ISSN:2320-0790

An International Journal of Advanced Computer Technology

A new cryptographic scheme with modified diffusion for digital images

Nidhi Sethi, Sandip Vijay
DIT University, Dehradun-248001

Abstract: In this paper, a new image block cipher encryption strategy for gray scale images using a different set of secret key and sizes is proposed. Initially, the swapping and dispersion is done without keys and in second stage the image is mixed with the chirikov map involving first secret key. 'N' rounds are taken to complete this process. The blended image is divided into blocks of block size 8X8.These blocks are also swapped to achieve good confusion. For making the encryption scheme more sturdy in each block the transmutation of pixels is done with the modified logistic map having three more secret keys. The proposed scheme is simple, rapid and sensitive to the secret key. Due to the high order of substitution, common attacks such as linear and differential cryptanalysis are unattainable. The experimental results show that the proposed encryption technique is effective and has high security features.

Keywords: symmetric encryption, modified logistic map, chirikov map, differential cryptanalysis, image encryption.

1. INTRODUCTION

Recently, with the high demand in digital signal transmission and big losses due to illegal data access, data security has become a critical and imperative issue. Encryption is being used to secure data and prevent them from unauthorized access. Due to certain characteristics of digital images- redundancy of data, strong correlation among adjacent pixel, less sensitive as compare to the text data, especially the bulk quantity of data and the requirement of real-time processing, traditional ciphers such as DES, AES, RSA etc. are not suitable for image encryption. In order to protect digital images from unauthorized users doing illegal reproduction and modifications, a variety of image encryption schemes have been proposed.

The various ideas used in the existing image encryption techniques can be classified into three major types: pixel shuffling [5,10,18,19], pixel transmutation [1,2,7,17] and the combination form [6,8,12,13,15]. The shuffling algorithms interchange the position of pixels within the image itself and usually have low security. While the transmutation process transforms the original values of image into transmuted values .This process has low hardware expense and estimating complications. In the hybrid form the combination of both transmutation and shuffling is used and has good potential for security. In the last decade many encryption schemes have been proposed to improve over security constraints in case of images. . In the following paragraph some recent image encryption schemes are discussed in crisp.

2. LITREATURE REVIEW

The conventional encryption scheme such as DES, T-DES, AES are not suitable to construct the cryptosystem for digital images . The reason behind this difficulty is inherent features of the images and high redundancy. Chengqing Li et al. [3] , have reviewed four chaos based image encryption schemes. He concluded that all lie under one umbrella and is composed of two basic techniques: permutation and combination of pixel value. But in general all methods have security problems like insensitivity to change of plain-image, insensitivity to change of secret key , insecure diffusion function and the schemes can be broken with no more than $[\log_l(MN)+3]$ chosen images when iteration number is equal to one, where MN is dimension of image. Chong Fu et.al [4] have used , Chirikov standard map , to decor relate the strong relationship among adjacent pixels hence employed to shuffle the pixel positions of the plain image. After the decor relating the pixels, the pixel values are modified sequentially to confuse the relationship between cipher image and plain image.
J. M. Blackedge et al. [11] have proposed a multilevel blocks scrambling scheme which is employed to scramble the blocks of coefficients which requires high computation. The control parameters of the scrambling are randomly generated from the secret key dependent. The key stream used to encrypt the scrambled image is extracted from the chaotic map and plain image.
W Puech et al. [14] have studied the various combination of chaotic maps based symmetric key cryptosystems like Logistic, Henon , Tent , Cubic and Cheyshev . He explained and reviewed the

security, performance and reliability issues, of mappings.

3. PROPOSED WORK

The proposed work comprises of image encryption algorithm which is broadly divided into two phases. The first phase of the algorithm consists of swapping and dispersion .Theses two processes do not involve any key. These processes are only integrated to increase the confusion, diffusion and non linearity, but they themselves do not provide any security because of the absence of the key. The second phase consists of the shuffling by Chirikov Standard map and mixing by modified logistic map. The control parameters of Chirikov map and modified logistic map are the control parameters of diffusion and confusion respectively. These control parameters and number of iterations is treated as secret keys.

The choice of chirikov map is made because after 'n' iterations the pixel at the corner most position or origin remain unchanged whereas in other maps the origin and some other pixel like (N,N) or (N-1,N-1) also remains same. The modified logistic map is chosen because inspite of its simple equation it provides complex dynamic chaos.

3.1 Steps of Proposed Algorithm

(I) *Selection of keys :*

S.No	Key Description	Key Value
1	Key 1-Chirikov map iteration	15
2	Key2-Chirikov map control parameter (dimensionless)	512
3	Key 3	67
4	Key 4	0.3628
5	Key 5	3.9898

(II) *First Phase(Without key)*

Step 1: Consider an image I (W x H) such that W and H are the width and height of I. Split the image I to a set of N vectors of length L (L=64 in this work)[9].

Step 2: Calculate the value of O1 and O2

$$O_1 = \sum_{i=1}^{W-1} \sum_{j=1}^{H-1} \frac{-1^{i+j}\, I(i,j)}{256L}$$

$$O_2 = \sum_{i=1}^{W-1} \sum_{j=1}^{H-1} \frac{-1^{i+j+1}\, I(i,j)}{256L}$$

Step 3: Set $x = O_1$ and $y = O_2$

For i = 0…..N-1, set the following information for each vector V_i from the set of N vectors .
Swapping Index= x, Swapping Iteration =V(x)
Dispersing Index=y, Dispersing Iteration=V(y)

$$x = x + 1,\ y = y + 1$$

Condition applied: If (x or y) >= L, set them treat them as zero

Step 4: Set the swapping index of the Vector V_i as a new start value from 0 to L-1. For j from 0 to swapping iteration of vector V_i, swap the values from 0 to L-1, depending upon the conditions mentioned in the method.

Step 5: Set Dispersion index of vectors V_i as a new start value of random number generation algorithm, which would be treated as initial condition parameter. For j from 0 to dispersion iteration of vector V_i, generate random number $N_1$with the values between (0 to L-1) , then perform $V_i(N_i)= V_i(N_i)+ \text{mod } V_i(N_i,100)$.

(III) *Second Phase (With key)*

Step 5: Apply the Chirikov Mapping for 'n' iterations where n=15 over the whole image .The initial parameter is K=512 used is key.

Step 6: Divide the whole image $I_1(x_1,y_1)$ into 8x8 size blocks, B1, B2, . . ., B_{nob} where nob= $I_1(x_1,y_1)$/8X8.Perform shuffling among the blocks.

Step 7: Create a matrix LM(x,y) . Convert each decimal gray value to its binary equivalent of the shuffled image LM(x,y). Also create another matrix DMj is the 8- bit binary number obtained from 1D modified Logistic map.

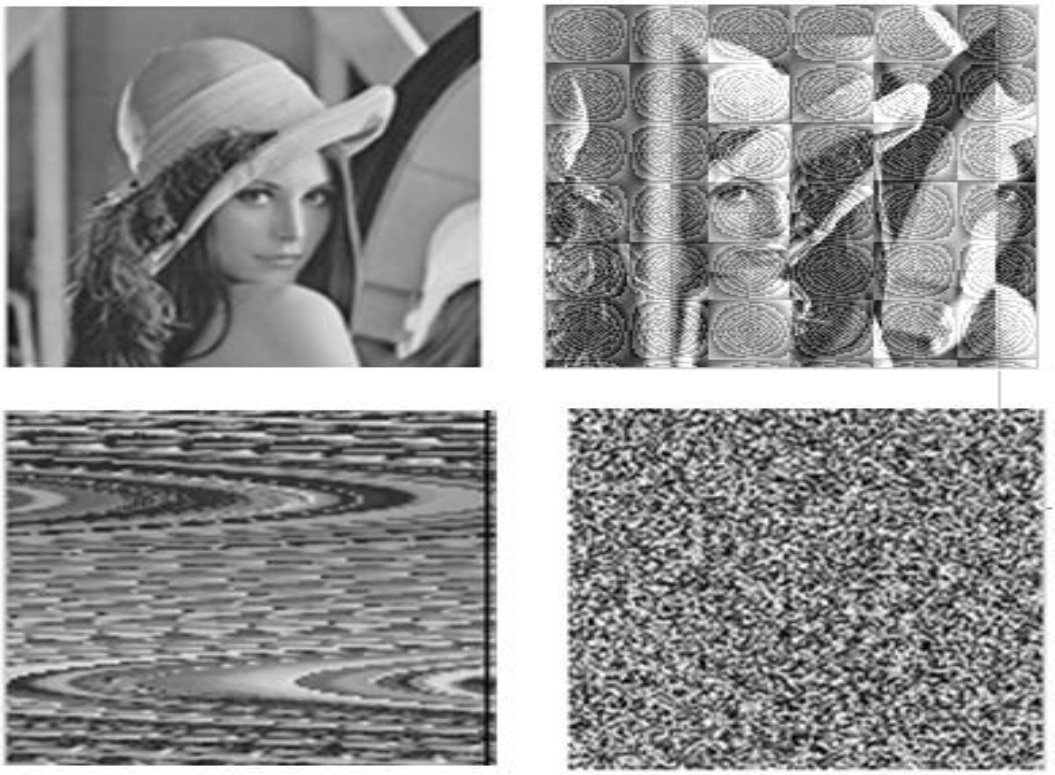
Step 8: Perform exclusive-OR between DM_j and SM(x,y) to obtain the encrypted image EN(x,y).

Decryption: By using all the processes in reverse order, the original image can be retrieved with satisfactory security level, less computational complexity and hence fast, which proves to be a good candidate for real-time secure image transmission.

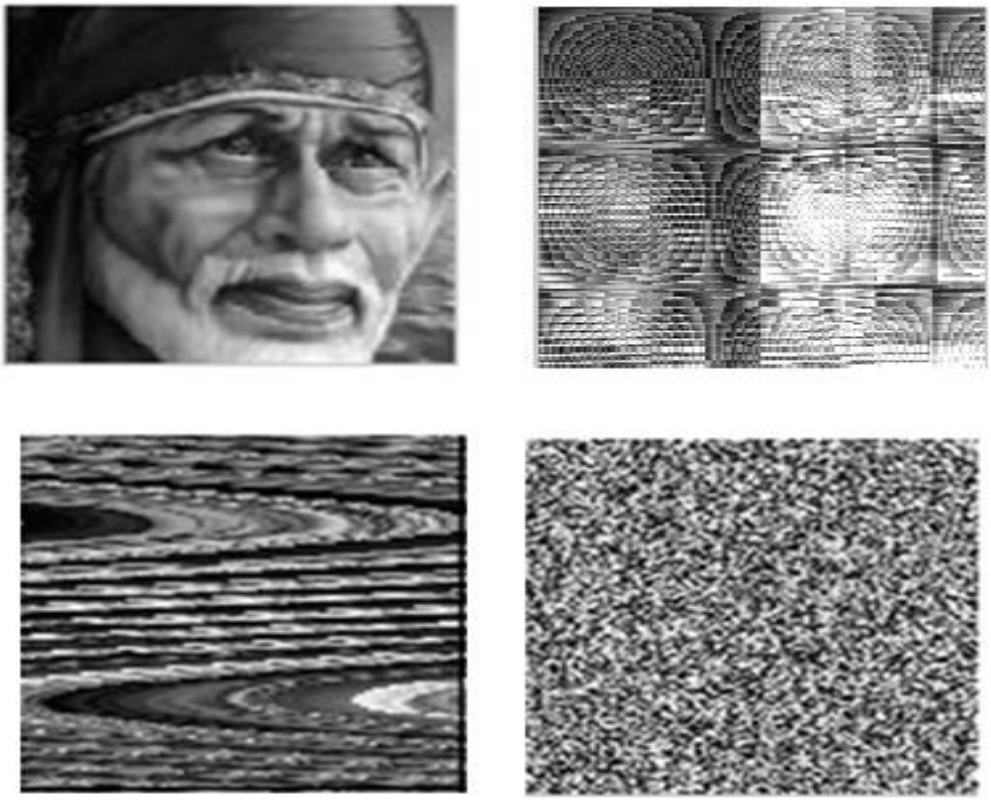
4. RESULTS AND DISCUSSION

The proposed encryption algorithm is implemented in MATLAB 7 for computer simulations. The standard a gray-scale "Lena" image of 128x128 in size and "Baba" image of 128 X 128 in size is taken for experimental purposes. The original Lena image, intermediate image and its histogram are shown in figure 2(a)-(b). The initial conditions and system parameters are: n=15, K= 512, $\lambda = 0.39898$, z(0)= 0.3628.

4.1 Experimental Results



(a)



(b)

Figure2: (a) Lena image original image, swapped & dispersed image, encrypted image (b) Baba image original image, swapped & dispersed image, encrypted image

4.1.1 Key Analysis:

i) Sensitivity of the keys: Almost all chaotic maps are sensitive to secret keys which means the initial parameter. The proposed encryption algorithm is receptive to any small difference to initial parameter. Any change to the power of 10^{-14} in one of these parameter will result into entirely different.

ii) Key Space: It is said in security that more is number of locks better is the safety .In the proposed algorithm there are a total five initial parameters: two of Chirikov map and three of modified logistics map .

4.1.2 Statistical Analysis:

Many attacks can be done which are based on the statistical analysis .Statistical analysis has been performed on the test images to demonstrate the bad correlation among the pixels of the encrypted images.The results shown below shows that there is negligible correlation between pixels of the encrypted image in comparison to original image.

i) Correlation Coefficient Analysis: To estimate the encryption quality of the proposed encryption algorithm , the correlation is used .For highly correlated image the correlation coefficients are almost 1 and for encrypted images the correlation coefficients is almost 0**.**

ii) **Entropy**: Entropy is defined as the degree of randomness in the system. It is known that the entropy $H(m)$ of a message source m can be calculated as:

$$H(s)=-SUM(p(s_i)\log_2 p(s_i))$$

4.1.3 Differntial Attack

Differential attack /cryptanalysis is a common name of attacks/cryptanalysis which is generally done to block ciphers which are working on binary sequences. In this type of attack the dependency of cipher image and input image is analyzed.

i) NPCR: NPCR is Number of pixel change rate. NPCR concentrates on the absolute number of pixels which changes value in differential attacks.The formula and the respective condition is given in eq.(5) & (6)[20];

$$D(i,j) = \begin{cases} 0 & C1(i,j)=C2(i,j) \\ 1 & \text{if } C1(i,j)=C2(i,j) \quad \ldots\ldots\ldots\ldots (5) \end{cases}$$

$$NPCR=\frac{\sum_{i,j} D(i,j) \times 100\ \%}{T} \quad \ldots.(6)$$

Here symbol T denotes the total number pixels in the cipher image. Table I shows the values of NPCR during experimentation .If the value of NPCR is near 0.99, it is treated as good.

Table: Results of Encryption Scheme

	Baba	Lena
Entropy(Encryption)	7.9866	7.9880
Correlation Coef.	0.0013	0.0054
NPCR	0.9912	0.9923
UACI	0.0149	0.0159

4.1.4 Histogram Analysis

The histograms of enciphered images were analyzed and it was found that the histograms are usually uniform. This property makes statistical attacks difficult in images .The test on lena and baba image is shown below:

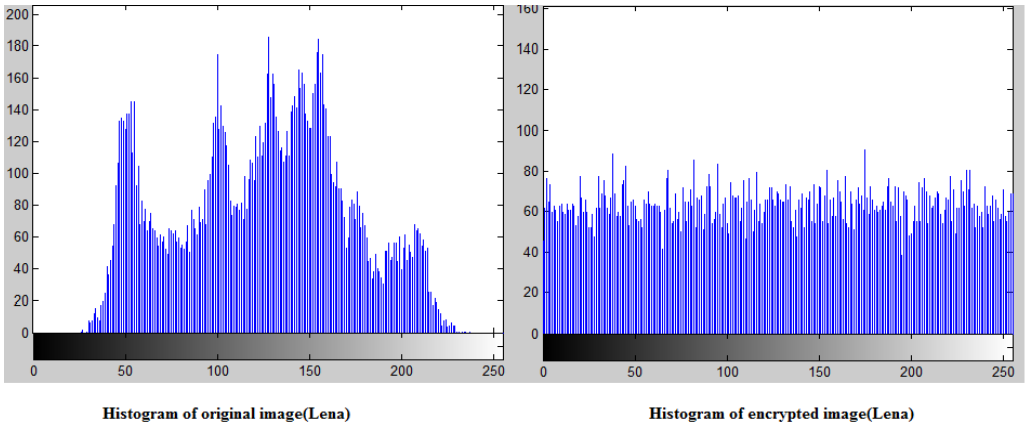


Figure 3: Histogram of original and encrypted image(Lena)

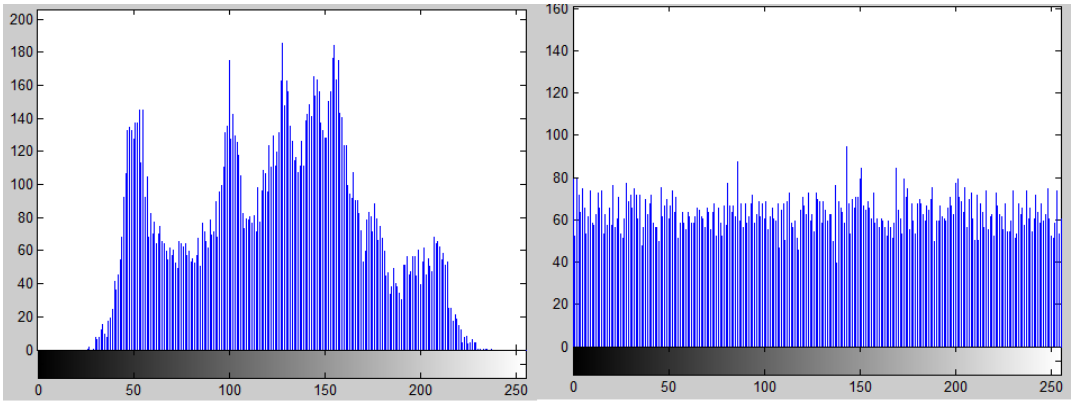


Figure 4: Histogram of original and encrypted image(Baba)

5. CONCLUSION

In the history the Chaotic theory have proven to be a very good candidate for encryption .The symmetric encryption schemes based on chaos theory have qualities like fast processing speed, simple, high sensitivity to keys and secure. In the proposed algorithm two chaotic maps are used Chirikov map and modified logistic map. To make the algorithm robust the image is scrambled and permuted without using key. Both security analysis and key analysis shows that the algorithm is resistant to many attacks like brute force attack, man in middle attack, plain text attack and chosen cipher attack. There are trade-offs between issues such as speed, cost, and complexity.

REFERENCES

[1] Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. A novel algorithm for image encryption based onmixture of chaotic maps. C, Sols and Fra 2008; 35: 408-419.

[2]Chen, Dongming, & Chang, Yunpeng . A novel image encryption algorithm based on logistic maps. A Inf Sci Ser S, 2011;3(7): 364-372.

[3]Chengqing Li, On the security of a class of Image Encryption Scheme, IEEE International Symposium on Circuit & System, Department of Electronics Engineering, University of Hong Kong. 2008; 3290-3293,.

[4]Chong Fu, Jun-jie Chen,Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen Yu, A chaos-based digital image encryption scheme with an improved diffusion strategy. OSA OPTICS EXPRESS. 2012 ; 2363.

[5] Gao, T., & Chen, Z.. Image encryption based on a new total shuffling algorithm. C, Sol and Fra 2008; 38: 213-220.

[6] Indrakanti, S.P., & Avadhani, P.S. Permutation based image encryption technique. Int. J of Comr App. 2011; 28(8): 45-47.

[7] Ismail, Amr Ismail, Mohammed, Amin, & Diab, Hossam. A digital image encryption algorithm based a composition of two chaotic logistic map. Int J Network Sec.2010;11(1),1-10.

[8] Jolfaei, Alireza, & Mirghadri, Abdolrasoul. Image encryption using chaos and block cipher. Com and Inf Sci. 2011;4(1):172-185.

[9] Sethi N., Krishna R., Arora R.P., "Image Encryption Using pixel transmutation and Transition in MATLAB" In: 5th International Multi-Conference on Intelligent Systems, Sustainable , New and Renewable Energy Technology & Nanotechnology (IISN-2011) at IST , Kalawad , Haryana from 18 Feb 2011

[10] Nayak, C.K., Acharya, A.K., & Das, Satyabrata. Image encryption using an enhanced block based transformation algorithm. Int J of Res and Review in Compr Sci. 2011; 2(2): 275-279.

[11] Jonathan M . Blackedge, Musheer Ahmed ,Omar Farooq "Chaotic image encryption algorithm based on frequency domain scrambling" ,School of Electrical Engineering systems Articles, Dublin Institute of Technology,2006;

[12] Pareek, N.K., Patidar, Vinod, & Sud, K.K. Image encryption using chaotic logistic map. Img and V Computing. 2006;24: 926-934.

[13] Patidar, Vinod, Pareek, N.K., & Sud, K.K. Modified substitution–diffusion image cipher using chaotic standard and logistic maps. Communication in Nonlinear Science and Numerical Simulation, 2010; 15: 2755-2765.

[14]Puech, W. and Rodrigues, J. M. A New Crypto- Watermarking Method for Medical Images Safe Transfer. In The 12th European Signal Processing Conference, 2004 ; Vienna , Austria pp: 1481-1484,

[15] Sathishkumar, G.A., & Bagan, K. Bhoopathy. A novel image encryption algorithm using pixel shuffling Base 64 encoding based chaotic block cipher. WSEAS Trans. on Computers, 2011;10(6): 169-178.

[16] Shannon, C.E. Communication theory of secrecy systems, Bell Systems Technical J.1940; 28: 656-715.

[17] Tong, X., Cui, M. Image encryption with compound chaotic sequence cipher shifting dynamically, Img and V Computing 2008; 26: 843-850.

[18] Yoon, Ji W., Kim, Hyoungshick. An image encryption scheme with a pseudorandom permutation based on chaotic maps. Comm. in Nonlinear Sci. and Numerical Sim.2010;01: 041.

[19] Younes, M.A.B., & Jantan, A. An image encryption approach using a combination of permutation technique followed by encryption. Int J of Comp Sci and Network Sec. 2008; 8: 191-197

[20]Yue, Wu, Joseph, P. Noonan, A.Sos. NPCR and UACI randomness tests for image encryption. J of Selected Areas in Telecomm 2011; 31-38.

[21] Sethi N., Vijay S., "A Hybrid Cryptosystem For Image Using Chaotic Mapping" Int J of Com Sci and Business Informatics (IJCSBI), 2013; Vol 5, No.1,2013.

[22] Sethi N., "A New Image Encryption Method Using Chirikov Map and Logistic Mapping", Int J of Computer Apps 2012;0975 – 8887:Vol 59-No. 3 .