An Image Encryption Process based on Chaotic Logistic Map

Article *in* IETE Technical Review · September 2012

DOI: 10.4103/0256-4602.103173

CITATIONS
33

READS
482

4 authors, including:

Mrinal Kanti Mandal
National Institute of Technology, Durgapur
60 PUBLICATIONS **387** CITATIONS
SEE PROFILE

Gourab Dutta Banik
S.N. Bose National Centre for Basic Sciences
25 PUBLICATIONS **177** CITATIONS
SEE PROFILE

Debashis Nandi
National Institute of Technology, Durgapur
71 PUBLICATIONS **195** CITATIONS
SEE PROFILE

An Image Encryption Process based on Chaotic Logistic Map

Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay and Debashis Nandi[1]

Department of Physics, [1]Information Technology, National Institute of Technology, Durgapur, West Bengal, India

Abstract

This paper proposes a high security image encryption technique using logistic map. The proposed image encryption algorithm is described in detail along with its security analysis such as key space analysis, statistical analysis and differential analysis. A comparison in terms of correlation between the initial and transformed images, Number of pixels change rate and unified average changing intensity is also done. The present algorithm has been tested using different images to prove that the encryption method has a great potential and has a good ability to achieve the high confidential security.

Keywords

Chaos, Lyapunov exponent, Correlation coefficient, Information entropy, Key space, Logistic map, Number of pixels change rate, Unified average changing intensity.

1. Introduction

In the past decades, the security of confidential digital images or video objects through a transmission channel against third party attacks becomes more and more attention in the field of information security. The encryption algorithms such as (i) private key encryption methods- DES or Blowfish [1], (ii) public key encryption methods- RSA or El-Gamal [2] are generally not suitable in view of the slow speed of operation, complexity and inability to handling different data formatting. Recently, the idea of using chaos in cryptosystems [3-16] have been explored by many researchers, because the chaotic map satisfied the requirements of a good cryptosystem like simplicity in implementation, sensitivity to initial conditions and parameters, ergodicity, high encryption rate, excellent security, etc. Basically, chaotic sequences are used to confuse the relation between original image and encrypted image by means of varying the pixel values and pixel position.

In this paragraph we will discuss in brief some chaos based image encryption techniques reported in the literature in the recent years. In reference [3] Chen *et al.* proposed to convert a two-dimensional chaotic map to a three-dimensional chaotic map for image encryption by using pixel shuffling and confusing the pixel value from the original image. Two logistic maps with different initial conditions are used in image encryption in [4]. They used 80-bit secret key for the generation of initial conditions of logistic maps and eight different types of operation for the encryption of plane image. A fast image encryption system is proposed in [5] by using chaotic sequences generated by the cascade of chaotic maps. In references [6,7] Gao *et al.* proposed a scheme of total shuffling of the image pixel position and then they used a hyper chaotic system to confuse the pixel value with respect to the original image. Four different third order chaotic systems are used for chaotic sequences generation and pixel shuffling for color image encryption in [8]. In reference [9] Wang and Yu proposed a block encryption technique using dynamic sequences generated by one dimensional multiple chaotic system. Recently, a chaotic block cipher scheme for image encryption based on chaotic tent map is proposed in [10]. In reference [11] Lin and Wang described image encryption algorithm based on chaos with the piecewise linear memristor in Chua's circuit. An image encryption scheme based on chaotic discrete quadratic map and parameter perturbation technique is also described recently in [12].

However, some reported encryption algorithms [13-17] are either inefficient or weak in view of computational complexity and strength of security. In this paper, we have proposed a novel scheme for image encryption based on chaotic logistic map. The proposed scheme uses logistic map with suitable initial condition for varying the pixel values randomly with respect to its initial values of the original image. Next the chaotic sequences of the logistic map are used for pixel shuffling. The proposed algorithm uses a secret key of 32 characters (256-bits) to generate the initial conditions of the logistic map.

The rest of the paper is organized as follows: In section 2 the nature of the chaotic logistic map is described. Section 3 presented the image encryption and decryption algorithms step by step. Experimental results are presented in the section 4. Section 5 presented the security analysis of the proposed encryption scheme such as key space analysis, key and plane image sensitivity analysis, statistical analysis, differential analysis, etc. The conclusion is drawn in the section 6.

2. Characteristics and Behavior of the Logistic Map

Recently, one very simple chaotic map has been studied for cryptography applications is logistic map [4,18]. Mathematically, the logistic map is written as

$$f(x) = rx(1-x)$$
$$x_{n+1} = f(x_n) \quad (1)$$

Where x_n represents the chaotic sequence which lies between zero and one as shown in the Figure 1. The initial condition of the map is $x_{n=0} = x_0 \in [0,1]$. The parameter r is a positive number in the range 0 to 4. Depending on the value of r the Eq. (1) has different properties as mention below. When r between 0 and 1 the value of $x_n = 0$ independent of the initial conditions x_0. When r between 1 and 3 the value of x_n stabilize on the value $(r-1)/r$ independent of the initial conditions x_0. When r between 3 and $1+\sqrt{6}$ (approximately 3.45) the value of x_n oscillate between two values forever depending on r. When r between 3.45 and 3.54 (approximately) the value of x_n oscillate between four values forever. With r slightly bigger than r the value of x_n oscillate between 8 values, then 16, 32, etc. This behavior is an example of a period-doubling cascade. At r approximately 3.57 is the onset of chaos, at the end of the period-doubling cascade. In this region slight variations in the initial condition yield dramatically different results over time, a prime characteristic of chaos. The values beyond 3.57 exhibit chaotic behavior, but there are still certain isolated values of r that appear to show non-chaotic behavior; these are sometimes called islands of stability. For instance, beginning at $1+\sqrt{8}$ (approximately 3.83) there is a range of parameters r which show oscillation between three values, and for slightly higher values of r oscillation between 6 values, then 12 etc. There are other ranges which yield oscillation between 5 values etc. In this way all oscillation periods do occur but beyond $r = 4$, the value of x_n eventually leave the interval $[0,1]$ and x_n diverge for almost all initial values of x_0. These phenomena are illustrated in Figure 2. The different region of chaos for r between 3.57 and 4 are shown in Figure 3 by plotting the Lyapunov exponents (Λ) with r. The expression of the Lyapunov exponent for the orbit starting at x_0 is given by

$$\Lambda = \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(x_i)\right|\right\}. \quad (2)$$

In this paper, we have taken the parameter $r = 3.999$ of the logistic map in the chaotic region having positive Lyapunov exponents as shown in Figure 3.

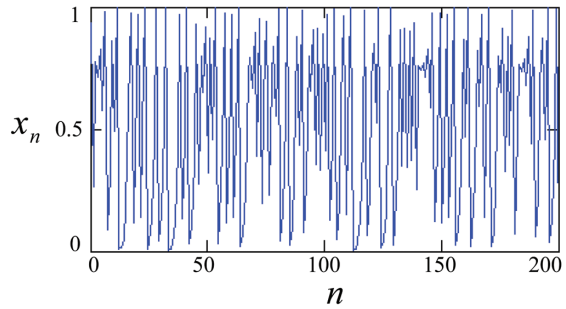

Figure 1: Variation of chaotic logistic map with iteration values.

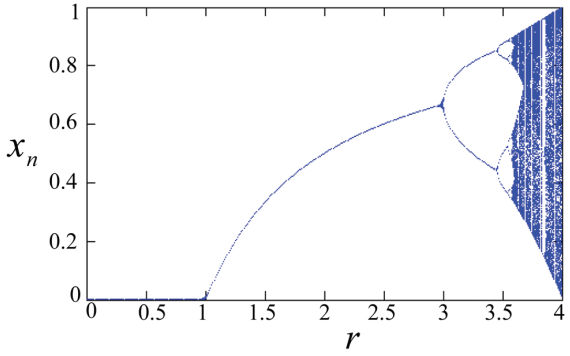

Figure 2: Bifurcation diagram of the logistic map.

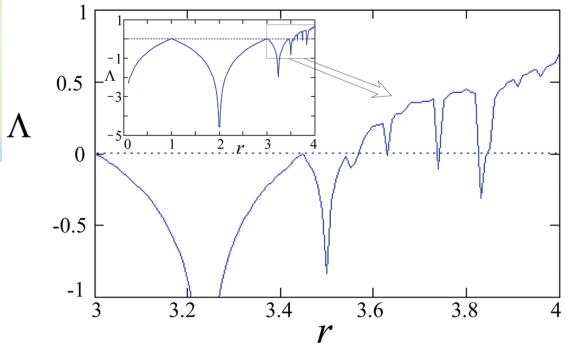

Figure 3: Lyapunov exponents of the logistic map.

3. The Proposed Image Encryption and Decryption Algorithm

The encryption algorithm includes three major steps. The first step is used to generate the chaotic sequences. Second step confused the pixel values and third step shuffled the pixel position to produce the required encrypted image. Let f be an image of size $M \times N$. The pixel of f is denoted by $f(i,j)$, where i and j is in the range of $1 \le i \le M$ and $1 \le j \le N$. Now, $f(i,j)$ denotes the gray value at the pixel position (i,j) of the image f. The initial condition for the logistic map is extracted from the secret key of 256 bits (32 characters) taken in ASCII form denoted as $K = K_1K_2K_3.....K_{32}$ (K_i denotes the 8-bit key character in the i-th key position). The value of the initial condition for the logistic map is given by.

$$x_0 = \sum_{i=1}^{32} \mathrm{mod}\left(K_i \times 10^i, 1\right) \quad (3)$$

The step by step procedure of the algorithm is discussed below.

Step 1: Transform the image of size $M \times N$ pixels into an array of $P_i = \{P_1, P_2, P_3, \cdots, P_n\}$, where $i = 1, 2, 3, \cdots, n$ and $n = M \times N$. Next convert the pixel values to unsigned integer in the range of 0 to 255 using mod operation.

Step 2: Generate n number of chaotic sequence $x_i = \{x_1, x_2, x_3, \cdots, x_n\}$ in the range 0 to 1 using the logistic map mention in Eq. (1) with initial condition x_0 and taking the parameter $r = 3.999$. Next convert x_i into unsigned integer in the range of 0 to 255 using mod operation.

Step 3: Generate the sequence $C_i = P_i \oplus x_i$ for confusing the pixel value. The sign $\oplus$ indicates bitwise XOR operation.

Step 4: Transform $C_i = \{C_1, C_2, C_3, \cdots, C_n\}$ to an array of size $M \times N$ to get the image f'. Next add one to the unsigned integer sequence $x_i = \{x_1, x_2, x_3, \cdots, x_n\}$ and transform it into an array of size $M \times N$ to get X.

Step 5: Finally execute the following two steps for pixel shuffling to get the required encrypted image f. Here j and k varies from 1 to 255. The symbol $\Leftrightarrow$ indicates the interchange the values between two pixel position of f'.

$$f'\left(X(j,j),k\right) \Leftrightarrow f'\left(X(j+1,j+1),k\right)$$

$$f'\left(k,X(j,j)\right) \Leftrightarrow f'\left(k,X(j+1,j+1)\right). \quad (4)$$

Now f is the final encrypted image. The decryption of the image is the inverse process of encryption.

4. Experimental Results

Experiments are done using different original images (plain-images) to prove the validity of the proposed algorithm. Figures 4a–7a show four different plain-images and Figures 4b–7b show their encrypted images (cipherimagrs) using key zxcvbnmlkjhgfdsa1234567890!@#$%**x**. All the encrypted images look like alike and they will carry no visual information about their plain-images. The decrypted images using the same key zxcvbnmlkjhgfdsa1234567890!@#$%**x** are shown in Figures 4c–7c, whereas decrypted images using slightly different key zxcvbnmlkjhgfdsa1234567890!@#$%**y** are also shown in Figures 4d–7d. From

Figure 4: Application of the encryption/decryption algorithm to the image Lena: (a) Plane image; (b) Encrypted image using key zxcvbnmlkjhgfdsa1234567890!@#$%**x**; (c) Decrypted image using same key of encryption; (d) Decrypted image using wrong key zxcvbnmlkjhgfdsa1234567890!@#$%**y**.

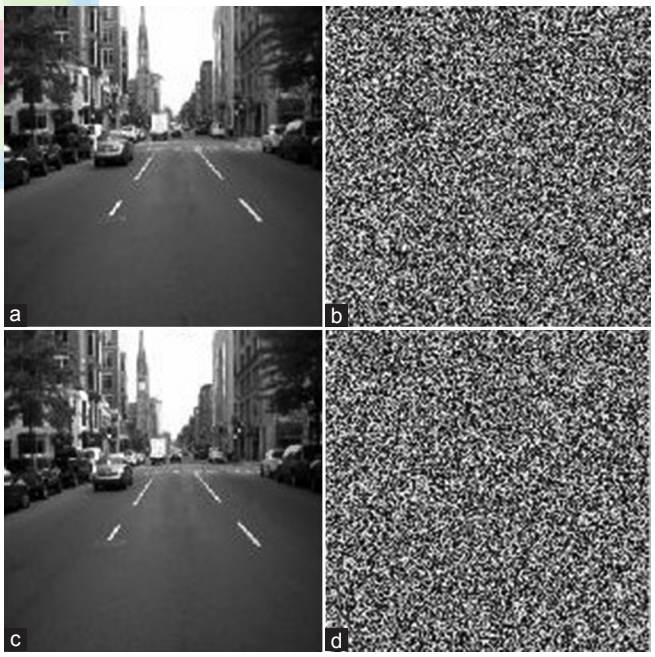

Figure 5: Application of the encryption/decryption algorithm to the image Road: (a) Plane image; (b) Encrypted image using key zxcvbnmlkjhgfdsa1234567890!@#$%**x**; (c) Decrypted image using same key of encryption; (d) Decrypted image using wrong key zxcvbnmlkjhgfdsa1234567890!@#$%**y**.

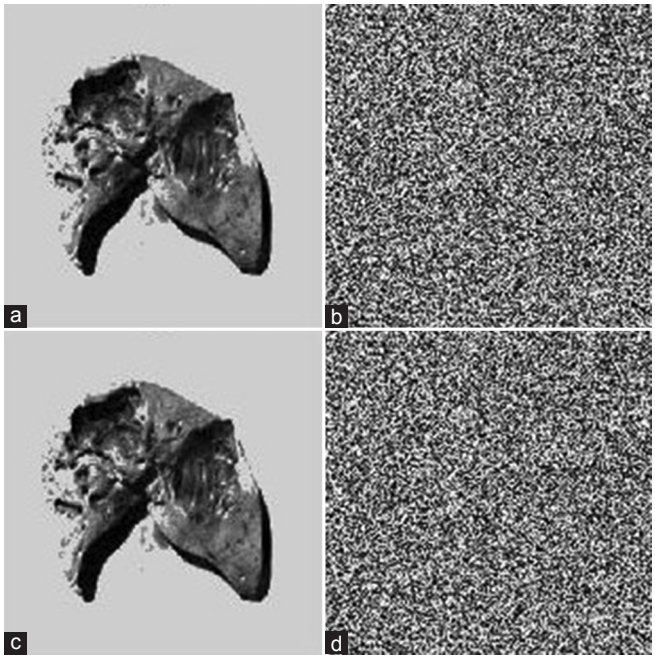

Figure 6: Application of the encryption/decryption algorithm to the image Liver: (a) Plane image; (b) Encrypted image using key zxcvbnmlkjhgfdsa1234567890!@#$%**x**; (c) Decrypted image using same key of encryption; (d) Decrypted image using wrong key zxcvbnmlkjhgfdsa1234567890!@#$%**y**.

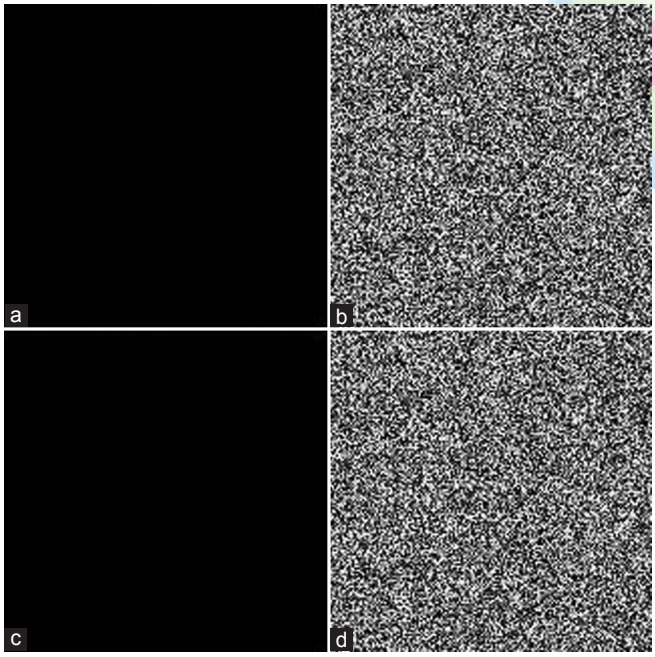

Figure 7: Application of the encryption/decryption algorithm to the image Black: (a) Plane image; (b) Encrypted image using key zxcvbnmlkjhgfdsa1234567890!@#$%**x**; (c) Decrypted image using same key of encryption; (d) Decrypted image using wrong key zxcvbnmlkjhgfdsa1234567890!@#$%**y**.

this figure it is clear that decrypted images using the wrong key will carry no information of the original images.

5. Security Analysis

A good chaotic encryption system should be robust against all types of attacks such as cryptanalytic, statistical and brute-force attacks. In this section, we will discuss the security analysis of the proposed algorithm by addressing key space and key sensitivity analysis, statistical analysis, and Differential analysis. The resistance against different types of attacks is a useful measure of the performance of a cryptosystem. Therefore some security analysis results are incorporated in the following subsection to prove the validity of the proposed cryptosystem.

5.1 Key Space Analysis and Key Sensitivity Analysis

A good cryptosystem should have sufficiently large key space to make the brute-force attack infeasible [19,20]. Key spaces imply the total number of different keys which can be used for the purpose of encryption and decryption. The algorithm proposed in the paper uses a 32 character, i.e., 32×8=256 bits key, so that the key space is 2^{256}, which is large enough to avoid brute-force attack according to the present computational speed. On the other hand the encryption and decryption algorithm is highly sensitive to the secret key. The change of a single bit in the secret key should produce a completely different encrypted/decrypted image. Two encrypted images using two different keys zxcv bnmlkjhgfdsa1234567890!@#$%**x** and zxcvbnmlkjhgf dsa1234567890!@#$%**y** (these two key have only one bit different) are more than 99% different in terms of pixel values. The encrypted image cannot be decrypted correctly with a slightly different key as shown in Figures 4d–7d. This analysis proved that the algorithm of the cryptosystem is highly sensitive to the secrete key and it guarantees the security against known plain-text attacks.

5.2 Statistical Analysis

Statistical analysis is crucial importance for a cryptosystem. An ideal cryptosystem should be resistive against any statistical attack. To prove the robustness of the proposed algorithm, we have performed the following statistical test such as histogram analysis, correlation analysis, etc.

5.2.1 Histogram Analysis

Image histogram describes how the image pixels are distributed by plotting the number of pixels (along the *y*-axis) at each intensity level (along the *x*-axis). A good image encryption system should provide uniform image histogram for all encrypted images irrespective the nature of the original plane image. The histogram of four different plane images like- Lena,

Road, Liver and Black are shown in Figures 8a–11a. These histograms show not uniform and large spikes, which correspond to the gray values that appear more often in the plain-images. The histograms of their encrypted images are shown in Figures 8b–11b respectively. Here all the spikes are almost uniformly distributed and significantly different from those of the original images. A histogram of the encrypted image bears no statistical similarity to the plainimage and hence do not provide any clue to employ any statistical attack on the proposed image encryption technique.

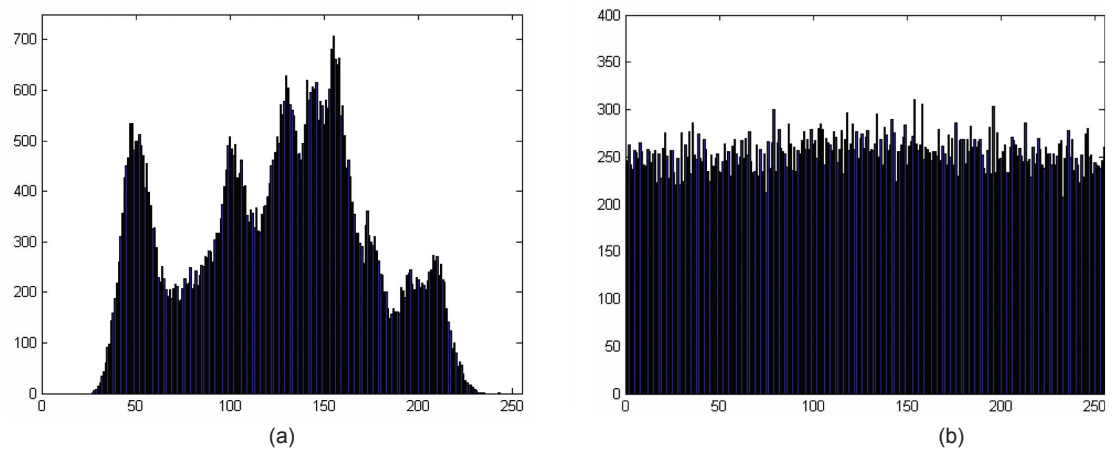

Figure 8: Histogram of the (a) Plane image and (b) Encrypted image of Lena.

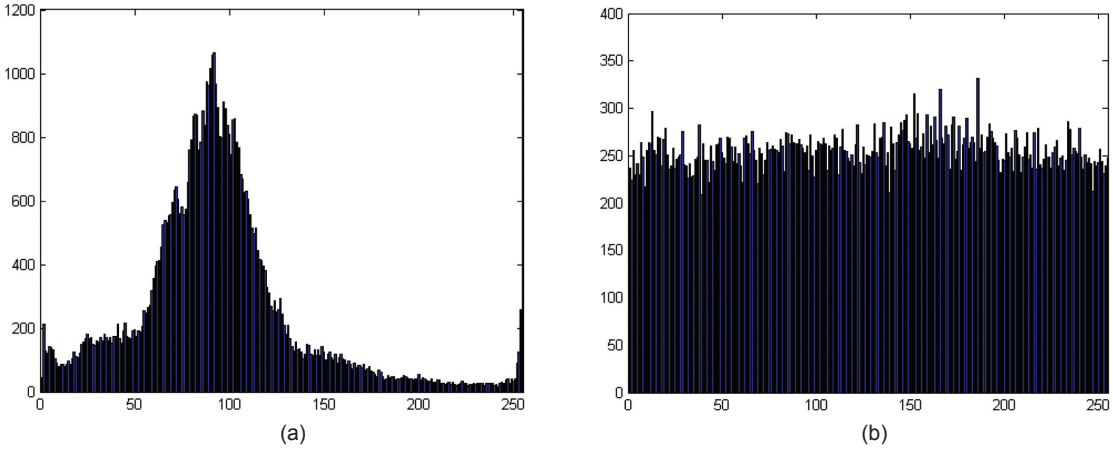

Figure 9: Histogram of the (a) Plane image and (b) Encrypted image of road.

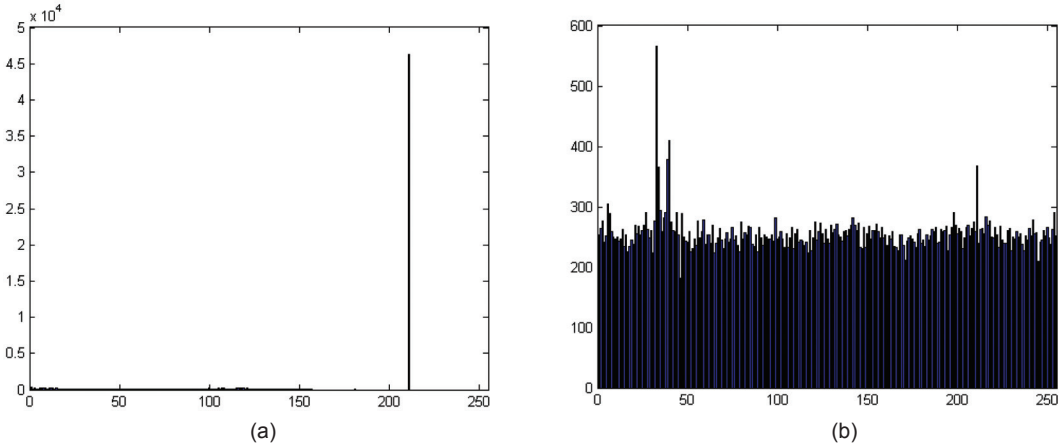

Figure 10: Histogram of the (a) Plane image and (b) Encrypted image of liver.

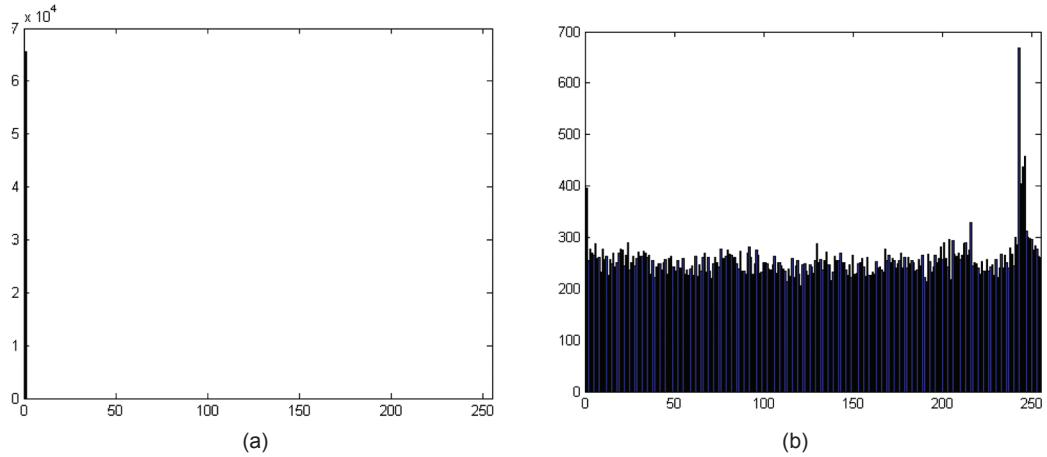

Figure 11: Histogram of the (a) Plane image and (b) Encrypted image of black.

Table 1: Correlation coefficient of two adjacent pixels of plane image and ciphered image

Images	Direction of adjacent pixels	Correlation coefficient of two adjacent pixels	
		Plain-image	Ciphered image using key zxcvbnmlkjhgfdsa1234567890!@#$%x
Lena	Horizontal	0.9242	-0.0564
	Vertical	0.9597	-0.0182
	Diagonal	0.9084	-0.0653
Road	Horizontal	0.9380	-0.0505
	Vertical	0.9584	0.0102
	Diagonal	0.9100	-0.0058
Liver	Horizontal	0.9652	0.0295
	Vertical	0.9659	0.0070
	Diagonal	0.9391	-0.0206

5.2.2 Correlation Co-efficient Analysis

In addition to the histogram analysis we have also studied the correlation between two adjacent pixels of the plane images and the encrypted images. Higher the correlation coefficient indicates high similarities between adjacent pixels and correlation coefficient decreases for adjacent pixels having different intensity. In case of plane image each pixel is usually highly correlated with its adjacent pixels but for good encrypted image these correlations will be very small. The correlation co-efficient ρ can be calculated by using the following formula [3]:

$$\rho = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5}$$

Where x and y are the values of two adjacent pixels of the plane images or ciphered images. To calculate the value of ρ the following discrete formulas can be used.

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

$$D(x) = \frac{1}{I}\sum_{i=1}^{I}\left(x_i - E(x)\right)^2 \tag{7}$$

$$\operatorname{cov}(x,y) = \frac{1}{I}\sum_{i=1}^{I}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{8}$$

Where I is the number of pixel pairs. To calculate correlation coefficient first randomly selects 1000 or more pairs of two adjacent pixels from both the images (i) plane image and (ii) ciphered image. According to the above equations the correlation coefficient of the plane image of Lena is 0.9242 and its ciphered image is -0.0564 along the horizontal direction. Similar results for vertical and diagonal direction are also obtained and shown in Table 1. Same results for the other two images Road and Liver are also obtained as shown in Table 1. The correlation distribution of two horizontally adjacent pixels and two vertically adjacent pixels of plane image with its encrypted image of Lena are shown in Figures 12 and 13 respectively. On the other hand the correlation coefficient between (i) plane image and encrypted image, (ii) plane image and decrypted image are also studied to test the similarity between two images. Here we have selected 1000 pixels from the same positions of two images one is plane image and other one is ciphered image or decrypted image. Table 2 shows the correlation coefficient between the (i) plane image and the ciphered image and (ii) plane image and the decrypted

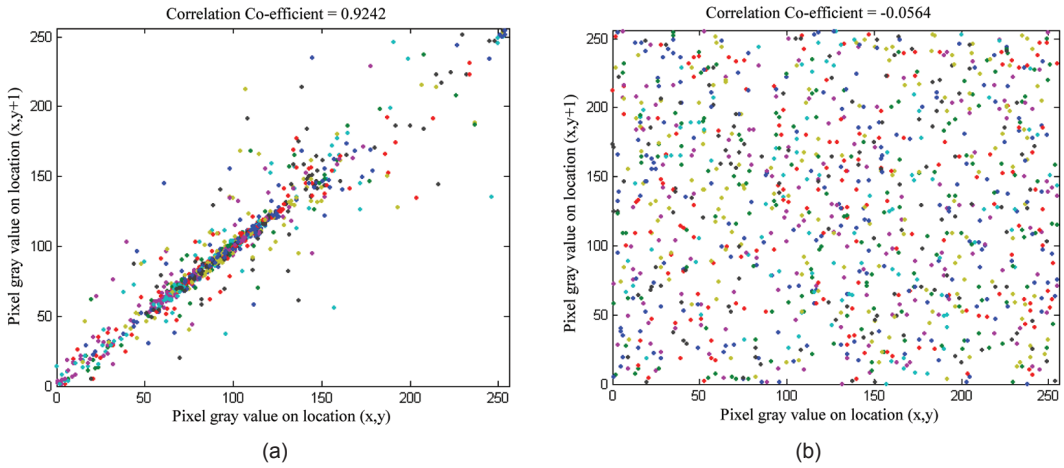

Figure 12: The correlation analysis of two horizontally adjacent pixels of Lena (a) Plane image; (b) Encrypted image.

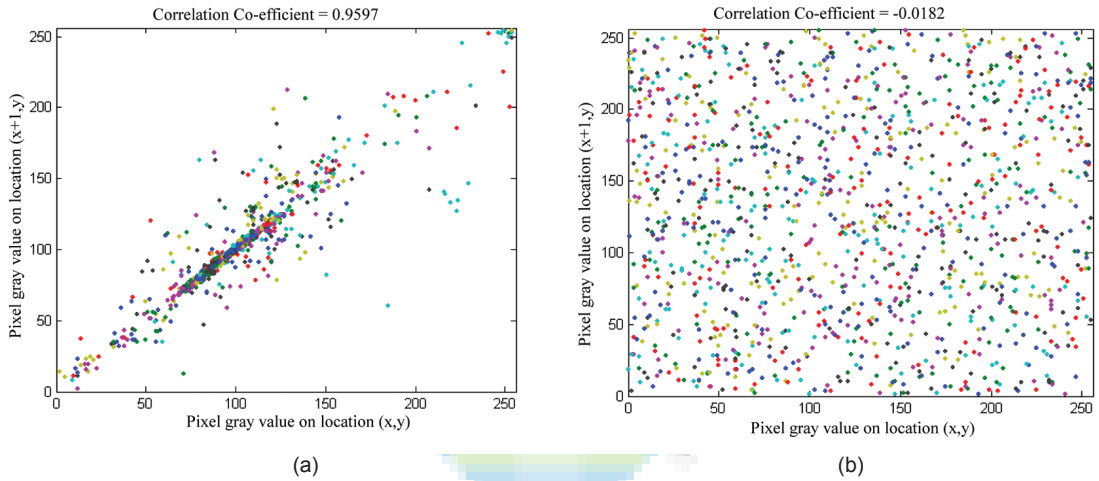

Figure 13: The correlation analysis of two vertically adjacent pixels of Lena (a) Plane image; (b) Encrypted image.

Table 2: Correlation coefficient between two images

Images	Image type & Key	Correlation coefficient
Lena	Plane image & Ciphered image (kay: zxcvbnmlkjhgfdsa1234567890!@#$%x)	-0.0457
	Plane image & decrypted image (kay: zxcvbnmlkjhgfdsa1234567890!@#$%x)	1.0000
	Plane image & decrypted image (kay: zxcvbnmlkjhgfdsa1234567890!@#$%y)	-0.0092
Road	Plane image & Ciphered image (kay: zxcvbnmlkjhgfdsa1234567890!@#$%x)	-0.0811
	Plane image & decrypted image (kay: zxcvbnmlkjhgfdsa1234567890!@#$%x)	1.0000
	Plane image & decrypted image (kay: zxcvbnmlkjhgfdsa1234567890!@#$%y)	-0.0149
Liver	Plane image & Ciphered image (kay: zxcvbnmlkjhgfdsa1234567890!@#$%x)	0.0267
	Plane image & decrypted image (kay: zxcvbnmlkjhgfdsa1234567890!@#$%x)	1.0000
	Plane image & decrypted image (kay: zxcvbnmlkjhgfdsa1234567890!@#$%y)	-0.0017

image with the same key and slightly different key values. These correlation coefficients are used to measure the similarities between the two images. The larger correlation value implies the best match between the two images.

5.2.3 *Information Entropy Analysis*

Entropy is a statistical measure of randomness that can be used to test the robustness of the image encryption algorithm. The measure of entropy [10] of a source m is defined as,

$$H(m) = \sum_i p(m_i) \log_2 \frac{1}{p(m_i)} \tag{9}$$

Where $p(m_i)$ represents the probability of the symbol (pixel value) m_i. Theoretically, a true random system should generate 2^8 symbols with equal probability, i.e., $m = \{m_1, m_2, m_3, \cdots, m_{2^8}\}$ for bit depth 8. Therefore,

according to the above equation the entropy of the system will be $H(m)=8$. All practical information source seldom generates random massages providing entropy value less than the ideal value. An ideal encrypted image should have entropy value 8 but if an encrypted image has entropy value less than 8 then there must be a certain degree of predictability, which threatens its security. Therefore, the higher the entropy value of an encrypted image, the better the security. Table 3 shows the entropy of the plain-images and the encrypted images. From these data it is clear that the entropy of the encrypted image is slightly less than 8, which proves the ability against the entropy attack.

5.3 Number of Pixels Change Rate and Unified Average Changing Intensity

To investigate the difference between the plane image and the encrypted image we have conducted two common tests: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). NPCR denotes the percentage of different pixel numbers between the plane image and the encrypted image and UACI denotes the average intensity of differences between the plane image and the encrypted image. Consider two images: original plane image P and encrypted image C. Let the grayscale values of the pixels at position (*i,j*) are $P(i,j)$ and $C(i,j)$ of the two images P and C respectively. The NPCR and UACI can be defined as [8]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (10)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{P(i,j)-C(i,j)}{2^{L}-1}\right] \times 100\% \quad (11)$$

$$D(i,j) = \begin{cases} 0, & P(i,j) = C(i,j) \\ 1, & P(i,j) \neq C(i,j) \end{cases} \quad (12)$$

Where L is the number of bits used to present the value of the pixel of the image. For 8-bit grayscale image L=8. $D(i,j)$ is a bipolar array with the same size as P and C. The test results for NPCR and UACI are shown in Table 4. The high value of NPCR means the pixel values are dramatically randomized. This result indicates that the plain-image and the encrypted image are significantly different from one another, so the proposed algorithm is highly resistive against differential attack.

5.4 Intensity Tampering Analysis

The proposed image encryption/decryption algorithm can resist illegal tampering of the intensity of the encrypted image to a certain extent. If an attacker modified the encrypted image intensity then the authentic receiver will receive encrypted image with some distortion. Figure 14a-c shows some modified encrypted

Table 3: Entropy analysis of plane image and ciphered image

Images	Plain image	Ciphered image using key zxcvbnmlkjhgf dsa1234567890!@#$%x
Lena	7.4436	7.9666
Road	7.0961	7.9671
Liver	2.9580	7.9607
Black	0.0000	7.9416

Table 4: NPCR and UACI between plane image and ciphered image

Images	NPCR (%)	UACI (%)
Lena	99.6246	28.3321
Road	99.6567	30.9743
Liver	99.4720	34.8958
Black	99.3958	50.7172

NPCR – Number of pixels change rate; UACI – Unified average changing intensity

Figure 14: Illegal tampering of the encrypted images and corresponding decrypted images.

images and their corresponding decrypted images are shown in Figure 14d-f. From these results it is clear that if an attacker modified the encrypted image, the authentic receiver can decrypt the image successfully with some noise as indicated in Figure 14 d-f. Therefore the proposed algorithm can resist illegal tampering to some extent.

6. Conclusion

The paper presented a novel chaos based image encryption technique. The XOR operations and pixel shuffling of the image are used to confuse and defuse the pixel value and pixel position. The key in the chaotic system generates the initial condition, so the security of the chaotic sequences totally dependent on the secrete key. The key of the proposed cryptosystem is very large and totally secure so it can resist brute-force attack also. Moreover, key sensitivity analysis, statistical analysis, information entropy analysis and differential analysis are discussed to prove the good performance of the proposed algorithm.

References

1. B. Schneier. "Applied cryptography- protocols, algorithms and source code in C". John Wiley & Sons, New York, 1996.
2. W. Stallings. "Cryptography and network security: Principles and practice". Prentice-Hall, New Jersey, 1999.
3. G. R. Chen, Y. B. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat map," Chaos, Solitons and Fractals, Vol. 21, pp. 749-61, Mar. 2004.
4. N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image Vision Comput, Vol. 24, pp. 926-34, Sept. 2006.
5. H. S. Kwok, K. Wallace, and S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," Chaos, Solitons and Fractals, Vol. 32, pp. 1518-29, Apr. 2007.
6. T. Gao, Q. Gu, and Z. Chen, "A new image encryption algorithm based on hyper-chaos," Phys. Lett. A, Vol. 372, pp. 394-400, Apr. 2008.
7. T. Gao, and Z. Chen, "Image encryption based on a new total shuffling algorithm," Chaos, Solitons and Fractals, Vol. 38, pp. 213-20, Jan. 2008.
8. C. K. Huang, and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," Optical communications, Vol. 282, pp. 2123-7, Feb. 2009.
9. X. Y. Wang, and Q. Yu, "A block encryption algorithm based on dynamic sequences of multiple chaotic systems," Commun Nonlinear Sci Numer Simulat, Vol. 14, pp. 574-81, 2009.
10. M. Amin, O. S. Faragallah, and A. A. El-Latif, "A chaotic block cipher algorithm for image cryptosystems" Commun Nonlinear Sci Numer Simulat, Vol. 15, pp. 3484-97, 2010.
11. Z. Lin, and H. Wang, "Efficient image encryption using a chaos-based PWL meristor," IETE Technical Review, Vol. 27, pp. 318-25, Jul-Aug 2010.
12. D. Chattopadhyay, M. K. Mandal, and D. Nandi, "Robust chaotic image encryption based on perturbation technique," ICGST- GVIP, Vol. 11, pp. 41-50, Apr. 2011
13. H. Cheng, and X. Li, "Partial encryption of compressed images and videos," IEEE Trans. Signal processing, Vol. 48, pp. 2439-51, Aug. 2000.
14. Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," Int J Bifurcation & chaos, Vol. 14, pp. 3613-24, Oct. 2004.
15. K. Wang, W. Pei, L. Zou, A. Song, and Z. He, "On the security of 3D cat map based symmetric image encryption scheme," Phys Lett A, Vol. 343, pp. 432-9, June. 2005.
16. R. Rhouma, and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper chaos," Phys Lett A, Vol. 372, pp. 5973-8, 2008.
17. G. Alvarez, and S. Li, "Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption," Commun Nonlinear Sci Numer Simulat, Vol. 14, pp. 3743-9, Nov. 2009.
18. A. Kanso, and N. Smaoui, "Logistic chaotic maps for binary numbers generations," Chaos, Solitons and Fractals, Vol. 40, pp. 2557-68, 2009.
19. L. Zhang, X. Liao, and X. Wang, "An Image Encryption Approach Based on Chaotic Maps," Chaos, Solitons & Fractals, Vol. 24, pp. 759-65, 2005.
20. G. Alvarez, and S. Li, "Some basic cryptographic requirements for chaos based cryptosystems," Int. J Bifurcation Chaos, Vol. 16, pp. 1-8, 2006.

AUTHORS

Mrinal Kanti Mandal received the B.Sc. degree in Physics (Hons.) from Burdwan University, India in 1998, and the M.Sc. and Ph.D. degrees from the same University in 2000 and 2008 respectively. Since 2003 he has been with the Department of Physics, National Institute of Technology, Durgapur as an Assistant Professor. He has published more than 20 National and International Journal papers and 15 conference papers in proceeding. His research interests include Design of Electronic Circuits & Systems, Nonlinear Dynamics & Chaos, Cryptography and Image Processing. He is a reviewer of IJE, IJPAP, JIIS, etc. He is a life member of IETE, IPS and IAPT. He was selected in the science and Technology chapter of "Marquis Who's Who" in 2010 edition.

E-mail: nitmkm@yahoo.co.in

Gourab Dutta Banik received the B.Sc degree in Physics (Hons.) from University of Calcutta, India in 2008, and the M.Sc degree from National Institute of Technology, Durgapur, 2011 and received INSPIRE FELLOWSHIP from Department of Science and Technology, Govt.of India. He is interested on chaos based secured communication system, cryptography, image processing and optical communication. He is working as a lecturer in Physics in Bidhan Chandra Institution, Durgapur from 2012.

E-mail: g1duttabanik@gmail.com

Debasish Chattopadhyay obtained his M.Sc. degree in Physics in 1997 from the University of Burdwan and received National Scholarship from the Govt. of India in 1997. During 1998-2000, he was an Assistant Teacher in Physical Science in SDC. High School, Somrabazar. During 2000-2001, he joined as lecturer in Physics in Kalna College, Kalna, West Bengal, India. In 2001, he joined as lecturer in M.B.C. Inst. of Eng. & Technology, Burdwan. Since 2002, he is attached to CSST Academy, Chinsurah, West Bengal, India. In 2003, he participated in a research team (COMPASS Expt.) in CERN, Geneva. He is now pursuing Ph.D. in the field of Chaos-based Cryptography in National Institute of Technology, Durgapur, India.

E-mail: debasis_9000@yahoo.co.in

Debashis Nandi received his B.E. degree in electronics and Communication Engineering from R. E. College, Durgapur (University of Burdwan), India, in 1994 and M. Tech. Degree from Burdwan University on Microwave Engineering in 1997. He received his Ph.D degree from IIT, Kharagpur, India on Medical Imaging Technology in 2012. His area of research includes Computer security and cryptography, Secure chaotic communication, Video coding. He has published more than 10 research papers in national and international journals and one patent. He is an Associate Professor in the Department of Information Technology, National Institute of Technology, Durgapur, India.

E-mail: debashisn2@yahoo.co.in

DOI: 10.4103/0256-4602.103173; Paper No. TR 278_11;