International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.4, pp.01-08, August (2018)

Research Paper

E-ISSN: 2320-7639

Image Encryption using Linear Cryptanalysis and different Fuzzy operations

Dipankar Dey

University of Mysore, Karnataka - 570006, Global Institute of Science and Technology, Haldia-721657, India

Available online at: www.isroset.org

Accepted: 19/Aug/2018, Online: 31/Aug/2018

Abstract — Nowadays, the security of digital image is one of the most essential terms. In this article, a piecewise linear chaotic map based image encryption has been proposed. For implementation protection from different types of attacks, the Linear Cryptanalysis system is applied to encrypt the image. The irreducible polynomial is implemented to design the confusion - diffusion architecture that scrambles the pixel position of the image. To alter pixel intensity, the Fuzzy operations have been applied which makes the scheme more secure. The proposed encryption scheme is applied to resist some cryptanalysis method such as plaintext or cipher text attacks. The different theoretical and statistical analysis shows that the scheme has high -level security. The two main statistical factors, the number of pixel change rate and the information entropy, gives the better result in this article.

Keywords— Encryption, PWLC map, irreducible polynomial, Fuzzy operations, Linear Cryptanalysis

1. Introduction

Nowadays, the human need to guard their sensitive data from unauthorized users. But, during the modern communication channel, it is being rather complex to protect sensitive information from different types of attacks. Since the attackers use different mathematical functions to crack the security code and access the sensitive information. There are different types of functions such as Plaintext Attack, Cipher text Attacks, Brute Force Attack, Birthday Attack etc are used to crack the sensitive information. So, it is more challenging to protect information different kinds of attacks and make the information more secure.

This article focus only to protect important images from unauthorized users. Here images are grayscale images mainly. There are different algorithm [11, 12] proposed by different authors that encrypt the images and make them secure. Here, this article develops a new cryptographic algorithm that not only encrypts the grayscale images but also makes them secure from different kinds of attacks. There are different fields where the image encryption is used and some of them are online communication, sending multimedia data, military encryption in the Armed Forces, protecting satellite image and many more.

In this article, a new scheme has been designed for protecting the sensitive image from unauthorized users and different types of attacks. This article states that the image is encrypted using a PWLC (piecewise linear chaotic) map, the Linear Cryptanalysis [10] and some Fuzzy operations. Actually, this scheme is divided into three sections. The first section develops the confusion - diffusion architecture using the irreducible polynomial. The confusion - diffusion architecture shuffles the positions of the pixel of the image. In the second section, the image changes their pixel intensity using the Fuzzy operations. In the final section, this scheme implements the Linear Cryptanalysis theory that not only encrypt the image but also make the scheme more secure from different types of attacks. Here, the PWLC map generates the random number sequence, which is used with the linear Cryptanalysis to encrypt the image. Then using different theoretical and statistical analysis, it is proved that the scheme is secure from different types of attacks and protects the important image from unauthorized access.

The remainder of this paper is organized as follows: Section 2 describes the literature review of some scheme. The preliminaries of this scheme are illustrated in Section 3. The proposed algorithm is dictated in Section 4 and security of this scheme is shown in Section 5. The last Section 6 describes the conclusion of this scheme.

1.1 Contribution of this study

This article describes a grayscale image encryption scheme and the contributions of this scheme are as follows:

1. An irreducible polynomial being used to implement confusion - diffusion architecture that scrambling the pixel positions of the image.

2. The Fuzzy operations are used to change the pixel intensity.

3. The PWLC map generates the random sequence.

4. The linear Cryptanalysis implements the security system of this scheme.

5. The numerous theoretical and statistical analyses show that the scheme is secure and protected from different types of attacks. The two important factors such as NPCR and Information Entropy display the satisfied results in this scheme.

Table 1: NOMENCLATURE

Term	Usage
μ	a Threshold value i.e., $3.57 \leq \mu \leq 4$
$\lfloor \rfloor$	Floor function
$\oplus$	Bitwise xor operation
dx	Change in the value of x
dx	Change in the value of y
W	Column of the image
H	Row of the image
X_0	Initial value of the chaotic map
X_i	i-th value of the chaotic map
P_i	i-th pixel's intensity value
C_i'	i-th pixel's modified intensity value
$H(S)$	Entropy
L	Total number of pixels
$k_{11}, k_{22}, k_{33}, k_{44}$	Secret keys
r	Correlation coefficient
η	Parameter of the PWLC map
$\vee$	Fuzzy union, ususally max
$\wedge$	Fuzzy intersection, usually min
$F(x_{i-1}, \eta)$	PWLC map
k_1, k_2, k_3, k_4	Secret keys

2. RELATED WORK

Thang et al. [1] introduce a color image encryption scheme using cryptanalysis. In this scheme, they protect the encryption algorithm from different types of attacks by using cryptanalysis. This scheme is successful by restoring the permutation process in the case of several rounds. The proposed algorithm is strongest for protecting its different equation from the chosen cipher text attack. The different statistical analysis focuses on the security system of this scheme.

David et al. [2] proposed an image encryption algorithm based on a new shuffling process. The proposed method consists of two methods, one method is the permutation process that encrypts the image and another is the xor operation that shuffles the pixel positions. The xor operations are controlled by the hyper-chaotic system. Based on cryptanalysis concept, the security system of this scheme is implemented. So this scheme has powerful protection against different types of attacks.

Alvarez et al. [3] present a scheme about a nonlinear chaotic algorithm (NCA) for image encryption. This scheme based on a pseudo-random stream generator function, which encrypts the image. This random number is generated by the nonlinear chaotic algorithm, which is

$$x_{n+1} = (1-\beta^{-4}) \cdot cot(\frac{\alpha}{1+\beta}) \cdot (1+\frac{1}{\beta})^{\beta} \cdot tan(\alpha x_n) \cdot (1-x_n)^{\beta}$$

where x $\in$ (0,1), α $\in$ (0,1.4), β $\in$ (5,43). The cryptanalysis here used to protect against security analysis.

Chao et al. [5] proposed this scheme. In this scheme, an image is encrypted using Fuzzy synchronization of Chaos Systems. They apply the Fuzzy sliding mode controller that implements the chaos synchronization. The Duffing-Holmes chaos states are used to determine the secret key that encrypts the image. In their algorithm, the chaos state sequence is uncorrelated. To alter pixel positions the xor operations are implemented in this algorithm. The different numerical analysis shows that this scheme is secure.

Hinal et al. [6] present a new Fuzzy logic based image encryption technique. This scheme describes that the confidential data transfer using (2,2) secret sharing method. Here fuzzy logic implements the concept of (2,2) secret sharing method. The attacker can not access the useful information or it is difficult to guess any information since the image is protected by fuzzy logic. So this scheme is secure.

Xingyuan et al. [7] proposed this scheme where they encrypt the image using Langton's Ant cellular automaton. In this scheme, an image is scrambled by the ant's cellular movement. The movement's of ants are controlled by PWLC map. This chaotic map alters the pixel position and also diffuses the image. The different experiment results and security analysis shows that this scheme is secure.

Ghebleh et al. [8] describe this algorithm where they encrypt the image using PWLC maps and least squares approximation. The proposed algorithm consists of two parts one is a shuffling phase and another is masking phase. Both phases are implemented with PWLC maps. The least squares approximations are used to scrambling the image. The

simulation results of this algorithm focus on the security system of this algorithm that protects the image from common statistical and security attacks.

3. BACKGROUND

This section focuses on the different parameters that are used in this scheme. Table 1 describes the different symbols, which are used in this scheme.

3.1. **Logistic Map**

A chaotic map [13, 14] is developed as a mathematical model. This map is used as an evolution function that has some chaotic characteristics. This chaotic map generates some discrete or continuous variables. The chaotic map is used to develop the dynamic model. This article implements the Logistic map as a chaotic map, which is given below:

$$X_{i+1} = \mu \cdot X_i \cdot (1 - X_i), \tag{3.1}$$

where $3.57 \le \mu \le 4$ and $0 < X_i < 1$; and $X_0 \in (0,1)$ is considered as a boundary value.

3.2. **Piecewise linear chaotic map**

The piecewise linear chaotic (PWLC) [8] map and logistic map simultaneously generate the random number sequences which are used as the secret keys in this scheme. The PWLC map is defined as:

$$x_i = F(x_{i-1}, \eta) = \begin{cases} \frac{x_{i-1}}{\eta}, & \text{if } 0 \le x_{i-1} < \eta \\ \frac{x_{i-1}-\eta}{0.5-\eta}, & \text{if } \eta \le x_{i-1} < 0.5 \\ F(1 - x_{i-1}, \eta) & \text{if } 0.5 \le x_{i-1} < 1 \end{cases} \tag{3.2}$$

where $x_i \in (0,1)$ and $\eta \in (0, 0.5)$. The PWLC map has the uniform distribution and it has some important features such as confusion, ergodicity and deterministic. These features make this as chaotic nature. So, this map provides a good random sequence, which is used in image encryption.

3.3. **Irreducible polynomial**

The third order irreducible polynomial [4] can be defined as

$$X^3 + X + 1 \tag{3.3}$$

An irreducible polynomial cannot be factored into nontrivial polynomials. Depends on this features, this polynomial is used to design the confusion - diffusion architecture. Here the irreducible polynomial is used to generate a matrix, which is used to implement the confusion - diffusion architecture.

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \tag{3.4}$$

This matrix is used in confusion - diffusion architecture that shuffles the pixel position of the image. Using the inverse matrix, the confused image transformed into the original form. The inverse matrix can be defined as

$$M^{-1} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \tag{3.5}$$

3.4. **Fuzzy operation**

The Fuzzy set [5, 15] theory was invented by Professor Lofti Zadeh at the University of California in 1965. Using membership function, each element of the fuzzy sets is mapped to [0,1]. The membership function can be described as

$$\mu_A : X \to [0, 1] \tag{3.6}$$

where [0,1] describes the real number between 0 and 1. The major two fuzzy operations are union and intersection. The union operation between two fuzzy sets A and B can be defined using membership function as

$$\mu_{A \cup B} = max(\mu_A, \mu_B) \tag{3.7}$$

Similarly, the intersection operation between two fuzzy sets can be defined as

$$\mu_{A \cap B} = min(\mu_A, \mu_B) \tag{3.8}$$

Based on these two fuzzy operations, this scheme design two functions that are used to encrypt and decrypt the images. Before applying the fuzzy operations to the image, the image first converts into fractional numbers and for this reason, the pixel intensities are divided by 257. All fractional pixel intensities are stored on the bi array. The fuzzy operation for encryption is defined below:

$$p_i = fun_1(a, b, n) = \begin{cases} min(1, a_i - b_i) & \text{if } a_i > b_i \\ min(1, 1 - b_i + a_i) & \text{if } a_i < b_i \\ a_i & \text{if } a_i = b_i \end{cases} \tag{3.9}$$

The value of a_i found from the logistic map, n is the number of iteration. The values of pi array again convert to integer form as

$$P_i = \lfloor p_i \cdot 100 \rfloor$$

Similarly, the fuzzy operations for decryption is defined as:

$$q_i = fun_2(a, p, n) = \begin{cases} max(0, a_i - p_i) & \text{if } a_i > p_i \\ max(0, 1 - p_i + a_i) & \text{if } a_i < p_i \\ a_i & \text{if } a_i = p_i \end{cases} \quad (3.10)$$

3.5. **Linear Cryptanalysis**

Linear Cryptanalysis [1, 3, 9] is one of the fundamental parts of the cryptography, which is discovered by Mitsuru Matsui. During the design of the cryptography algorithm, the cryptanalysis is used to test the security system of the algorithm. The cryptanalysis break the security system using different types of attacks such as known plaintext attack, cipher text-only attack, chosen plaintext attack, Man-in-the-middle attacks, dictionary attack etc. In this scheme, the objective of the cryptanalysis is to reduce the weakness of this algorithm and make the scheme more secure that protect the algorithm against different types of attacks.

4. OUR PROPOSED SCHEME

4.1. First step for image encryption: Confusion - Diffusion Architecture

To implement confusion - diffusion architecture, the grayscale image is divided into several 4×4 sub-blocks. Then each sub-block is combined with the irreducible polynomial M (from equation 3.4) and creates new resultant matrices. After combining all the sub-blocks, create another matrix. The new matrix becomes the first encrypted matrix, which shuffles the pixel position of the image. This matrix represents the confusion – diffusion architecture. Figure 1 describes the confusion – diffusion architecture.

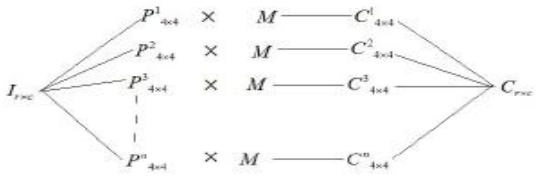

Figure 1: Confusion - diffusion architecture

4.2. Second step for image encryption: Fuzzy operations

After completion of the first stage of the confusing – diffusing architecture, the image is encrypted using different fuzzy operations, which is the second stage of image encryption. In this stage, the intensity of pixels is transformed into a floating-point value and this can be done by dividing the pixel intensity with 257. The resultant floating points value are stored in the b_i array. Then apply the function $fun_1(a,b,n)$ (from equation number 3.9) to change the pixel intensity. Here $fun_1(a,b,n)$ is the function that is generated from the fuzzy operations and the value of a_i is an array generated from the logistic map (from equation 3.1) and n is the number of iterations for successful operations. The resultant floating-point values are again converted to round off pixel intensity operation by equation number 3:4. All the modified pixel intensities are stored in Pi array.

4.3. The third step for image encryption: Linear Cryptanalysis

After changing the intensities of the pixels, the scheme is implemented its security system against different types of attacks by applying the Linear Cryptanalysis concept and this is the third step of the image encryption. The procedure of the third step of image encryption is defined below:

Step 1:

$$\begin{aligned} x_1 &= F(x_1, k_1) \\ x_2 &= F(x_2, k_2) \\ x_3 &= F(x_3, k_3) \\ x_4 &= F(x_4, k_4) \end{aligned}$$

$$\begin{aligned} k_{11} &= \lfloor (x_1 \cdot 10^{14}) \rfloor \,\%253 + 1 \\ k_{22} &= \lfloor (x_2 \cdot 10^{14}) \rfloor \,\%253 + 1 \\ k_{33} &= \lfloor (x_3 \cdot 10^{14}) \rfloor \,\%253 + 1 \\ k_{44} &= \lfloor (x_4 \cdot 10^{14}) \rfloor \,\%253 + 1 \end{aligned}$$

Step 2:

$$\begin{aligned} C_i &= P_i \oplus k_{11} \oplus P_{i+1} \oplus k_{22} \\ C_{i+1} &= C_i \oplus P_{i+2} \oplus k_{33} \\ C_{i+2} &= P_{i+1} \oplus k_{22} \oplus P_{i+2} \oplus k_{33} \end{aligned} \quad (4.1)$$

where $i = 1, 2, ..., 512 \times 512$. Here P_i is the second encrypted image and C_i is the cipher image.

Step 3:

$$\begin{aligned} C'_2 &= C_2 \oplus C'_1 \\ C'_i &= ((C_i + k_{44}) \,\%\, 255) \oplus C'_{i-1} \oplus C'_{i-2} \end{aligned} \quad (4.2)$$

where $i = 3,4,...,512 \times 512$. Here the secret keys k_1, k_2, k_3 and k_4 are found from the chaotic map and the parameters x_1, x_2, x_3 and x_4 are found from the PWLC map. The initial values of the secret keys are k_1 = 0:6779, k_2 = 0:6648, k_3 = 0:2454 and k_4 = 0:3789. The initial values of the parameters of the PWLC map are x_1 = 0:76788, x_2 = 0:99998, x_3 = 0:66345 and x_4 = 0:9789. The values of the secrets keys and the parameters of the PWLC map are changed with respect to each iteration. The initial value of C'_1 = 247. The function F (from equation 3.2) is defined as the PWLC map. Using the above equation (4.2), this scheme generated its final encrypted image C'_i. The following figures describe some examples of encryption and decryption of Lena, Baboon and Barbara grayscale images.

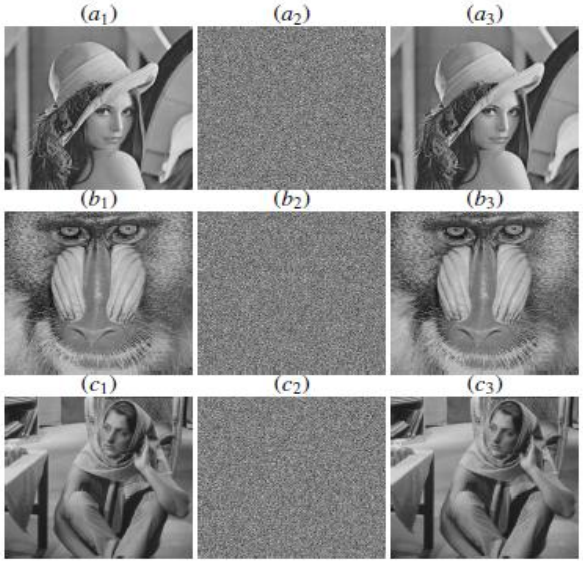

Figure 2: Experimental result of test image

Lena Image: (a_1) Original, (a_2) Encryption, (a_3) Decryption,
Baboon Image: (b_1) Original, (b_2) Encryption, (b_3) Decryption,
Barbara Image: (c_1) Original, (c_2) Encryption, (c_3) Decryption

5. STATISTICAL AND SECURITY ANALYSIS

The confusing - diffusing architecture, irreducible polynomial, PWLC map, fuzzy operations and linear cryptanalysis are used in this scheme to encrypt the images which sufficiently confusing the image so that the attacker cannot access the meaningful information and the image is also protected from unauthorized access. The following different statistical and security analysis shows that the scheme is secure from unauthorized access.

5.1. Histogram Analysis

One of the major parts of the statistical analysis is the histogram analysis [7, 9]. Here, the histogram describes the performance of the image encryption scheme. Figure 3 describes the histogram of the plain images and the chipper images. The histogram between the plain images and the cipher images are distinct from each other and the histograms are uniformly distributed in each of the cipher images. The cipher images have low correlations among the pixel's neighborhood than the plain image, so from this result, it can be proved that the cipher image is confusing sufficiently and the proposed scheme is protected from different types of attacks.

5.2. Information entropy

In 1949, Information entropy [7] concept was proposed by Shannon. It evaluates the unpredictability and randomness of the grayscale images. The following equation (5.1) describes the information entropy concept:

$$H(S) = \sum_{i=0}^{2^L-1} P(S_i) \log_2 \frac{1}{P(S_i)}, \qquad (5.1)$$

where $P(S_i)$ is the probability of the source image S_i, L is the sum of the pixels of the image and $H(x)$ represents the information entropy. This paper calculates the information entropy, which is nearest to the absolute value 8 and using this value 256 gray level values are calculated. This information entropy has been proved that the confusion properties of the image. The information entropy also describes the degree of disorder between the plain image and the cipher images. This scheme calculates the information entropy on different gray scale images such as Lena, Baboon, and Barbara etc. The result shows the unpredictable and randomness of the proposed scheme. Form the result, it is proved that the scheme is secure from different statistical attacks. The following table 2 shows the information entropy of different grayscale images.

Table 2: Entropy test of the different cipher images

	Lena	Baboon	Barbera
Plain image	7.4455	7.3579	7.4664
Cipher image	7.9993	7.9993	7.9993

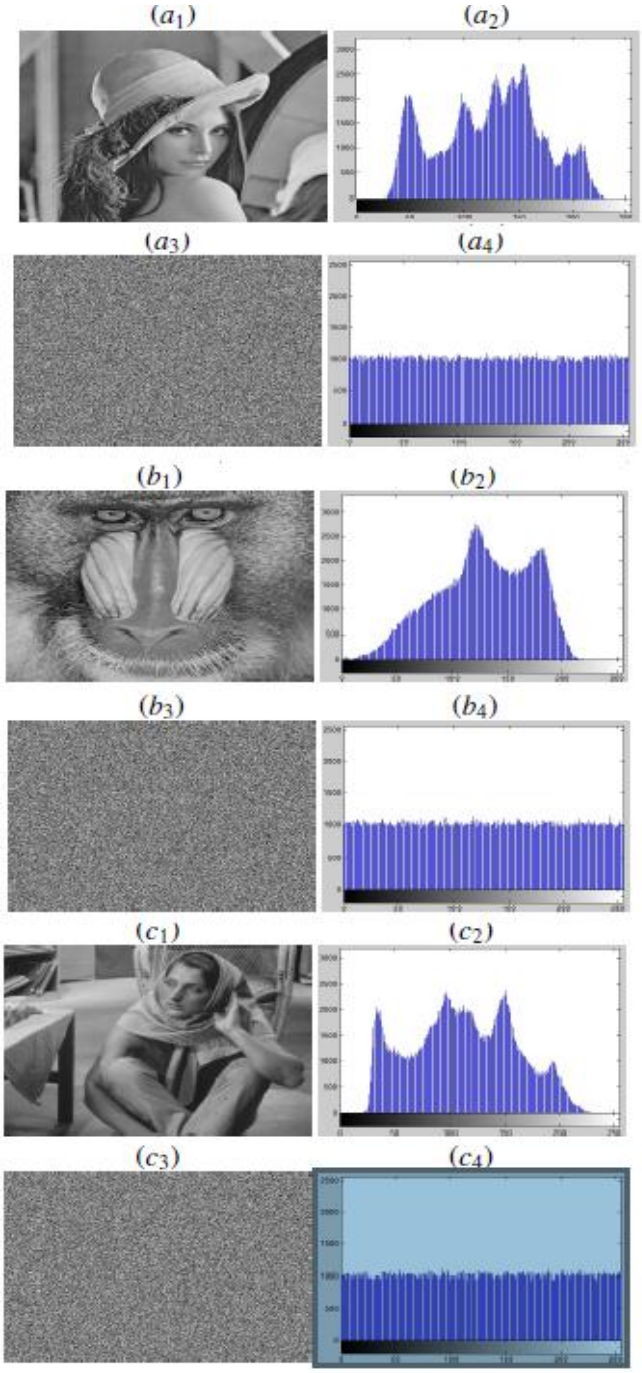

Figure 3: Experimental result of test image

Lena's Components:(a_1) Original Image, (a_2) Histogram of Original image, (a_3) Encrypted image, (a_4) Histogram of Encrypted image,

Baboon's Components: (b_1) Original Image, (b_2) Histogram of Original image, (b_3) Encrypted image, (b_4) Histogram of Encrypted image,

Barbara's Components: (c_1) Original Image, (c_2) Histogram of Original Image, (c_3) Encrypted image, (c_4) Histogram of Encrypted image

5.3. Sensitivity analysis

An attacker tries to break the security system [16] of this scheme by finding some clues by different mathematical calculation or permutation operation. He does it by hacking the secret information or modifying the secret keys of the cipher images. If the attacker tries to change the small information about the encrypted image, he unable to recover the meaningful information from this scheme.

5.3.1. Key Sensitivity

The most vital part of the sensitivity analysis is the key sensitivity. This part describes the decryption algorithm that transforms the cipher image to original form. The following steps describe the decryption algorithm:

Step 1:

$$\begin{aligned} x_1 &= F(x_1, k_1) \\ x_2 &= F(x_2, k_2) \\ x_3 &= F(x_3, k_3) \\ x_4 &= F(x_4, k_4) \end{aligned}$$

$$\begin{aligned} k_{11} &= \lfloor (x_1 \cdot 10^{14}) \rfloor \,\%253 + 1 \\ k_{22} &= \lfloor (x_2 \cdot 10^{14}) \rfloor \,\%253 + 1 \\ k_{33} &= \lfloor (x_3 \cdot 10^{14}) \rfloor \,\%253 + 1 \\ k_{44} &= \lfloor (x_4 \cdot 10^{14}) \rfloor \,\%253 + 1 \end{aligned}$$

Step 2:

$$\begin{aligned} C_1 &= C_1' \\ C_2 &= C_2' \oplus C_1' \\ C_i &= (C_{i-2}' \oplus C_{i-1}' \oplus C_i' + 253 - k_{44}) \,\%\, 253 + 1 \end{aligned}$$

where $i = 3,4,...,512\times512$ and C_1' is the initial pixel of the cipher image.

Step 3:

$$\begin{aligned} P_{i+1} &= k_{22} \oplus C_i \oplus C_{i+1} \oplus C_{i+2} \\ P_{i+2} &= k_{33} \oplus C_i \oplus C_{i+1} \\ P_i &= k_{11} \oplus C_{i+1} \oplus C_{i+2} \end{aligned} \qquad (5.2)$$

where $i = 1,2,...,512 \times 512$. The same secret keys k_1, k_2, k_3, k_4, x_1, x_2, x_3 and x_4 are used for both encryption and decryption algorithms.

Step 4:

The fuzzy operation fun_2 [equation no 3.10] is used for transformed the pixel intensities to the original value.

Step 5:

Use the inverse matrix M^{-1} [equation no 3.5] to use the confusion - diffusion architecture again for reshuffling the pixel positions back to the original form. But any small changes in the secret keys, the attacker is unable to find out the original image (See Figure 7).

Figure 7: Experimental result of test image:

(a_1) Decrypted with the appropriate keys of Lena image,

(a_2) Decrypted with the incorrect keys of Lena image

5.3.2. Plain image sensitivity

The most important factors of the sensitivity analysis [7] are the number of pixels change rate (NPCR) and the unified average changing intensity (UACI). The NPCR and UACI describe the randomness text of this scheme. NPCR states that when one pixel of the plain image is changed, the cipher image should be changed largely so that the attacker is unable to extract the meaningful information. Similarly, UACI states that the average intensities dissimilarities between the cipher image and the original image. The different experimental results show that the estimated expectations and variance of NPCR and UACI get closer to the theoretical values. The theoretical value of NPCR is nearest to 100% and UACI is nearest to 34%. These values state that the attacker cannot crack this scheme

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \cdot H} \cdot (100), \quad (5.3)$$

$$UACI = \left| \frac{\sum_{i,j} |C_1(i,j) - C_2(i,j)|}{L} \right| \cdot \frac{(100)}{W \cdot H}, \quad (5.4)$$

where C_1 and C_2 are two cipher images and the size of the image is $W \cdot H$ (W is column and H is row) and L is the maximum pixel intensity of the image. If $C_1(i,j) = C_2(i,j)$, then $D(i,j) = 1$; otherwise, $D(i,j) = 0$. After encryption, the intensity of almost all pixels is changed in the cipher image. This means that that the disparity between the neighborhood pixels became greater. So this scheme is sensitive to the plain image. Following Table 3 describe the outcome of NPCR and UACI of different ciphered images such as Lena, Bubbon and Barbara.

Table 3: Outcome of NPCR and UACI of different grayscale images

	Lena	Bubbon	Barbara
NPCR	99.7424	99.7284	99.7295
UACI	33.5823	33.4888	33.4589

5.3.3. Correlations of two adjacent pixels

The correlation coefficient [16] is one of the most essential parts of the statistical analysis. The correlation coefficient of the image describes the relationship among the pixels. In the original grayscale image, the correlation values among the pixels are high whereas the cipher image has the lower correlations among the pixels. Here, this scheme determines the correlations among the pixels in x-direction (horizontal), y-direction (vertical) and z-direction (diagonal). The equation (5.5) describes the correlation among the pixels.

$$r = \frac{\sum dxdy}{\sqrt{\sum dx^2 \sum dy^2}} \quad (5.5)$$

where $dx = \left(x - \bar{x}\right)$, $dy = \left(y - \bar{y}\right)$, $\bar{x} = \frac{\sum dx}{n}$, $\bar{y} = \frac{\sum dy}{n}$ and n is the number of values.

Following Table 4 shows the coefficients correlation among the neighborhood pixels in x, y and z directions.

Table 4: Correlations of two adjacent pixels

		Horizontal	Vertical	Diagonal
Lena	Plain Image	0.9398	0.9726	0.9271
	Cipher Image	0.1696	0.1325	0.0159
Baboon	Plain Image	0.8783	0.8476	0.7900
	Cipher Image	0.1363	0.1817	0.0481
Barbara	Plain Image	0.9376	0.9616	0.9219
	Cipher Image	0.1734	0.0985	0.0044

5.3.4. Speed analysis

The speed analysis is the vital part of the image encryption. This section describes that the time required for the execution of this algorithm. The proposed scheme has the less number of computational which help this scheme more simple and the optimal execution time. This scheme is implemented in Matlab 7.50, Intel Core 2 Duo 2.00 GHz, 3.00 GB Memory, and Windows 7 operating system.

6. CONCLUSION

This article has been proposed a grayscale image encryption concept using a confusing - diffusing architecture, irreducible polynomial, PWLC map, fuzzy operations and linear cryptanalysis. Using the confusing-diffusing architecture, this scheme shuffling the pixel position, the image alters its pixel intensities using the fuzzy operations, and then using linear cryptanalysis image is encrypted. The different experimental analysis shows that this scheme is good. This scheme is also focused on protection from different types of known attacks.

References

[1] Thang Manh Hoang and Hoang Xuan Thanh, "Cryptanalysis and security improvement for a symmetric color image encryption algorithm", Optik International Journal for Light and Electron Optics, Vol. 155, pp. 366-383, 2018.

[2] David Arroyo, Chengqing Li, Shujun Li, Gonzalo Alvarez, Wolfgang A. Halang, "Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm", Chaos, Solitons and Fractals, Vol. 41, pp. 2613-2616, 2009.

[3] G. Alvarez, Shujun Li, "Cryptanalyzing a nonlinear chaotic algorithm NCA) for image encryption", Commun Nonlinear Sci Numer Simulat, Vol. 14, pp. 3743-3749, 2009.

[4] https://en.wikipedia.org/wiki/Irreducible polynomial

[5] Chao-Lin Kuo, Lung-Chuan Huang, Shun-Jih Wang, Jui-Sheng Lin, Cheng-Chi Wang and Jun-Juh Yan, "Image Encryption Based on Fuzzy Synchronization of Chaos Systems", IEEE 37th Annual Computer Software and Applications Conference, Vol. 23, pp. 153-154, 2013.

[6] Hinal M. Mudia and P. V. Chavan, "Fuzzy logic based image encryption for confidential data transfer using (2, 2) secret sharing scheme-review", International Conference on Advances in Computer Engineering and Applications, Vol. 10, pp. 404 - 408, 2015.

[7] Xingyuan Wang and Dahai Xu, "A novel image encryption scheme using chaos and Langtons Ant cellular automaton", Nonlinear Dynamics, Vol. 79, pp. 2449-2456, 2015.

[8] M. Ghebleh, A. Kanso and D. Stevanovic, "A novel image encryption algolorithm based on piecewise linear chaotic maps and least squares approximation", Springer Science+Business Media New York, Vol. 77, pp. 7305-7326, 2018.

[9] Wun-She Yap, Raphael C.-W. Phan, Wei-Chuen Yau and Swee-Huay Heng, "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map", Nonlinear Dynamics, Vol. 80, pp. 483-1491, 2015.

[10] Eun-Jun Yoon and Kee-YoungYoo, "Cryptanalysis of a modulo image encryption scheme with fractal keys", Optics and Lasers in Engineering, Vol. 48, pp. 821826, 2010.

[11] Xiao Jun Tong, ZhuWang , Miao Zhang , Yang Liu , Hui Xu and Jing Ma, "An image encryption algorithm based on the perturbed high-dimensional chaotic map", Nonlinear Dynamics, Vol. 80, No. 3, pp. 1493-1508, 2015.

[12] X. Deng and W. Wen, "Optical multiple-image encryption based on fully phase encoding and interference", Optik-International Journal for Light and Electron Optics, Vol. 126(21), pp. 3210-3214, 2015.

[13] N.K.Pareek, VinodPatidar and K.K.Sud, "Image encryption using chaotic logistic map", Image and Vision Computing, Vol. 24, pp. 926-934 ,2006.

[14] Kwok-Wo Wong, "Image Encryption Using Chaotic Maps", Intelligent Computing Based on Chaos, Vol. 184, pp. 333-354, 2009.

[15] Yasaman Hashemi, "Design a new image encryption using fuzzy integral permutation with coupled chaotic maps", International Journal of Research in Computer Science, Vol. 3, pp. 27- 34, 2013.

[16] Jun-xin Chen Zhi-liang Zhu, Chong Fu and Hai Yu, "Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains", Optics Communications, Vol. 341, pp. 263-270, 2015.

Authors Profile

Dipankar Dey pursed B.Sc. Math Honours from Burdwan University, West Bengal in 2001 and MCA Maulana Abul Kalam Azad University of Technology, West Bengal (Formerly known as West Bengal University of Technology), in 2005. He is currently pursuing Ph.D. from University of Mysore, Karnataka and currently working as an Assistant Professor in Global Institute of Science and Technology, Haldia, West Bengal, in Computer Science Technology Department, since 2006. His main research work focuses on Image encryption using chaotic map. He has 12 years of teaching experience.

