I J C T A, 9(34) 2016, pp. 17-28
© International Science Press

A Secure Chaos-based Image Encryption and Decryption Using Crossover and Mutation Operator

Poluri Samhita[*], Prateek Prasad[*], K Abhimanyu Kumar Patro[**] and Bibhudendra Acharya[**]

ABSTRACT

In this world of digital media, security concerns are one of the most pondered tasks upon the dimension of communication. Now the researchers focus is on developing secure schemes which will enhance the security in the way of communication. In this paper, a secure chaos-based image encryption and decryption using crossover and mutation operator is proposed. The implementation is based on the chaotic logistic map is in combined with the crossover & mutation operator. The proposed methodology works in three steps. In the first step, initial population is formed by using the chaotic logistic map function. In the second step, 4-point crossover operation is performed between the two adjacent bytes. Finally, in the last step, Mutation (2-point crossover) is performed within a single byte. In the similar way, the decryption operation is performed. The proposed image encryption scheme is simple and easy to implement. The experimental results and security analysis show that the proposed image encryption and decryption scheme not only achieve good encryption effect but also obtain best entropy (7.9953 for 'Lena' Image, 7.9933 for 'Cameraman' image and 7.9934 for 'Peppers' image) and correlation coefficient (– 0.0125 for 'Lena' image and – 0.0074 for 'Cameraman' image) through only one round encryption process. The major advantage of proposed method is that even in the first iteration, the use of crossover and mutation operation gives better results. The correlation coefficient and entropy results show that the proposed method is highly efficient as compared with the other methods.

Keywords: Image Encryption, Chaotic Logistic Map, Crossover, Mutation.

1. INTRODUCTION

With the faster progress of sharing of information in the public network such as internet, a great challenge arises for maintaining the security of information mainly the image data. The most important task is to secure image data against the third party such as eavesdroppers. Cryptographic techniques are required to be applied for obtaining the confidentiality of images. Cryptography is the study of techniques for secure communication of information [1]. Over the past 20 years, a lot of techniques have been proposed for image encryption based on different principles for protecting the confidentiality of images. Because of some basic inherent features of images such as massive data capacity and strong correlation among adjacent pixels, the traditional techniques such as DES, IDEA, AES, etc. are not suitable for practical image encryption [2, 3]. A low-level of efficiency is achieved when the image is large [4]. Thus a new research in image encryption is urgently needed which will give high efficiency as compared to the traditional techniques. The chaotic image encryption techniques has suggested as a highly secure and highly efficient image encryption technique compared to the other techniques. Chaotic systems have several properties. Some of the properties which are very much essential for designing a secure encryption system are high sensitivity to initial conditions and system parameters, high complex behavior, ergodicity, non-periodicity, determinacy, mixing property, etc [5, 6].

[*] Department of E & TC, NIT Raipur, Chhattisgarh, India, *E-mails: samhita.poluri@yahoo.com; prateekdan@gmail.com*

[**] Department of ETC, NIT Raipur, Chhattisgarh, India, *E-mails: abhimanyu.patro@gmail.com; bacharya.etc@nitrr.ac.in*

Fridrich [7] suggested a permutation - substitution based image encryption model by using two-dimensional chaotic maps. Now days many of the image encryption systems are modeled by using this permutation-substitution principle. Afterwards, many numbers of chaotic image encryption techniques based on logistic map, standard map and PWLCM have been proposed [8-11]. The most important criteria for improving the design of any image encryption technique are security, running time, etc [6]. Recently, a compound chaotic sequence based image encryption technique was proposed [12]. The working steps of this scheme are divided into two phases. In the first phase, the pixel values are changed by using XOR operations, and in the second phase, the pixel positions are changed by performing the circular permutation operation of rows and columns. The new and innovative methods are developed by combining chaos theory and the existing encryption/decryption methods [13, 15]. In 2010, Liu *et al.* [14] proposed a double image encryption scheme by using random binary encoding and gyrator transform. In this algorithm, an iterative structure is designed for enhancing the security by using random binary encoding method.

Chaos based image encryption is the current research hotspot in the modern security world. Authors are worked to enhance the security and the efficiency of chaos based image encryption. This paper proposes a secure chaotic image encryption and decryption scheme using crossover and mutation operator. In the proposed scheme, the numbers of initial populations are developed by using chaotic logistic map and the key. The key is extracted from the plain-image. Finally, the result is optimized by using crossover and mutation operation.

Following to the introduction in Section 1, Section 2 outlines some basis theories related to the proposed algorithm. The proposed methodology is explained in Section 3. Simulation results and security analysis of the proposed methodology are presented in Section 4. Finally, the paper is concluded in Section 5.

2. PRELIMINARIES

This section presents the brief knowledge of chaotic logistic map function, the genetic crossover operation and the genetic mutation operation. At first, the chaotic logistic map function is delivered and then the genetic crossover operation and the genetic mutation operation are outlined.

2.1. The Chaotic Logistic Map

Chaos theory is typically a mathematical property of nonlinear dynamical systems. The interactive component parts, which are combined to form the larger and whole one is called as *system*. When the individual parts of a system are added up, the result is something smaller than the whole system because of some multiplicative or feedback effects occurs in that whole system. This defines the n*onlinear* property of a system. Based on the current state, the nonlinear system which will change over time, then that nonlinear system is referred as the nonlinear *dynamical* system [16].

One of the simple nonlinear dynamical systems is the chaotic system, that has less number of interactive parts and these systems follow very simple rules to show their chaotic behavior. The chaotic behaviors are highly sensitive to initial conditions, non-periodicity, determinacy, ergodicity, unpredictability, etc [16]. Edward Lorenz, the father of chaos theory, described chaos [16, 17] as

> *"When the present determines the future, but the approximate present does not approximately determine the future."*

The logistic map signal is one of the signals that exhibit chaotic behaviors. The equation for chaotic logistic map signal is as follows:

$$X_{n+1} = rX_n (1 - X_n) \tag{1}$$

where X_n is in between [0, 1]. According to Reference [15], when the parameter $r \in [3.57, 4]$ and $X_0 = 0.3$, the signal is completely chaotic.

2.2. The Crossover Operation

Crossover is a process of biological recombination between a pair of homologous chromosomes. It is an operator used in genetic algorithms. In this operation, the two chromosomes are linearly combined to generate a new chromosome which is called as offspring. The generated offspring is the replacement of their parent chromosomes [18]. It is a convergence operation whose aim is to locally minimize/maximize the population.

2.3. The Mutation Operation

Mutation starts their operation after crossover which guarantees to the locally minimum/maximum of the population. It is an operator also used in genetic algorithm. In this operation, one or more bits are changed in a chromosome to generate a newer one. That means, it randomly changes the child (changing one or more bits) from what its parents produced in crossover. For an example, let the string be 00000101. Now the mutation operation applied in the second and fourth position. After mutation operation the newly generated string is 01010101 [18]. It is a divergence operation, whose aim is to generate a better minimum/maximum by breaking one or more members of the population.

3. PROPOSED METHODOLOGY

This section presents the procedure of chaos based image encryption and decryption by using crossover and mutation operator. The proposed scheme divides into three sections. In the first section, initial populations are generated from the plain-image by using chaotic logistic map function as in Reference [15]. After forming the initial population, in the second section, 4-point crossover is performed between the two adjacent bytes. Finally, in the last section, mutation operation (2-point crossover) is performed within a single byte. Similarly, the process for decryption also includes three sections. In the first section, the same numbers of the initial population is generated from which the final image is composed. In the second section, 4-point crossover operation is performed and finally, in the last section, mutation operation (2-point crossover) is performed. Figure 1 shows the process for image encryption and decryption by using the proposed algorithm.

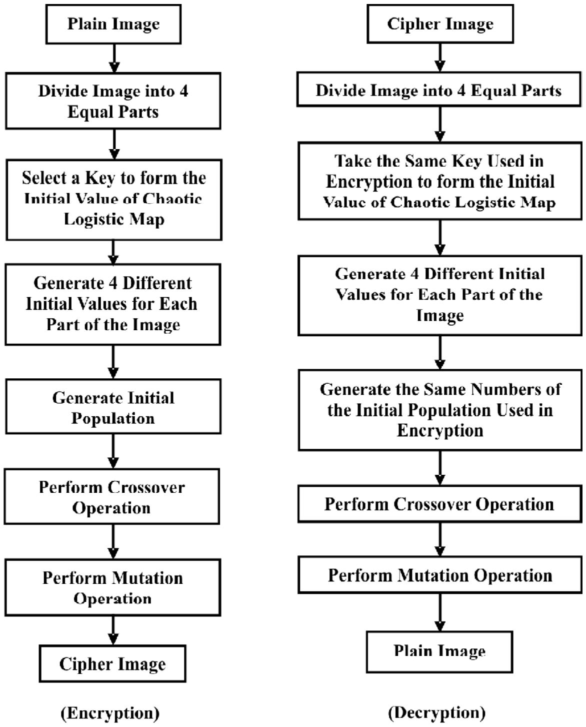
Plain Image
Divide Image into 4 Equal Parts
Select a Key to form the Initial Value of Chaotic Logistic Map
Generate 4 Different Initial Values for Each Part of the Image
Generate Initial Population
Perform Crossover Operation
Perform Mutation Operation
Cipher Image
(Encryption)
Cipher Image
Divide Image into 4 Equal Parts
Take the Same Key Used in Encryption to form the Initial Value of Chaotic Logistic Map
Generate 4 Different Initial Values for Each Part of the Image
Generate the Same Numbers of the Initial Population Used in Encryption
Perform Crossover Operation
Perform Mutation Operation
Plain Image
(Decryption)

Figure 1: Process for encryption and decryption by using the proposed algorithm

3.1. Encryption Algorithm

3.1.1. Generation of Initial Population

According to Reference [15], the basic steps for generating the initial populations are as follows. The first step performs the division operation of plain-image into four equal parts. The second step performs the initial value formation of the chaotic logistic map by selecting five pixels from each of the four parts of the image and the same five pixels of each part are also used to encrypt that part of the image. The pixel selection is based on the offspring's number. Third step performs the determination of four different initial values of chaotic logistic map by using five pixels' gray scale values of that part. Finally, encryption occurs in each part by using the initial values of that part. In this way, the first member of the population is built. By repeating the above steps, the rest of the population is built.

3.1.2. Crossover Operation

In this paper, entropy is used as the fitness function. The process for crossover operation is as follows.

1. Convert each pixel value into its corresponding 8-bit binary.
2. Generate 4 crossover points in the range of (0 – 15).

   Let it will be 7, 2, 14, 10. These four random numbers will serve as the four crossover points.
3. Sort the crossover points in ascending order.

   These four crossover points are sorted as: 2, 7, 10, and 14. That means,

   Crossover point 1 = 2,

   Crossover point 2 = 7,

   Crossover point 3 = 10, and

   Crossover point 4 = 14
4. Perform four point crossover operations between adjacent bytes (i.e., by considering each byte as a parent and generate the offspring between first-second bytes; third-fourth bytes and so on).

   Let the blocks are

   $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}$

   $y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12}, y_{13}, y_{14}, y_{15}$

After crossover operation, the blocks are modified as given below.

$x_0, x_1, x_2, y_3, y_4, y_5, y_6, y_7, x_8, x_9, x_{10}, y_{11}, y_{12}, y_{13}, y_{14}, x_{15}$

$y_0, y_1, y_2, x_3, x_4, x_5, x_6, x_7, y_8, y_9, y_{10}, x_{11}, x_{12}, x_{13}, x_{14}, y_{15}$

3.1.3. Mutation Operation

Similar to 4-point crossover, mutation operation is performed, which is the 2-point crossover within a single byte.

3.2. Decryption Algorithm

1. Divide the cipher image into 4 equal parts.
2. Choose the same key as used in encryption for generating the initial value of chaotic logistic map.

3. Generate four different initial values for each part of the image.
4. Generate the same numbers of the initial population used in encryption.
5. Perform 4-point crossover operation.
6. Perform mutation (2-point crossover) operation.

4. SIMULATION RESULTS AND SECURITY ANALYSIS

In this paper, the two images ‘Cameraman’ and ‘Lena’ are used for testing the simulation results. The images are taken as gray level images having size 256×256. MATLAB R2012a is used for simulation. The simulation was carried out in a system with windows 8 operating system, i3 processor, 1.60 GHz CPU, 4.00 GB memory and 500 GB hard disk. The simulation results are shown in Figure 2. The encryption results are shown in Figure 2(b) and (e). From the two encryption results, it is clearly shows that both images are properly encrypted by using the proposed algorithm. The decryption results are shown in Figure 2(c) and (f). Both the decryption results show that the encrypted images are properly decrypted by using the proposed algorithm. From the encryption and decryption results, it is noticeable that the proposed scheme provides good encryption and decryption with more confusion and diffusion leading to avalanche effect due to crossover and mutation operation.

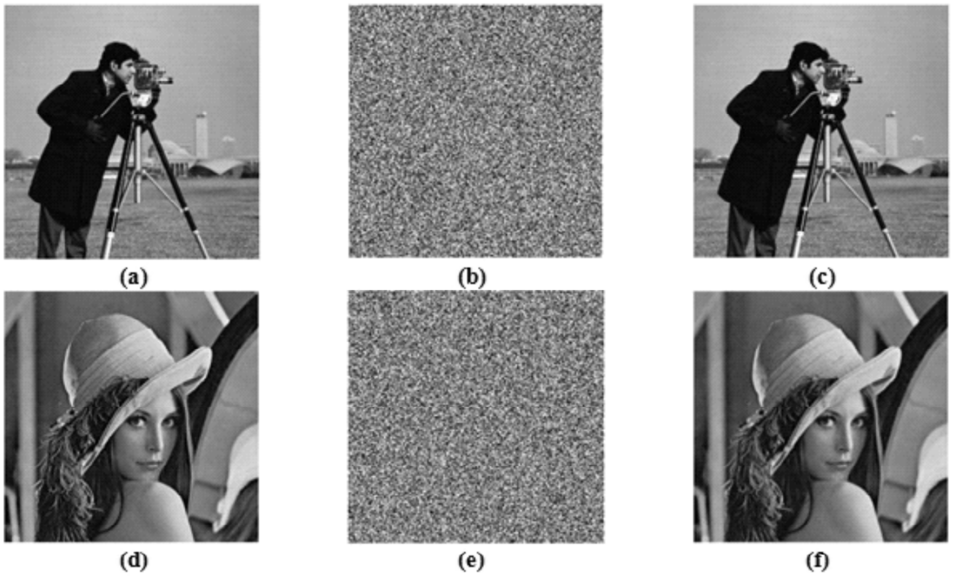

Figure 2: (a, d) Original images of ‘Cameraman’ and ‘Lena’ respectively, (b, e) Corresponding encrypted images by using the proposed method, (c, f) Corresponding decrypted images by using the proposed method

An algorithm is good to use for image encryption if it resists some of the known popular attacks, such as exhaustive attack, statistical attack and differential attack. A brief analysis of the security is discussed in this section.

4.1. Ability to Resist Exhaustive Attack

4.1.1. Key Space and Key Sensitivity Analysis

Key space defines the total number of different keys used for the complete execution of the algorithm [19]. The security depends on the key length that means longer key provides higher security and high resistivity to brute-force attacks [19, 20]. Five pixels or 40-bit key is used for generating the initial value of chaotic logistic map function for each part of the image, so for the total of 4-parts, a 160-bit key is used for the process of encryption. Along with 160-bit key, 4-point and 2-point crossover points are used for the complete execution of the algorithm. This will produce a key space of $2^{160} + 4 + 2$ which is very much resistive to brute-force attack. In the proposed algorithm, the chaotic logistic map is used which is sensitive to both the initial values and also to the system parameters. Therefore, the proposed algorithm is also sensitive to the secret keys.

4.2. Ability to Resist Statistical Attack

4.2.1. Gray Histogram Analysis

Histogram is the graph between the number of pixels and the corresponding pixel intensities of an image. Statistical attack is very much effective and provides higher performance when some data are captured from an histogram image [21]. It is desirable that after encryption the pixel gray values are to be scatter in the entire pixel value space. The histograms of original, encrypted and decrypted ‘Cameraman’ and ‘Lena’ images are shown in Figure 3. To analyze the statistical performance, the comparison of the gray histogram image before and after encryption is required. The histogram of original images and the corresponding encrypted image histograms of ‘Cameraman’ and ‘Lena’ are shown in Figure 3(a) & (d) and Figure 3(b) & (e) respectively. From the two groups of histogram figures, it can be observed that the pixel gray values of the original image are intense by some value on some points, but in histogram of encrypted image the pixel gray values are scattered throughout the pixel value space. This shows that the two images before encryption and after encryption have lower similarity. If the pixel gray values of the encrypted image are uniformly distributed then it is very much difficult to the attacker to recover the original image. Thereby, the proposed scheme is highly resistive to statistical attack. When we observe decrypted image histograms of ‘Cameraman’ and ‘Lena’ (Figure 3(c) and (f)), it is cleared that there is no data loss after decryption. Scattered diagram is a plot of two variables to investigate the relationship between them. Here the two variables to investigate are pixel gray values of original image and pixel gray values of encrypted image or pixel gray values of original image and pixel gray values of decrypted image. The scattered diagram between original image and encrypted image of ‘Cameraman’ and ‘Lena’ are shown in Figure 4(a) and (c) respectively by using the proposed method. This shows that, the points are spread throughout the entire surface results weaker correlation between them. This proves that the proposed algorithm provides good encryption. The scattered diagram between original image and decrypted image of ‘Cameraman’ and ‘Lena’ are shown in Figure 4(b) and (d) respectively by using the proposed method. From these two figures, it can be observed that the entire points are along a line results stronger correlation between them. This proves that there is no data loss during encryption and decryption.

4.2.2. Correlation of Adjacent Pixels

Correlation coefficient finds the degree of linear correlation between two adjacent pixels [22]. Generally we can say that, it reflects the degree of image scrambling [23]. Let it be represented as r whose range is defined within the interval $[-1, 1]$. If the value of r is greater than zero then it indicates positive correlation and if it is less than zero then it indicates negative correlation. $|r|$ represents the degree of correlation between two adjacent pixels. When $r = \pm 1$, it indicates perfect correlation and when $r = 0$, it indicates no correlation or simply uncorrelated pixels [22]. The correlation between the two adjacent pixels in an original image is almost close to 1. An effective encryption algorithm should reduce the correlation between adjacent pixels which is almost close to 0 and no matter in horizontal, vertical and diagonal directions [23]. That means the correlation coefficient between two adjacent pixels of original image has very strong linear correlation, while the correlation between two adjacent pixels of encrypted image is very small.

The mathematical expression for calculating the correlation coefficient is

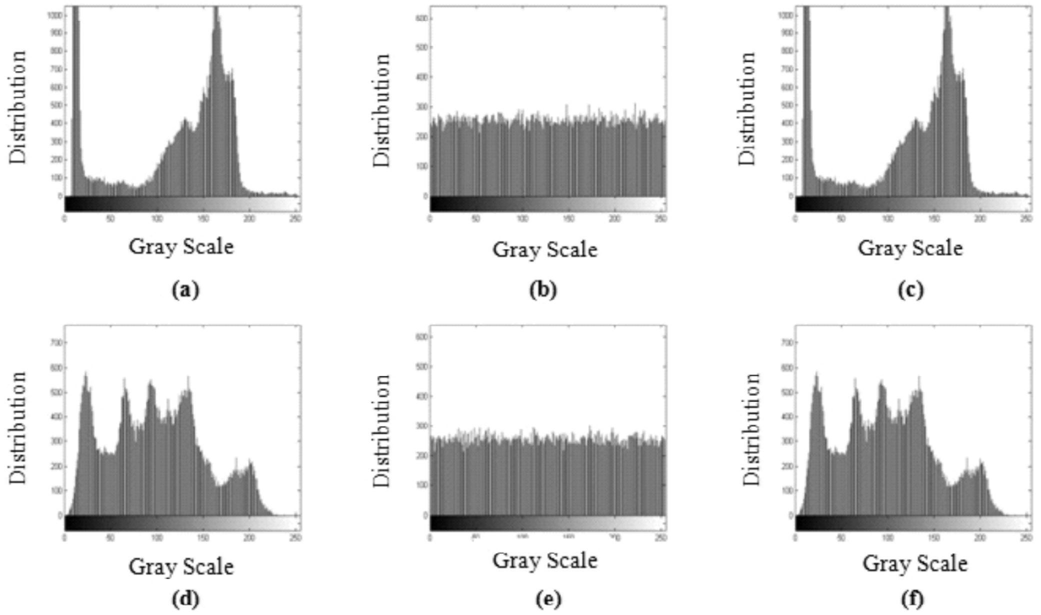

Figure 3: (a, d) Histograms of original ‘Cameraman’ and ‘Lena’ images respectively, (b, e) Histograms of corresponding encrypted images by using the proposed method, (c, f) Histograms of corresponding decrypted images by using the proposed method

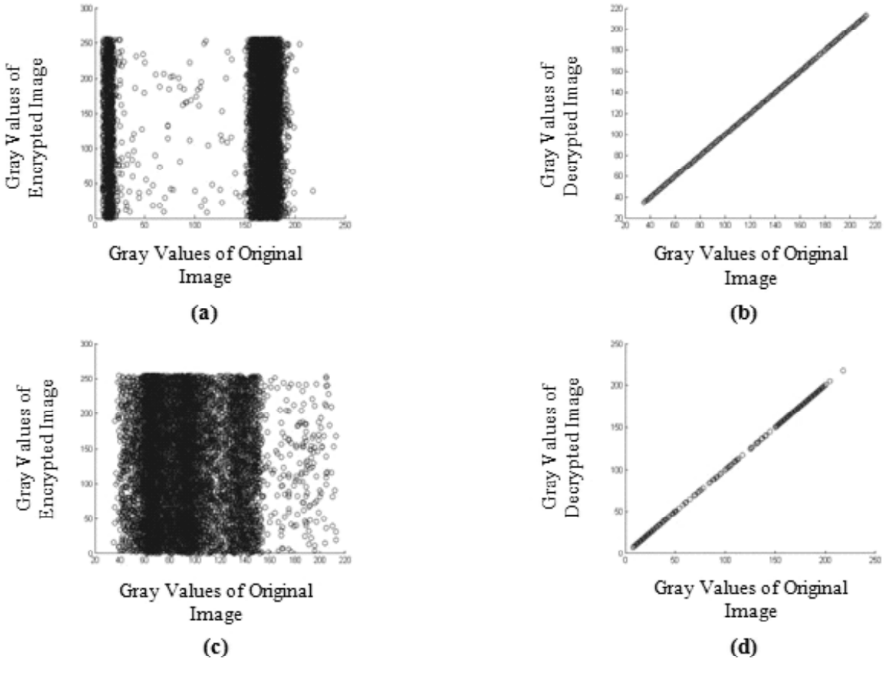

Figure 4: (a, c) Scattered diagram between original and encrypted images of ‘Cameraman’, and ‘Lena’ respectively by using the proposed method; (b, d) Scattered diagram between original and decrypted images of ‘Cameraman’, and ‘Lena’ respectively by using the proposed method.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2}$$

where

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{3}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \, , E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{4}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2,\ D(y) = \frac{1}{N}\sum_{i=1}^{N}\left(y_i - E(y)\right)^2 \tag{5}$$

To calculate the correlation coefficient, 2500 pairs of two adjacent pixels in horizontal, vertical and diagonal directions are randomly selected from both the original image and the encrypted image. The comparison of correlation coefficient results of Reference [15] and the proposed method are shown in Table 1. From Table 1 it is clear that original image have very strong correlation of adjacent pixels in all the three directions while encrypted image have very weak correlation approximately zero in all the three directions. From Table 1 it found that the correlation coefficient (when fitness function is entropy) of encrypted image by using the technique of Reference [15] in 100th iteration is close to 0 while by using the proposed method in single round iteration itself it is close to 0. Therefore the proposed algorithm can effectively resist pixel correlation statistical attack. The correlation distribution of two adjacent pixels for ‘Cameraman’ and ‘Lena’ images by using the proposed method is shown in Figure 5 and 6 respectively. From both the figures, it finds that the correlation of pixels in original image is much higher while the correlation of pixels in encryption image is very much small. Therefore the proposed algorithm can effectively resist pixel correlation statistical attack.

Table 1
Comparison of Correlation Coefficients between Reference [15] and the Proposed Method

			Encrypted images							
Correlation Coefficient	*Plain images*		*Reference [15]*						*Image encryption by proposed method*	
			Lena			*Peppers*				
	Lena	*Peppers*	*10th iteration*	*70th iteration*	*100th iteration*	*10th iteration*	*70th iteration*	*100th iteration*	*1st iteration*	*1st iteration*
Horizontal (H)	0.9400	0.9478	0.0135	–0.0092	0.0049	0.019	0.0072	0.0043	-0.0112	- 0.0039
Vertical (V)	0.9693	0.9482							-0.0280	-0.0377
Diagonal (D)	0.9179	0.9036							0.0018	-0.0009

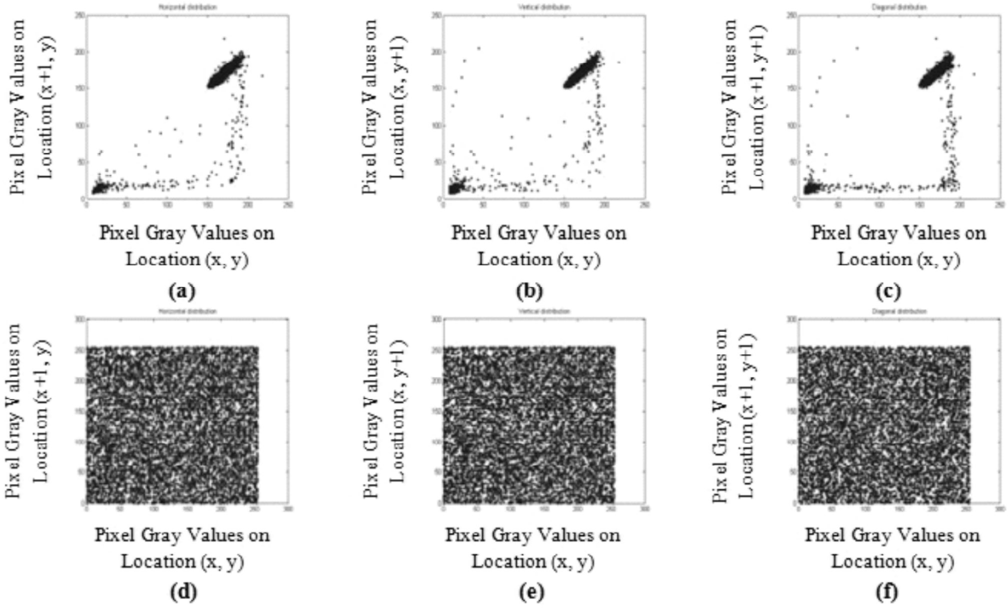

Figure 5: Correlation distribution of two adjacent pixels for ‘Cameraman’ image: (a) Horizontal correlation, (b) vertical correlation, and (c) diagonal correlation of two adjacent pixels of original ‘Cameraman’ image ; (d) Horizontal correlation, (e) vertical correlation, and (f) diagonal correlation of two adjacent pixels of encrypted ‘Cameraman’ image by using the proposed method

4.3. Ability to Resist Differential Attack

The role of all the encryption technique is to convert original image into encrypted image. The conversion is such that there should be large difference between encrypted image and original image. To quantify such differences, three measures mostly used, which are MAE (Mean Absolute Error), NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) [25].

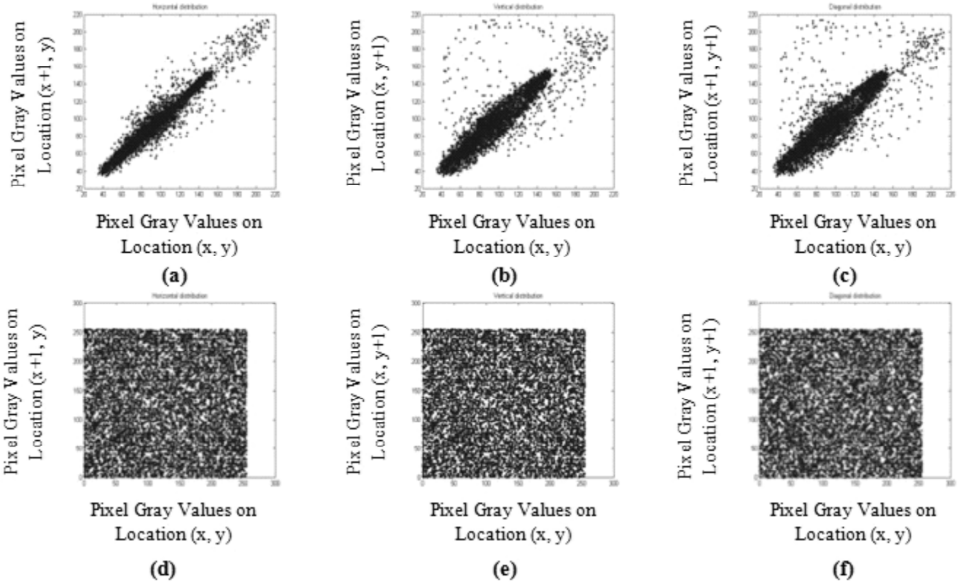

Figure 6: Correlation distribution of two adjacent pixels for 'Lena' image: (a) Horizontal correlation, (b) vertical correlation, and (c) diagonal correlation of two adjacent pixels of original 'Lena' image ; (d) Horizontal correlation, (e) vertical correlation, and (c) diagonal correlation of two adjacent pixels of encrypted 'Lena' image by using the proposed method

The mathematical expression [25] for calculating MAE is

$$MAE = \frac{1}{M \times N} \Sigma_{i=1}^{M} \Sigma_{j=1}^{N} \left| a_{ij} - b_{ij} \right| \tag{6}$$

where $M \times N$ is the size of the original and encrypted images. are the parameters used to represent the gray scale pixel values in original images and encrypted images respectively. The security of the encrypted images is dependent on the value of MAE. For a good quality of encryption, the MAE value should be larger [25].

NPCR is the pixel changing rate of encrypted image when changing one pixel in the original image during the process of encryption. The sensitivity of key and the plaintext depends on the closeness of NPCR value towards 100%. The more closeness towards 100%, the more resistive towards the plaintext attack [24].

The mathematical expression for calculating NPCR [25] is

$$NPCR = \frac{1}{W \times H} \Sigma_{i=1}^{W} \Sigma_{j=1}^{H} D(i, j) \times 100\% \tag{7}$$

where,

$$D(i, j) = \begin{cases} 0, \ if \ C_1(i, j) = C_2(i, j) \\ 1, \ if \ C_1(i, j) \neq C_2(i, j) \end{cases} \tag{8}$$

W and H represents the width and height of the images respectively, C_1 is the original cipher image and C_2 is the cipher image after changing one pixel in a plain image at position (i, j). For a 256 gray-scale image, the ideal value of NPCR is found to be 99.6094%. The larger is the value; the better is the encryption quality [26].

UACI is the rate of change of average strength of the original image and the encrypted image. For an effective cryptosystem, the UACI value should be larger and larger the UACI value, more resistive towards the differential attack [24].

The mathematical expression for calculating UACI [25] is

$$UACI = \frac{1}{W \times H}\left(\Sigma_{i=1}^{W} \Sigma_{j=1}^{H} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right) \times 100\% \tag{9}$$

Where and represents the width and height of the images respectively, C_1 is the original cipher image and C_2 is the cipher image after changing one pixel in a plain image at position (i, j). For a 256 gray-scale image, the ideal value of UACI is found to be 33.4635 %. The larger is the value; the better is the encryption quality [26].

The NPCR, UACI and MAE criteria of the proposed method are presented in Table 2.

Table 2
NPCR, UACI, and MAE criteria of the Proposed Method

Criteria (expected value)	*Image*	*Proposed Method*
NPCR (99.61%)	Cameraman	99.6414
	Lena	99.5926
UACI (above 33.46%)	Cameraman	46.3616
	Lena	38.4996
MAE (Larger Value)	Cameraman	118.2247
	Lena	98.1725

4.4. Information Entropy Analysis:

Information entropy is the randomness measurement of an image which will characterize the appearance of an image [21]. The formula [15] for measuring information entropy is:

$$H = \Sigma_{i=0}^{M-1} p_i \log \frac{1}{p_i} \tag{10}$$

Where H is the information entropy, M is the total number of symbols used for randomness measurement and p_i is the probability of the number of symbols used [21].

For a gray level image of 256 symbols, the maximum information entropy will be $H = 8$ [21]. It will be harder for the eavesdroppers to decode the cipher images, if the value for information entropy is close to 8. Table 3 presents the comparison of information entropy of encrypted image between Reference [15] and

Table 3
Comparison of information entropy between Reference [15] and the proposed method

Fitness function : Entropy				
Images		*Reference [15]*		*Image encryption by proposed method*
	10th Iteration	*70th Iteration*	*100th Iteration*	*1st Iteration*
Lena	7.9822	7.9888	7.9923	7.9953
Peppers	7.9873	7.9928	7.9929	7.9934

the proposed method. The proposed system presents more randomness through only one round encryption process resulting better encryption.

5. CONCLUSION

In this paper, a secure image encryption and decryption method has been suggested by using chaotic logistic map function, crossover and mutation operator. The novelty of this scheme is that even in the first iteration, the use of crossover and mutation operation gives better results. The proposed image encryption scheme has strong ability of resisting all the known attacks. This shows that the proposed scheme is good and is more appropriate for image encryption.

ACKNOWLEDGEMENTS

This research work is supported by Information Security Education Awareness (ISEA) project phase – II, Department of Electronics and Information Technology (DeitY), Govt. of India.

REFERENCES

[1] M. Prasad, and K. L. Sudha, “Chaos image encryption using pixel shuffling,” Computer Science & Information Technology (CS & IT) CCSEA, pp. 169-179, 2011.

[2] Q. Zhang, L. Guo, and X. Wei, “Image encryption using DNA addition combining with chaotic maps,” Mathematical and Computer Modelling, Vol. 52, no. 11, pp. 2028-2035, 2010.

[3] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” Chaos, Solitons & Fractals, Vol. 21, no. 3, pp. 749-761, 2004.

[4] H. Gao, Y. Zhang, S. Liang, and D. Li, “A new chaotic algorithm for image encryption,” Chaos, Solitons & Fractals, Vol. 29, no. 2, pp. 393-399, 2006.

[5] R. Guesmi, M. A. Farah, A. Kachouri, and M. Samet, “A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2,” Nonlinear Dynamics, Vol. 83, no. 3, pp. 1123-1136, 2016.

[6] R. Guesmi, M. A. Farah, A. Kachouri, and M. Samet, “Hash key-based image encryption using crossover operator and chaos,” Multimed Tools Appl, Vol. 75, pp. 4753–4769, 2016.

[7] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” International Journal of Bifurcation and chaos, Vol. 8, no. 06, pp. 1259-1284, 1998.

[8] N. K. Pareek, V. Patidar, and K. K. Sud, “Image encryption using chaotic logistic map,” Image and Vision Computing, Vol. 24, no. 9, pp. 926-934, 2006.

[9] K. W. Wong, B. S. Kwok, and W. S. Law, “A fast image encryption scheme based on chaotic standard map,” Physics Letters A, Vol. 372, no. 15, pp. 2645-2652, 2008.

[10] X. Y. Wang, L. Yang, R. Liu, and A. Kadir, “A chaotic image encryption algorithm based on perceptron model,” Nonlinear Dynamics, Vol. 62, no. 3, pp. 615-621, 2010.

[11] A. Kanso, and M. Ghebleh, “A novel image encryption algorithm based on a 3D chaotic map,” Communications in Nonlinear Science and Numerical Simulation, Vol. 17, no. 7, pp. 2943-2959, 2012.

[12] X. Tong, and M. Cui, “Image encryption with compound chaotic sequence cipher shifting dynamically,” Image and Vision Computing, Vol. 26, no. 6, pp. 843-850, 2008.

[13] A. Nikolaidis, and I. Pitas, “Asymptotically optimal detection for additive watermarking in the DCT and DWT domains,” IEEE Transactions on Image Processing, Vol. 12, no. 5, pp. 563-571, 2003.

[14] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. Liu, “Double image encryption by using iterative random binary encoding in gyrator domains,” Optics Express, Vol. 18, no. 11, pp. 12033-12043, 2010.

[15] A. H. Abdullah, R. Enayatifar, and M. Lee, “A hybrid genetic algorithm and chaotic function model for image encryption,” AEU-International Journal of Electronics and Communications, Vol. 66, no. 10, pp. 806-816, 2012.

[16] [Available online]

http://geoffboeing.com/2015/03/chaos-theory-logistic-map/.

[17] [Available online]

http://mpe2013.org/2013/03/17/chaos-in-an-atmosphere-hanging-on-a-wall/.

[18] N. K. Pareek, and V. Patidar, "Medical image protection using genetic algorithm operations," Soft Computing, Vol. 20, no. 2, pp. 763-772, 2016.

[19] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," Optics Communications, Vol. 284, no. 19, pp. 4331-4339, 2011.

[20] A. Kulsoom, D. Xiao, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," Multimedia Tools and Applications, Vol. 75, no. 1, pp. 1-23, 2016.

[21] X. Wang, and H. L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," Nonlinear Dynamics, Vol. 83, no. 1-2, pp. 333-346, 2016.

[22] J. Zhang, D. Fang, and H. Ren, "Image encryption algorithm based on DNA encoding and chaotic maps," Mathematical Problems in Engineering, 2014.

[23] Q. Zhang, and X. Wei, "RGB color image encryption method based on Lorenz chaotic system and DNA computation, IETE Technical Review, Vol. 30, no. 5, pp. 404-409, 2013.

[24] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," Signal Processing, Vol. 92, no. 4, pp. 1101-1108, 2012.

[25] E. Borujeni, Shahram, and M. Eshghi, "Chaotic image encryption design using Tompkins-Paige algorithm," Mathematical Problems in Engineering 2009.

[26] C. Chattopadhyay, B. Sarkar, and D. Mukherjee, "Encoding by DNA Relations and Randomization Through Chaotic Sequences for Image Encryption," arXiv preprint arXiv:1505.01795, 2015.