Indian Journal of Science and Technology Vol. 4 No. 5 (May 2011) ISSN: 0974- 6846

Symmetric key chaotic image encryption using circle map

D. Chattopadhyay[1], M. K. Mandal[1] and D. Nandi[2]
[1]*Department of Physics, National Institute of Technology, Durgapur, Pin-713209, India*
[2] *Department of IT, National Institute of Technology, Durgapur, Pin-713209, India*
nitmkm@yahoo.co.in

Abstract

The security of information and digital images has become a major issue during the last three decades. A large number of algorithms for data and image encryptions are reported in the literature. However, many of the proposed algorithms are not suitable in the fields of application, because they are cryptographically weak. In the present work, a novel algorithm for encoding digital images by using a circle map with 3 parameters has been proposed. In this article different images are used for testing the validity of the proposed algorithm. The algorithm has increased the strength of security of the image encryption against cipher-text-only, chosen-plaintext and chosen-cipher-text attacks. The analysis of cryptographic strength has also been performed to confirm the fact. The results of several experimental tests, such as, key space analysis, key sensitivity analysis and statistical analysis show that the proposed algorithm for image cryptosystems provides an efficient and secure way for image encryption. A comparison in terms of correlation between the initial and transformed images, number of pixels change rate (NPCR) and unified average changing intensity (UACI) is also done.

Keywords: Circle map, Chaos, Lyapunov exponent, anti-differential attack, NPCR, UACI.

Introduction

In the recent years, the security of digital images in the world of modern telecommunication has become immensely important since communication of digital products over network occur more and more frequently such as ISDN, HDTV, medical imaging, confidential video conferencing, military and defense data-base, mobile computing, personal communication etc. In particular, the field of security has become a current interest of research (Li & Zheng, 2002; Chen *et al.,* 2004; Rhouma & Belghith, 2008; Giesl & Vlcek, 2009; Amin *et al.,* 2010). Many security models and crypto-systems based on number theory and chaotic map have already been proposed (Bourbakis & Alexopoulos, 1992; Alexopoulos *et al.,* 1995; Jan & Tseng, 1996; Ker-Chang & Liu, 1997; Fridrich, 1998; Miyamoto *et al.,* 1999; Dang & Chau, 2000; Cheng & Li, 2000; Yen & Guo, 2000). But it is found that some of them (Bourbakis & Alexopoulos, 1992; Alexopoulos *et al.,* 1995; Ker-Chang & Liu, 1997) are either inefficient or weak in view of computational complexity and strength of security (Jan & Tseng, 1996; Cheng & Li, 2000).

After 1990s, chaotic encryption systems have got tremendous importance for their capability to improve the degree of security. This improvement in the degree of security is due to the fundamental characteristics of chaos, such as ergodicity (the dynamical system, broadly speaking, has the same behaviour averaged over time as averaged over space), mixing property and sensitivity to the initial conditions and parameters. As a consequence, many works have been done in the field of chaos-based cryptography and image encryption as stated in Fridrich (1998) and Kocarev *et al.* (1998). But most of them are not so strong to the different types of attacks, especially to known-plaintext attack. In this paper, a new chaos-based crypto-system that employs circle map for encryption and decryption has been proposed to provide a good resistance against the common attacks. The algorithm employs chaos feedback stream cipher for image encryption and works using an iterative cipher mechanism. The circle map is chosen to obtain the values of chaotic sequence of samples in a large range. The ultimate values of the samples in the sequence have been restricted between 0 and 1 by mod operation. The values of the sequence are converted into the range 0 to 255 unsigned integer gray levels. Then final encrypted image is obtained from pixel-by-pixel XOR operation between plain-image and chaotic sequence.

Characteristics of an image cryptosystem

A good information security system should be able to protect confidential messages in the text form as well as in the image form. In general, there are 3 basic characteristics in the field of security (Ahmed *et al.,* 2006). These are: (i) Privacy: An unauthorized user cannot disclose a message, (ii) Integrity: An unauthorized user cannot change a message anyway, (iii) Availability: Messages are available to the authorized user. Besides these, the security should require the following properties also: (i) The encryption algorithm must require an extremely long computation time to break. (ii). Encryption/decryption should be fast enough and the algorithm should be simple enough. (iii). The security mechanism should be widely acceptable to design a cryptosystem like a commercial product. (iv). The security mechanism should be flexible. (v). There should not be a large expansion of the image data.

Characteristics of the circle map

Chaotic phenomenon is certain and analogous to stochastic process appearing in non-linear dynamical systems. Such a process is non-periodic, non-convergent and extremely sensitive to the initial conditions. Because of this wonderful property of the chaotic systems, these are applied extensively in encryption and decryption of information (Jan & Tseng, 1996; Dang & Chau, 2000; Cheng & Li, 2000; Yen & Guo, 2000). The classical encryption algorithm uses 2 general principles-confusion and diffusion. Diffusion is the spreading out of local information on the entire image i.e. diffusion spreads out the influence of individual plain-text or key bits over as much of the cipher-text as possible. This also hides the statistical relationships and makes cryptanalysis more difficult. The diffusion property is established or guaranteed by chaos because of its extreme sensitivity to initial condition. Confusion serves to hide any relationship between the plain-text, the cipher-text and the key. Good confusion makes the relation statistics so complicated that even powerful cryptographic tools do not work. In chaotic map, two trajectories starting from very close initial states diverge exponentially as the time evolves.

In this paper, we have used the circle map for the purpose of image encryption. This map exhibits chaos for an infinite set of real parameters. Generally, a discrete dynamical chaotic map may be expressed as:

$$\left.\begin{aligned} x_{n+1} &= G(x_n, a) \\ x_{n=0} &= x_0 \end{aligned}\right\} \quad (1)$$

Where *a* is a set of parameters. The map is chaotic for infinitely large range of parameters in which the Lyapunov exponents are positive. The mathematical representation of the circle map used for the purpose of encryption in the present scheme is

$$\left.\begin{aligned} x_{n+1} &= \operatorname{mod}\left[\left\{\left(\sqrt{k_1} + k_2.x_n + \sin\left(2.\pi.k_3.x_n\right)\right\}, 1\right]\right. \\ x_{n=0} &= x_0 \end{aligned}\right\} \quad (2)$$

Which is highly chaotic in large parameters' space. In the present map the set of parameters is given by,

$$a = \left[k_1, k_2, k_3\right]. \quad (3)$$

Lyapunov exponent

In order to characterize the approach or separation of the movement of the track produced by nonlinear mapping, the Lyapunov Exponents are introduced. If *f* be a smooth map of the real line ℝ, the Lyapunov number $L(x_1)$ of the orbit $\{x_1, x_2, x_3, \cdots\}$ is defined as $L(x_1) = \lim_{n\to\infty}\left[\left|f'(x_1)\right|\cdots\left|f'(x_n)\right|\right]^{\frac{1}{n}}$, if this limit exists. Then the Lyapunov exponent is defined by $\Lambda(x_1) = \lim_{n\to\infty}\left(\frac{1}{n}\right)\left[\ln\left|f'(x_1)\right| + \cdots + \ln\left|f'(x_n)\right|\right]$, if this limit exists. If the Lyapunov exponent is positive, the system is chaotic. The plot of Lyapunov exponent (Λ) vs. the parameter (k_1) is shown in fig. 1 which shows a portion of parameters' space for which the Lyapunov exponent is positive (i. e. the map is chaotic). The time series plots of the proposed chaotic map exhibiting the chaotic trajectories are illustrated in fig. 2a and 2b for k_1=1.001, *k*k_2=2.002, k_3=3.003, x_0=0.5 and k_1 =1.001, k_2 =2.002, k_3=3.003, x_0=0.49 respectively.

Encryption and decryption algorithm

In this section, we discuss the step-by-step procedure of the proposed algorithm for encryption processes. 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 $1 \le j \le N$. Basically, $f(i, j)$ denotes the gray levels in the range 0 to 1 at the pixel position (i, j) of an image.

Step1: Transform the $M \times N$ pixels into an array of $P_i = \{P_1, P_2, P_3, \cdots, P_n\}$, ($i = 1, 2, 3, \cdots, n$ and $n = M \times N$). 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 circle map mention in equation (2) with initial condition x_0 and taking the parameters k_1, k_2, k_3. Next convert x_i into unsigned integer in the range of 0 to 255 using mod operation.

Step 3: Generate $C_i' = P_i \oplus x_i$. The sign $\oplus$ indicates bitwise XOR operation. Next consider the steps below to construct C_i.

$p_i = \operatorname{mod}(C_i', x_i).$, $p_i = round\left(p_i * 50\right).$

$C_j = C_j' \oplus p_{j-1}$, here *j* varies from 2 to *n*.

Step 4: Transform $C_i = \{C_1, C_2, C_3, \cdots, C_n\}$ to an $M \times N$ array to get the image f'. To get the final encrypted image after rotation one should follow the following steps starting from $i = 1$ to $i = 256$.

$X_i = \operatorname{mod}\left(x_i, 99\right).$

$X_i = X_i - \operatorname{mod}\left(X_i, 1\right).$

$X_i = 50 - X_i.$

$Y_i = sign(X_i)$

$f' = imrotate\left(f', \left(Y_i * 90\right)\right).$

Save f'.

The function $imrotate\left(I, \varphi\right)$ indicates rotation of image I by an angle φ degree in the direction of counter clock-wise when φ is positive and the direction of rotation will be clock-wise when φ is negative. Now f' is the final encrypted image. The secret keys in this algorithm are

Fig. 1. Lyapunov exponents as a function of K_1; $K_2 = K_3 = 1$

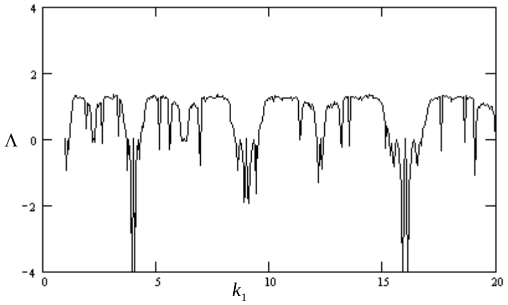


Fig. 3. Application of the encryption/decryption algorithm to the image Lena. (a) Plane image; (b) image encrypted with Key {66.8721, 1.4822, 1.3254, 9.2701}; (c) Decrypted image using same key of encryption; (d) Image decrypted with wrong key {66.8721, 1.4821, 1.3254, 9.2701}.

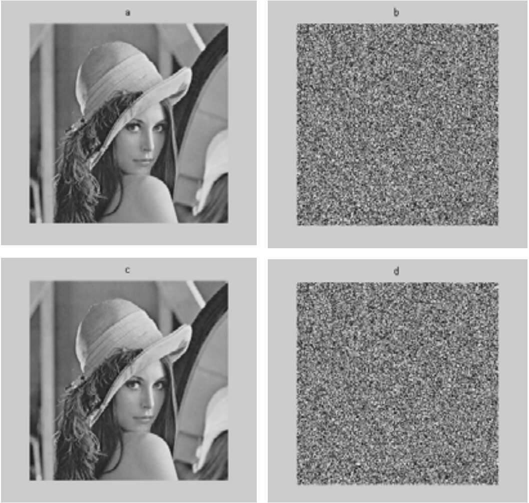


Fig. 4. Application of the encryption/decryption algorithm to the image road. (a) Plane image; (b) mage encrypted with Key {66.8721, 1.4822, 1.3254, 9.2701}; (c) Decrypted image using same key of encryption; (d) Image decrypted with wrong key {66.8721, 1.4822, 1.3253, 9.2701}.

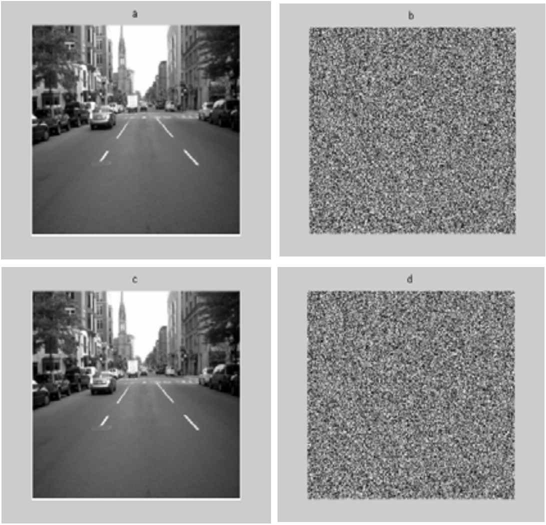


Fig. 2a. Time series of the chaotic map for $x_0 = 0.5$.

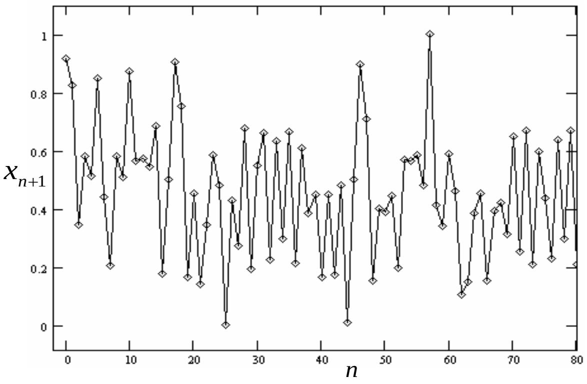


Fig. 2b. Time series of the chaotic map for $x_0 = 0.49$.

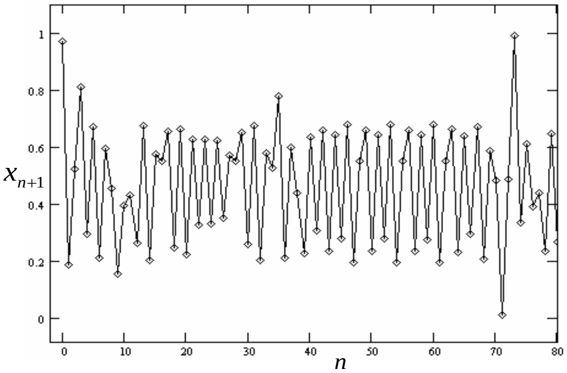
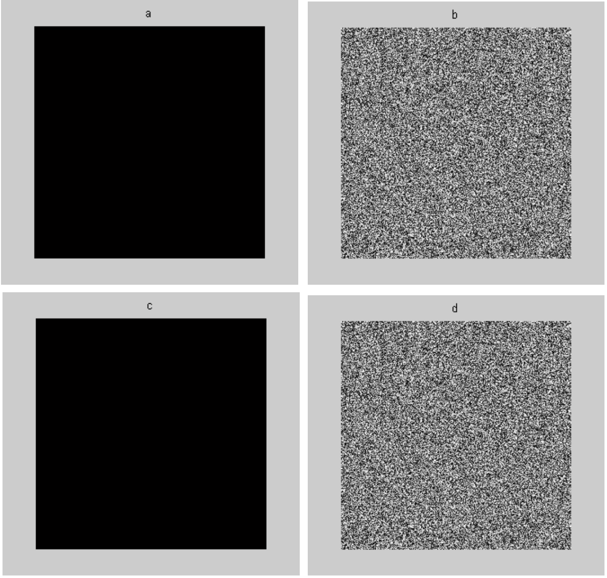


Fig. 5. Application of the encryption/decryption algorithm to the image black. (a) Plane image; (b)Image encrypted with key {66.8721, 1.4822, 1.3254, 9.2701}; (c) Decrypted image using same key of encryption; (d) Image decrypted with wrong key {66.8721, 1.4822, 1.3254, 9.2702}



the initial condition and the map- parameters. A key set for encryption is given in a sequence as $\{x_0, k_1, k_2, k_3\}$. The decryption is the inverse process of encryption.

Experiment results

Experiments are done using different original images plain images to prove the validity of the proposed algorithm. Fig. 3a-5a show 3 different plain images and Fig. 3b-5b show the encrypted images (cipher images) using key {66.8721, 1.4822, 1.3254, 9.2701}. The encrypted images are totally invisible. The decrypted images using the same key are shown in Fig. 3c-5c, where as decrypted images using wrong key (as indicated in the figures) are also shown in Fig. 3d-5d. From these figures it is clear that decrypted images using wrong key will carry no information of the original images.

Security analysis

A good encryption technique should be robust against cryptanalytic, statistical and brute-force attacks. In this section, we discuss the security analysis of the present algorithm such as key space analysis, sensitivity analysis, statistical analysis, complexity analysis and differential analysis to prove the security level of the proposed algorithm against the most common attacks stated in Chen *et al.* (2004) and Mao *et al.* (2004).

Key space & key sensitivity analysis

For the purpose of making the brute-force attack infeasible, the key space should be large enough in a secure image cryptosystem. In this regard fig. 3b-5bobviate the fact that the encrypted image appear to be rambling. The attacker cannot get anything from the cipher images. The key includes $\{x_0, k_1, k_2, k_3\}$ combination and they are real numbers. In this paper, x_0, k_1, k_2, k_3 are of 64 bits. Hence, the proposed circle map based algorithm has (2^{64}×2^{64} ×2^{64} ×2^{64}) = 2^{256} different combinations of the secret keys which is same as the recently reported work in Amin *et al.* (2010). An image cipher with such a long key space is sufficient in the field of reliable practical use. A good image encryption scheme should be sensitive to the secret key. The change of a single bit in the secret key should produce a completely different encrypted/decrypted image. In the proposed cryptosystem, the cipher image cannot be decrypted correctly although the slightly different key as depicted from Fig. 3d-5d. At the time of encryption we have used k_1 = 1.4822 and during wrongly decryption we have used k_1 = 1.4821 for the plain images fig. 3a-5a. The difference value is $|k_1 - k_1| = 0.0001$ which produced decrypted images totally different from the original plain images. This analysis proved that the algorithm of the cryptosystem is sensitive to the key and it guarantees the security against known plain-text attacks also.

Complexity analysis

Cryptanalysis of CKBA image encryption algorithm is done by Li & Zheng (2002). It was proved that the security of the CKBA (Yen & Guo, 2000) was over-estimated and an improvement of CKBA has been done by the authors Li & Zheng (2002). They have also estimated complexity for cipher text-only attack was approximately $2^{123.16}$ for 512×512 image. But again this algorithm is also weak to the known-plaintext and chosen-plaintext attack because the keys can be extracted from the mask image or by searching procedure described in Li and Zheng (2002) and the estimated complexity is O(M×N). In the present algorithm, it is difficult to extract the keys from the mask-image by using the above-mentioned searching procedure, because in this algorithm M×N number of chaotic sequences are used in XOR operations after mod operation. Generally, the key values are determined by known plain-text attack if the sequence generated by the map is known. But in this algorithm, the mod operation is done after generating the sequence to resist knowing the actual sequence generated by the map. Because the mod operation restricts the values of the sequence between 0 and 1 whatever larger (finite) the values of the sequence may be. Therefore, the mod operation does not provide any information about the keys used in the map and hence, it is not possible to extract the keys from the sequence obtained by known plain-text attack. The approximate average brute force cipher text-only attack complexity can be estimated as follows: For each guessed key $\{x_0, k_1, k_2, k_3\}$, the number of computations required for generating the chaotic sequence is MN. Consequently, The average brute force attack complexity for cipher text-only attack is, $\frac{1}{2}[(2^{4n-1})MN] \approx 2^{4n-1}MN$. For 256×256 image and three 64-bit keys, the complexity is $2^{4\times 64-1} \times 256 \times 256 = 2^{271}$ which is larger than 2^{128} as recommended in Li & Zheng (2002).

Statistical analysis

An ideal cryptosystem should be resistive against any statistical attack (Ahmed *et al.,* 2006). To prove the robustness of our algorithm, we have performed statistical analysis by calculating the histograms and the correlations of two adjacent pixels in the plain image as well as in the cipher image.

Histogram analysis

To prevent the leakage of information, it is necessary for the cipher image to bear no statistical similarity to the plain image. An image-histogram describes how the image-pixels are distributed by plotting the number of pixels at each intensity level. The histograms present the statistical characteristics of an image. If the histograms of the encrypted image are similar to the random image, the encryption algorithm has good performance. An attacker finds it difficult to extract the pixels statistical nature of the plain image from the cipher image and the algorithm can resist a chosen plain text or known plain text attacks. Histograms reveal the fact that the random numbers

Fig. 6. Histogram of Lena image.
(a) Histogram of plane image;
(b) Histogram of encrypted Lena image.

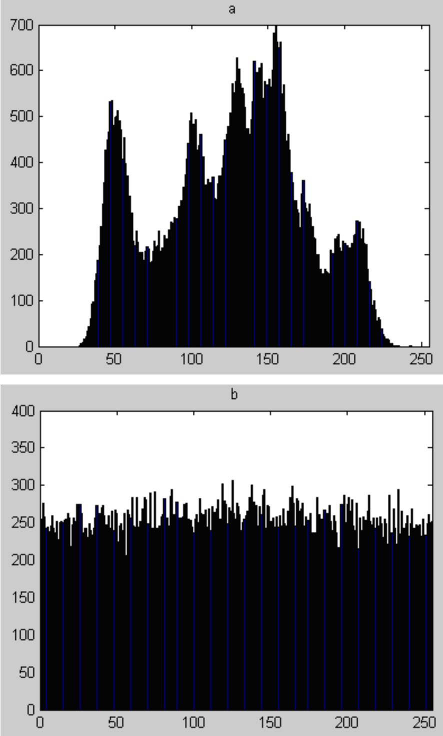


Fig. 10. The correlation analysis of two vertically adjacent pixels of Lena.bmp
(a) plane image; (b) Encrypted image.

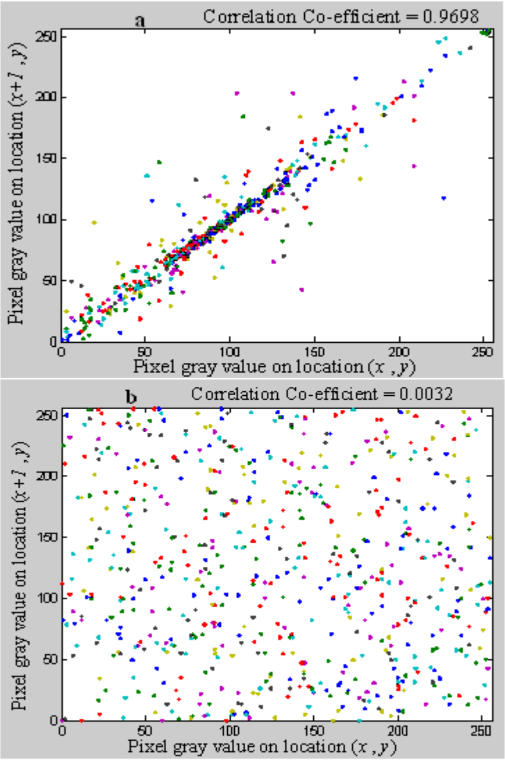


Fig. 7. Histogram of road image
(a) Histogram of plane image;
(b) Histogram of encrypted road image.

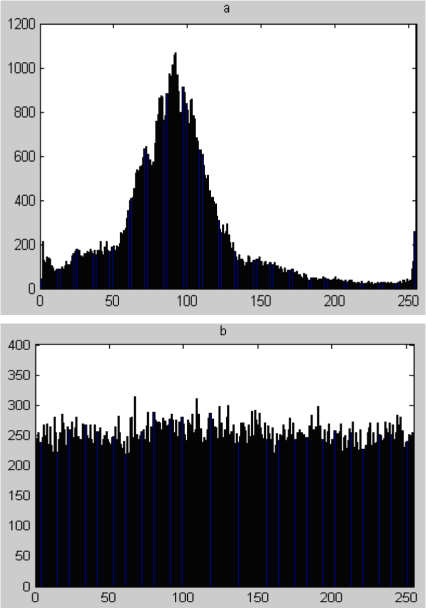


Fig. 8. Histogram of black image
(a) Histogram of plane image;
(b) Histogram of encrypted black image.

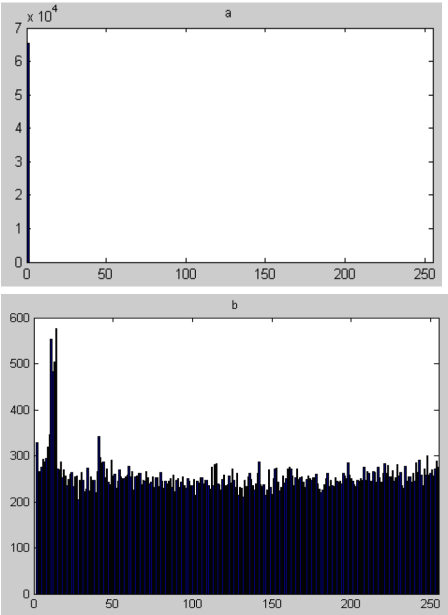
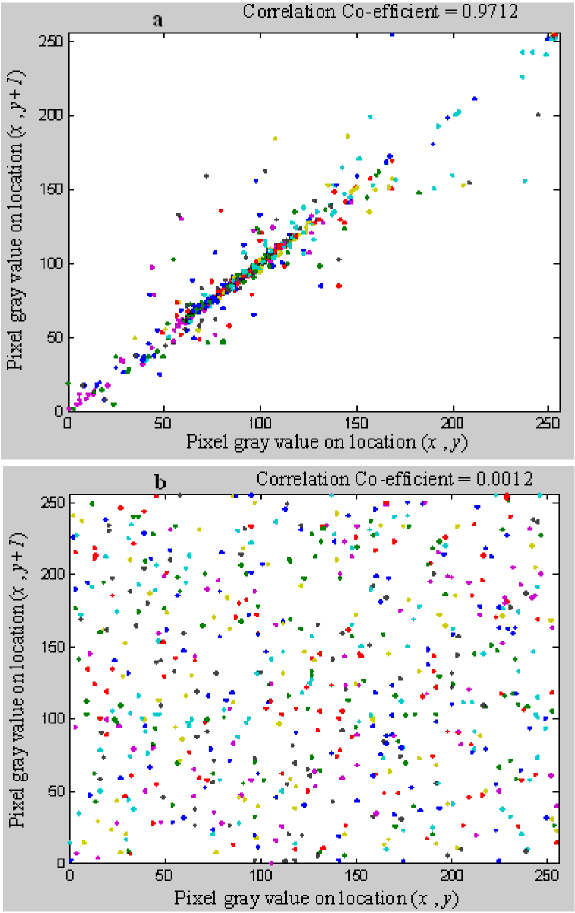


Fig. 9. The correlation analysis of two horizontally adjacent pixels of Lena.bmp
(a) Plane image; (b) Encrypted image.



generated from the chaotic map are uniformly distributed like white-noise. We have shown and analyzed the histograms of the encrypted images along with the original image that have widely different contents.

Fig. 6a, 7a and 8a represent the histograms of the plane images Lena.bmp, Road.bmp and Black.bmp respectively. These histograms show large spikes, which correspond to the gray values that appear more often in the plain-images. Fig. 6b, 7a and 8b show the histograms of the encrypted images of Lena.bmp, Road.bmp and Black.bmp respectively for the keys {66.8721, 1.4822, 1.3254, 9.2701}. Here all the spikes are almost uniformly distributed and significantly different from those of the original images and therefore bear no statistical resemblance to the plain-image and hence do not provide any clue to employ any statistical attack on the proposed image encryption technique.

Correlation co-efficient analysis

In addition to the histogram analysis we have also studied the correlation between two horizontally adjacent pixels, two vertically adjacent pixels and two diagonally adjacent pixels of the plane images and the encrypted images. In case of plane image each pixel is usually highly correlated with its adjacent pixels either in horizontal, vertical or diagonal directions but for encrypted image these correlation will be very small. The correlation co-efficient ρ can be calculated by using the following formulas given by Chen *et al.* (2004):

$$E(x)=\frac{1}{P}\sum_{i=1}^{P}x_i$$

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

$$\mathrm{cov}(x,y)=\frac{1}{P}\sum_{i=1}^{P}(x_i-E(x))(y_i-E(y))$$

$$\rho=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \qquad (4)$$

Where *x* and *y* are the values of two adjacent pixels of the plane images or ciphered images. To calculate correlation coefficient we have selected 1000 pairs of two adjacent pixels from both the images (i) plane image and (ii) ciphered image of Lena.bmp. According to eqn. 4 the correlation coefficient of the plane image of Lena is 0.9712 and its ciphered image is 0.0012 along the horizontal direction. Similar results for vertical and diagonal direction are also obtained and shown in Table 1. The correlation distribution of two horizontally adjacent pixels and two vertically adjacent pixels of the image Lena.bmp are shown in Fig. 9 and Fig. 10 respectively.

We have also studied the correlation coefficient between (i) plane image and encrypted image, (ii) plane image and decrypted image to test their similarity. The larger correlation value implies the best match between the two images. This means that if the correlation coefficient of the initial image and the decrypted image is large, there is maximum similarity between two images. Here we have selected 1000 pairs of pixels from two images one is plane image and other one is ciphered image or decrypted image. Table 2 shows the correlation coefficient between the plane image and the ciphered image and plane image and the decrypted image with same key and slightly different key values.

The above diagrams and the correlation coefficients of the adjacent pixels of the ciphered image obviate that the proposed algorithm has a good ability of diffusion and confusion and highly resistive against the statistical attack (Fei *et al.,* 2005).

Information entropy analysis

To analyze the robustness of the encryption algorithm, the concept of entropy (Amin *et al.,* 2010) is also introduced here as given below.

$$H(m)=\sum_i p(m_i)\log_2\frac{1}{p(m_i)}. \quad (5)$$

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 equation (5) entropy of the system will be $H(m)=8$. 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.

Differential attack analysis

Two criteria NPCR and UACI are used to test the sensitive of a single bit change the plain-image. Number of pixels change rate (NPCR) denotes the percentage of different pixel numbers between two encrypted images, whose plain images have only one pixel difference. Unified average changing intensity (UACI) denotes the average intensity of differences between 2 cipher images, whose corresponding plain images have only one pixel difference. Consider 2 ciphered images C_1 and C_2, whose corresponding plain-images have only one pixel difference. Let the gray-scale values of the pixels at position (*i,j*) are $C_1(i,j)$ and $C_2(i,j)$ of the two ciphered images C_1 and C_2 respectively. Define a bipolar array *D* with the same size as C_1 and C_2. Then *D*(*i,j*) is determined by the conditions: if $C_1(i,j)=C_2(i,j)$, then $D(i,j)=1$; otherwise, $D(i,j)=0$. NPCR and UACI are defined through the equations (6) and (7) respectively.

$$NPCR=\frac{\sum_{i,j}D(i,j)}{M\times N}\times 100\% \quad (6)$$

$$UACI = \frac{1}{M \times N}\left[\sum\nolimits_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \quad (7)$$

Experimentally measured value of NPCR is 99.63% and UACI is 33% for Road image. This result indicates that small change in plain image creates significant changes in the ciphered images, so the proposed algorithm is highly resistive against differential attack.

Table 1. Correlation coefficient of plane image & ciphered image of Lena.

Direction of adjacent pixels	Correlation coefficient of 2 adjacent pixels	
	Plain-image	Ciphered image using key {66.8721, 1.4822, 1.3254, 9.2701}
Horizontal	0.9712	0.0012
Vertical	0.9698	0.0032
Diagonal	0.9861	0.0058

Table 2. Correlation coefficient between 2 images.

Image	Image type & key	Correlation coefficient
Lena	Plane & ciphered image {66.8721, 1.4822, 1.3254, 9.2701}	0.0052
	Plane & decrypted image {66.8721, 1.4822, 1.3254, 9.2701}	1.0000
	Plane & decrypted image {66.8721, 1.4821, 1.3254, 9.2701}	0.0023
Road	Plane & ciphered image {66.8721, 1.4822, 1.3254, 9.2701}	0.0039
	Plane & decrypted image {66.8721, 1.4822, 1.3254, 9.2701}	1.0000
	Plane & decrypted image {66.8721, 1.4822, 1.3253, 9.2701}	0.0078

Table 3. Entropy analysis of plane images & ciphered images.

Image	Plain-image	Ciphered image using key {66.8721,1.4822, 1.3254, 9.2701}
Lena	7.4312	7.9878
Road	7.1327	7.9886
Black	0.0000	7.9963

Conclusion

A chaos-based encryption algorithm for image encryption and decryption using circle map has been proposed and discussed. Two different XOR operation and rotation of the image are used to confuse the pixel value and shuffle the pixel position. Key space analysis, key sensitivity analysis, statistical analysis, information entropy analysis and differential analysis are discussed to prove the good performance of the proposed algorithm.

References

1. Ahmed HEH, Kalash HM and Allah OSF (2006) An efficient Chaos-based feedback stream cipher (ECBFSC) for image encryption. *SITIS*. pp110-121.
2. Alexopoulos C, Bourbakis NG and Ioannou N (1995) Image encryption method using a class of fractals. *J. Elec. Imaging*. 4, 251-259.
3. Álvarez G, Montoya F, Romera M and Pastor G (2000) Cryptanalysis of chaotic encryption system. *Phys. Lett. A*. 306, 191-196.
4. Álvarez G, Montoya F, Romera M and Pastor G (2004) Breaking parameter modulated chaotic secure communication. *Chaos Solitons Fractals*. 21, 783-787.
5. Amin M, Faragallah OS and El-Latif AA (2010) A chaotic block cipher algorithm for image cryptosystems. *Commun. Nonlinear Sci. Numer. Simulat*. 15, 3484-3497.
6. Bourbakis N and Alexopoulos C (1992) Picture data encryption using scan patterns. *Pattern Recog*. 25, 567-581.
7. Chen G, Mao Y, and Chui CK (2004) A symmetric image encryption based on 3D chaotic maps. *Chaos Solitions Fractals*. 21, 749-761.
8. Cheng H and Li X (2000) Partial encryption of compressed images and videos. *IEEE Trans. Signal proc*. 48, 2439-2451.
9. Dang PP and Chau PM (2000) Image encryption for secure internet multimedia applications. *IEEE trans. consumer elec*. 46, 395-403.
10. Fei P, Qiu SS and Min L (2005) An image encryption algorithm based on mixed chaotic dynamic systems and external keys. *IEEE int. conf. commun. circuits & systems*. pp:1135-1139.
11. Fridrich j (1998) Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurcation Chaos*. 8, 1259-1284.
12. Giesl J and Vlcek K (2009) Image encryption based on strange attractor. *ICGST-GVIP J*. 9, 19-26.
13. Jan JK and Tseng YM (1996) On the security of image encryption method. *Information Proc. Letts*. 60, 261-265.
14. Ker-Chang H and Liu JL (1997) A linear quadtree compression scheme for image encryption. *Signal Proc. Image Commun*. 10, 279-290.
15. Kocarev L, Jakimoski G, Stojanovski T and Parlitz U (1998) From chaotic maps to encryption schemes. *Proc. IEEE int. symposium circuits & systems.* 4, 514-517.
16. Li S and Zheng X (2002) Cryptanalysis of a Chaotic image encryption method. *Proc. IEEE int. conf. circuits & systems.* 2, 708-711.
17. Mao Y, Chen G and Chui CK (2004) A novel fast image encryption scheme based on 3D chaotic Baker maps. *Int. J. Bifurcation Chaos*. 14, 3613-3624.
18. Miyamoto M, Tanaka K and Sugimura T (1999) Truncated Baker transformation and its extension to image encryption. *Proc. SPIE*. 3814, 13-25.
19. Rhouma R and Belghith S (2008) Cryptanalysis of a new image encryption algorithm based on hyper-chaos. *Phys. Letts. A*. 372, 5973-5978.
20. Yen JC and Guo JI (2000) A new chaotic key-based design for image encryption decryption. *Proc. IEEE Int. Conf. Circuits Systems*. 4, 49-52.