encryption

End

2.1 Key Generation

Input: 64 bit key

Output : Random sequence

Method :

Begin

Step 1. To take arbitrarily 8 characters as a key

$$\mathbb{K} = \{k_1, k_2, \dots \dots, k_8\}$$

Step 2. To convert each character into its equivalent 8 bit ASCII value.

$$\mathbb{K} = \{ASCII(k_1), ASCII(k_2), \dots \dots, ASCII(k_8)\}$$

$$\mathbb{K} = \{(K_{17,} K_{16,} \dots . K_{10,}), (K_{27,} K_{26,} \dots . K_{20,}) \dots \dots, (K_{87,} K_{86,} \dots . K_{80,})\}$$

Step 3. To divide K into 4 equals parts i.e. each part containing 16 bits. Each 16 bits converted into its equivalent decimal value.

$$\mathbb{K} = \{dec\left(K_{17,} K_{16,} \dots K_{10,} K_{27,} K_{26,} \dots K_{20,}\right), \dots, dec(K_{77,} K_{76,} \dots K_{70,} K_{87,} K_{86,}, \dots K_{80,})\}$$

$$\mathbb{K} = \{p_1, p_2, p_{3,} p_4\} \quad where\ 0 \le p_i \le 65543$$

Step 4. To generate four different sequences of integer numbers are ranging from 1 to p_i for each which satisfy the equation described below.Sequences are stored in reverse order one by one in

seq (p_i) = {x | 1 ≤ x ≤ p_i and (12 × x + 1) is prime}

$$\mathbb{K} = \{rev(seq(p_i)) \,|\, 1 \le i \le 4\}$$

Step 5. To divided set $\mathbb{K}$ into 16 parts.

$$\mathbb{K} = \{pt_1, pt_2, pt_{3, \dots\dots} pt_{16}\}$$

Step 6. To construct a magic square matrix using these 16 parts.

pt_{16}	pt_2	pt_3	pt_{13}
pt_5	pt_{11}	pt_{10}	pt_8
pt_9	pt_7	pt_6	pt_{12}
pt_4	pt_{14}	pt_{15}	pt_1

Step 7. To stored all the parts one by one in row major order into$\mathbb{K}$.

$$\mathbb{K} = \{pt_{16}, pt_2, pt_{3,} pt_{13}, pt_5, pt_{11}, pt_{10, \dots\dots} pt_{15,} pt_1\}$$

End

2.2   Image Diffusion

Input : Gray scale image

Output: Diffuse Image

Method

Begin

Step 1. The gray scale image is a set of pixels represented by matrix $\mathbb{M}$

$$\mathbb{M} = \{a_{ij}\}_{m \times n}$$

Step 2. To fold vertically of the image matrix exactly at the half line leads to the change of the elements of , such that

$$\alpha_{ij} \leftrightarrow \alpha_{ik}, \forall i = 1,2,3, \dots\dots\dots, m;$$

$$j = 1,2,3, \dots., \frac{n}{2}; k = \frac{n}{2}+1, \frac{n}{2}+2, \dots..n-2, n-1, n$$

Step 3. To convert each element into 8 bits binary equivalent as

$$a_{ij} = \alpha_1^{ij} \alpha_2^{ij} \dots\dots\dots\dots \alpha_8^{ij}$$

$$i = 1,2,3, \dots\dots m;\ j = 1,2,3, \dots.. \frac{n}{2}; k = \frac{n}{2}+1,$$

and $\alpha_{jk} = \alpha_1^{ik} \alpha_2^{ik} \dots\dots\dots\dots \alpha_8^{ik}$ where

$$\alpha_1^{ij},....,\alpha_1^{ik},......=0or1$$

Step 4. To apply cross over operation on elements as shown below

1st position cross over results in

$$\alpha_{ij}^{i}=\alpha_1^{ij}\alpha_2^{ij}..........\alpha_l^{ij}\alpha_{l+1}^{ik}\alpha_{l+2}^{ik}............\alpha_8^{ik}$$

$$\alpha_{ik}^{i}=\alpha_1^{ik}\alpha_2^{ik}..........\alpha_l^{ik}\alpha_{l+1}^{ij}\alpha_{l+2}^{ij}............\alpha_8^{ij}$$

The index may take any value between 1 to 8.

Step 5. To apply mutation operation (here last bit NOT operation) on the resulting elements after the cross over operation leads to

$$\alpha_{ij}^{ii}=\alpha_1^{ij}\alpha_2^{ij}..........\alpha_8^{ij}\alpha_1^{ij}\alpha_2^{ij}............\approx\alpha_8^{ij}$$

$$\alpha_{ik}^{ii}=\alpha_1^{ik}\alpha_2^{ik}..........\alpha_8^{ik}\alpha_1^{ik}\alpha_2^{ik}............\approx\alpha_8^{ik}$$

where $\approx\alpha_8^{ij}$ = NOT α_8^{ij} & $\approx\alpha_8^{ik}$ = NOT α_8^{ik}

Step 6. To repeat step 2 to step 5 after folding the resulting elements vertically

End

2.3 Image Encryption

Input : Diffuse image and random sequence

Output: Encrypted Image

Method:

Begin

At this point logical XOR operation is perfomed on diffused image matrix $\mathbb{M}''=\{b''_{ij}\}_{m\times n}$ element by element with the elements of set $\mathbb{K}$.

$$c_{ij}=\{b_{ij}\otimes y:\forall\ i-1,2,3,....,m;\ j=1,2,3\ ....,n;$$
$$y = 1, 2, 3\ .....,\ k\ \&\ \text{so on}\}$$

when m, n $\leq$ k

If m, n > k

$$c_{ij}=\{b_{ij}\otimes y:\forall\ i=1,2,3,....,m;\ j=1,2,3\ .....,n,$$
$$y = 1, 2, 3\ .....,\ k\ \&\ \text{so on}\}$$

In this way the image is encoded in the form $\mathbb{M}'''=\{c_{ij}\}_{m\times n}$

End

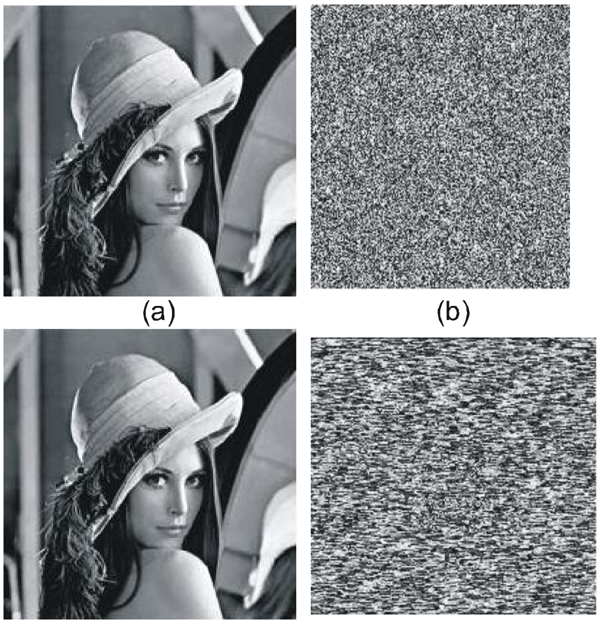
3. EXPERIMENTAL SETUP

A PC with Intel Core 2 Duo 1.50GHz CPU, 1GB RAM, 500GB hard disk with Windows7 operating System and with MATLAB 7.9.0.529 have been used to perform the proposed method. Gray level images with dimension 256×256 and 512×512 have been taken for experiments.

4.EXPERIMENTAL RESULT AND SEQURITY LEVEL TESTING

4.1 Key Sensitivity Test

To test the proposed algorithm it has been applied on the famous image of Lena. The key has been generated by taking an ABC@1234. The original, the encrypted and the decrypted images have been furnished in Fig's 1. a) to c). The figure 1. d) represents the decrypted image with wrong key.



(a) (b)

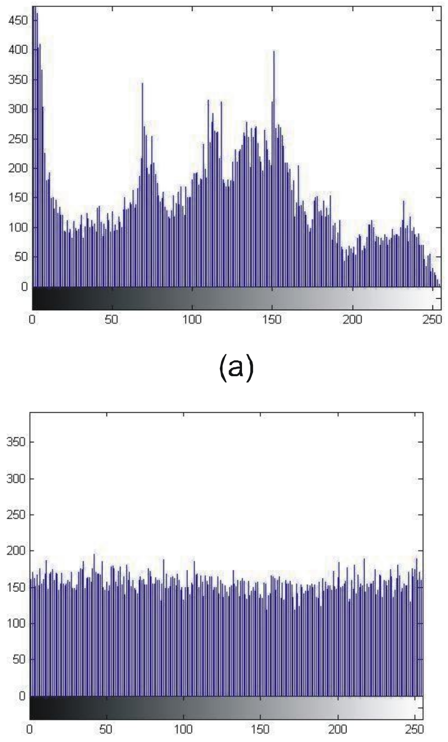
(c) (d)

Fig 1. a) Plain image (lena) b) encrypted image with key value ABC@1234 c) decrypted image with corect key value d) decrypted image with wrong key value

4.2 Security Level Testing

4.2.1 Histogram Analysis

An image-histogram describes how the image-pixels are distributed by plotting the number of pixels at each intensity level. The histogram represents the statistical characteristics of an image. If the histograms of the encrypted image are similar to the random image, the encryption algorithm has good performance. It is very difficult for an attacker to extract from the statistical nature of pixels the plain image out of the encrypted image. The histogram of plain and encrypted Lena image have been furnished in figure 2. a) and 2. b) . Later histogram of some plain and encrypted images have been given in figure 3.



(a)

(b)

Fig 2. a) Histogram of plain image (Lena) b) Encrypted image

4.2.2 NPCR and UACI Analysis

Two criteria, number of pixels change rate (NPCR) and unified average changing intensity (UACI), are often used to test the sensitive of a single bit change of the plain-image. Suppose, encrypted images before and after one pixel change in an image are C^1 and C^2 respectively. The pixel value at grid (i, j) in C^1 and C^2 are denoted as $C^1(i, j)$ and $C^2(i, j)$, then a bipolar array D can be defined by Eqn.(1). The NPCR and UACI have been defined by Eqns.(2) and (3) respectively, where symbol T denotes the total number pixels in the ciphertext and symbol F denotes the largest supported pixel value compatible with the ciphertext image format. Whereas - denotes the absolute value function.

$$D(i,j) = \begin{matrix} 0 & \text{if } C^1(i,j) = C^2(i,j) \\ 1 & \text{if } C^1(i,j) \neq C^2(i,j) \end{matrix} \qquad (1)$$

NPCR: $$N\left(C^1, C^2\right) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \qquad (2)$$

UACI:

$$U\left(C^1, C^2\right) = \sum_{i,j} \frac{\left|C^1(i,j) - C^2(i,j)\right|}{F \cdot T} \times 100\% \qquad (3)$$

It has also been found that the range of NPCR and UACI is [0,1]. The NPCR = 0 implies that pixels in C^1 and C^2 remains unchanged, whereas NPCR = 1 implies that all pixels in C^2 are changed compared to those in C^1. The NPCR and UACI of Lena image have been calculated as 99.99 and 33.26 respectively. The NPCR and UACI of different sample images is furnished in table 1.

4.2.3. Mean Squared Error (MSE) Analysis

Mean Squared Error (MSE) in signal processing is defined as

$$MSE = 1/mn \sum_{i=1}^{m} \sum_{j=1}^{n} \left(x(i,j) - y(i,j)\right)^2 \quad (4)$$

Where $x(i, j)$ represents the original (reference) image and $y(i, j)$ represents the distorted (modified) image. MSE is zero when $x(i, j) = y(i, j)$. In this experiment MSE values for all images and their corresponding decrypted images come as 0, this proves that the algorithm guarantees possibility of extraction of original image after decryption.

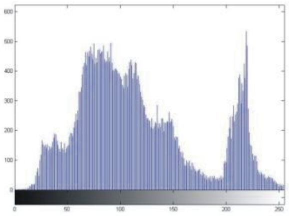
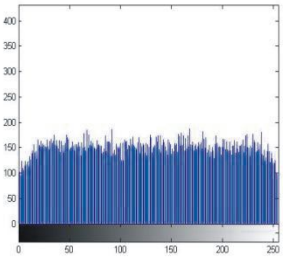
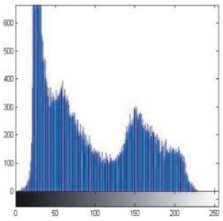
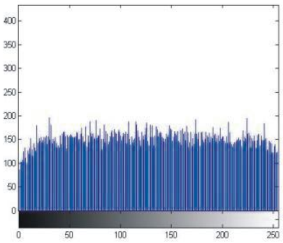
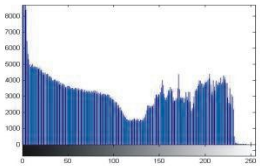
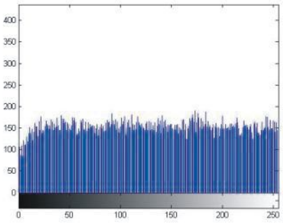
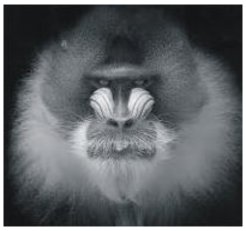
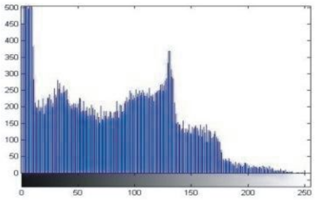
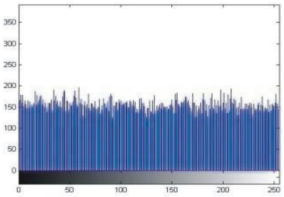
Image Name	Image	Histogram of plain image	Histogram of encrypted image
Hill			
Mona lisa			
Desert			
Babun			

Fig. 3: Histogram of some plain and encrypted images

4.2.4. Information Entropy Analysis

Information entropy is analyzed to test the robustness of the encryption algorithm and it is defined as

$$H(m) = \sum p(m_i) \log_2 \frac{1}{p(m_i)} \qquad (5)$$

Where $p(m_i)$ represents the probability of the pixel value m_i. Theoretically, a true random system should generate 2^8 symbols with equal probability, i.e., $m = \{m_1, m_2, m_3, \ldots \ldots, m_{2^8}\}$ for bit depth 8. The entropy of the plain and encrypted Lena image have been calculated as 7.74 and 7.99 and the entropy of the plain and encrypted other images have been given in table 2.

4.2.5. Correlation Analysis

The correlation coefficient [5] of each pair of pixels is given as

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \qquad (6)$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))2 \qquad (7)$$

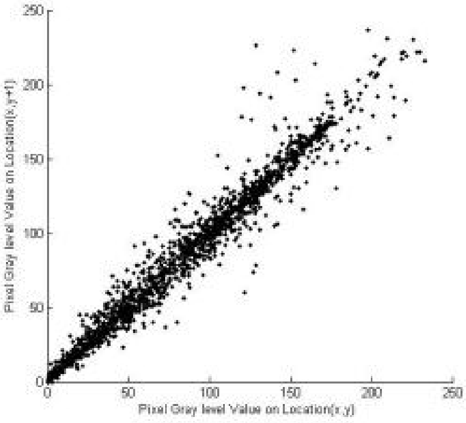
$$COV(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \qquad (8)$$

$$r=\frac{COV(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (9)$$

where x and y are grey-scale values of two adjacent pixels in the image.

In this experiment, 1000 pairs of two adjacent (in horizontal, vertical, and diagonal directions) pixels from plain and encrypted Lena image have been tested. The correlation coefficient in each directions have been furnished in table 3. The correlation coefficient of plain and encrypted images, plain and decrypted images have been calculated as 0.0097 and 1. The correlation coefficients of some sample images have been furnished in table 4.

Total 1000 random adjoining pixels of plain image and its corresponding cipher image have been chosen and their correlation distribution of two vertical, horizontal and diagonal adjacent pixels are furnished in fig 4 to fig 6.



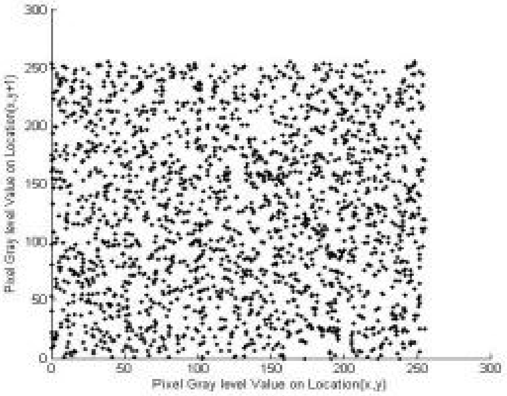


Fig. 4 : Correlation plot of two adjacent pixels of plain image (lena) and its corresponding cipher image in horizontal direction.

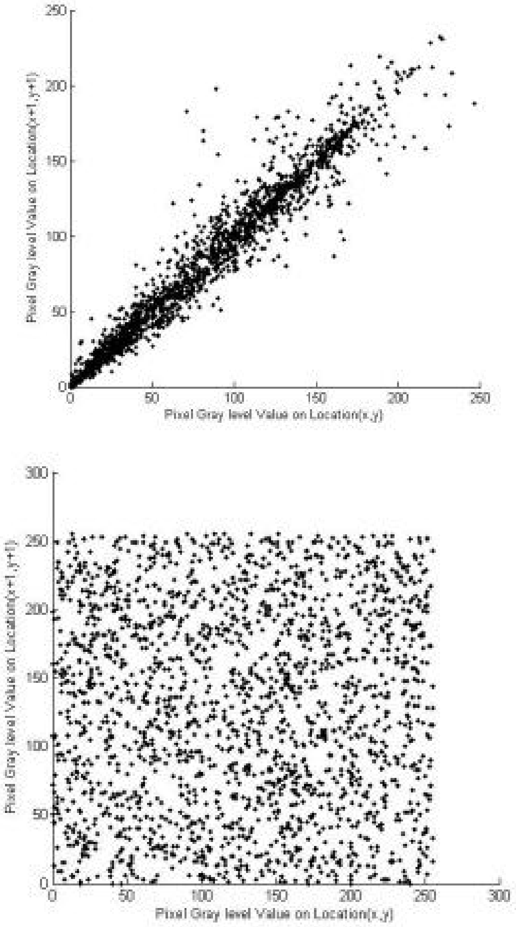


Fig. 5 : Correlation plot of two adjacent pixels of plain image(lena) and its corresponding cipher image in vertical direction.

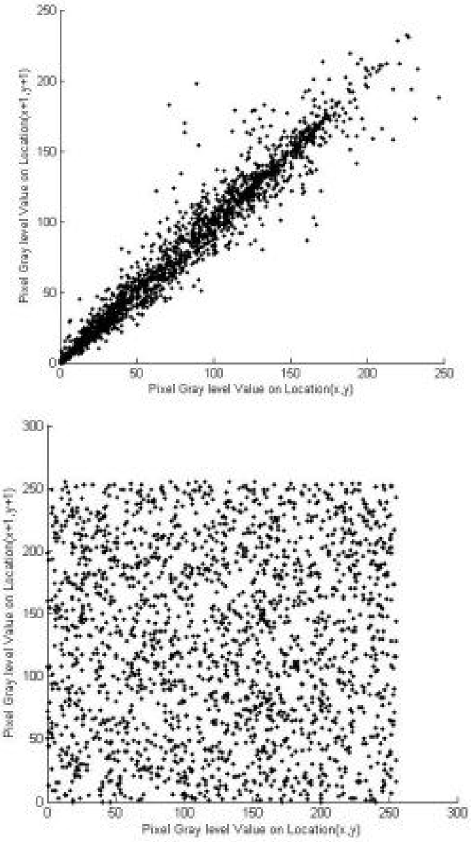


Fig. 6: Correlation plot of two adjacent pixels of plain image(lena) and its corresponding cipher image in diagonal direction.

Table 1. The NPCR and UACI of different images

Image	NPCR [in %]	UACI [in %]
Lena	99.9975	33.26
Desert	99.995	33.31
Babun	99.9968	33.65
Monalisa	99.9943	33.18
Nature	99.9987	33.29

Table 2. Entropy of the plain image and encrypted different images

Image	Plain image	Ciphered image
Lena	7.7460	7.9954
Desert	7.4812	7.9948
Babun	7.4069	7.9937
Monalisa	7.7684	7.9898
Nature	7.4354	7.9765

Table 3. Correlation coefficient of plain and encrypted of different images

	Plain image	Encrypted image
Horizontal	.9996	.0012
Vertical	.9765	.0032
Diagonal	.92612	.00043

Table 4. Correlation coefficient of plain and encrypted Lena image

Image	Correlation coeffient of plain and cipher image	Correlation coeffient of plain and decrypted image
Lena	.0097	1
Desert	.0087	1
Babun	.0089	1
Monalisa	.0096	1
Nature	.0067	1

5. CONCLUSION AND FUTURE WORK

In this paper, genetic algorithm has effectively been used to encrypt an image information with symmetric key. The same key has been applied for both encryption and decryption of image. It is found that no information can be retrived with wrong key. While encryption the image informations have been modified by genetic algorithm and XOR operation has been performed between the modified image pixels and elements of random sequence. It is found that the pixel values of image have been well diffused and that is evident from histogram analysis. To compare two histograms, it is seen that the encrypted image bears no statistical resemblance to the plain image. The NPCR and UACI values of all images are nearly 1 and are greater than 32 respectively. This shows the strength of the algorithm against differential attacks. The algorithm gives zero value in mean squared error (MSE) analysis for all images. It has been proved in the algorithm that the original images can be recovered by application of right keys only. The correlation values in different directions indicats that there is no correlation between the original images and decrypted images. The entropy values nearly 8 in different analysis is indicative of the fact that the algorithm has truely distributed the intensities of image pixels from 0 to 255. More test, comparison with other existing algorithm and other soft computing algorithms will be used in future.

ACKNOWLEDGMENTS: The authors would like to thank to the All India Council for Technical Education (F. No- 20/AICTE/RIFD/RPS/(POLICY-1)43/2013-14) for funding this research work.

REFERENCES

[1] Liu, S., Song, Y. and Yang, J., Image Encryption Algorithm Based on Wavelet Transforms and Dual Chaotic Maps, Journal of Software, Vol. 9, No.2, pp.458-465, 2014.

[2] Mohammed, A.F. and Al-Husainy, Image Encryption Using Genetic Algorithm, Information Technology Journal 2006, Asian Network For Scientific Information, pp.516-519, 2006.

[3] Soni, A. and Agrawal, S., Using Genetic Algorithm for Symmetric key Generation in Image Encryption, International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1, No.10, pp.137-140, 2012.

[4] Srikanth, V., Asati, U., Natarajan, V., Kumar, T.P., Mullapudi, T. and Iyengar, N.Ch.S.N., Bit-Level Encryption of Images using Genetic Algorithm, TECHNIA International Journal of Computing Science and Communication Technologies, Vol. 3, No.1, pp.546-550, 2010.

[5] Kumar, J. and Nirmala, S., Encryption of Images Based on Genetic Algorithm– A New Approach, Advances in Computer Science, Eng. & Appl., AISC 167, Springer-Verlag, Berlin, Heidelberg, pp.783-791, 2012.

[6] Liu, H., Wang, X. and Kadir, A., Image encryption using DNA complementary rule and chaotic maps. Appl Soft Computing, Vol. 12, pp.1457–1466, 2012.

[7] Das, S., Mondal, S.N. and Ghosal, N., An Innovative Approach in Image Encryption, ACEEE Proceedings of the Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC 2014, pp.158-166, 2014.

[8] Jolfaei, A. and Mirghadri, A., A novel image encryption scheme using pixel shuffler and A5/1, Proceedings of the International Conference on Artificial Intelligence and Computational Intelligence, pp.369-373, 2010.

[9] Sabouri, N., Javadi, H.H.S. and Asoudeh, T.Z., A Comparative Study on the Effect of Used Crossover Operator on Performance of GA as a Web Page Classifier, International Journal of Computer Applications, Vol. 71, No.23, pp.32-37, 2013.

[10] Gupta, R.K., Genetic Algorithms- An Overview, Impulse, Vol. 1, pp.30-39, 2006.

[11] Wu, S. and Zhang, Y., A Novel Encryption Algorithm Based on Shifting and Exchanging Rule of Bi-column Bi-row Circular Queue, Proceedings of the International Conference on Computer Science and Software Engineering, pp.841-844, 2008.

[12] Huang, F. and Feng, Y., Security Analysis of Image Encryption Based on Two Dimensional Chaotic Maps and Improved Algorithm, Front. Electr. Electron. Eng. China, pp.5-9, 2009.

[13] Mohammad, S., Farshchi, R. and Ebrahimi, I.D., A Novel Encryption Algorithm for Transmitting Secure Data based on Genetic Hyper Chaos Map, Proceedings of the International Conference on Computer Communication and Management, IACSIT Press, Singapore, pp.623-627, 2011.

[14] Nambi, P., https://oeis.org, sequence No. A110801.