



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

An Efficient Chaotic Image Encryption Algorithm Resistant to Attacks

Anchal Jain¹ and Navin Rajpal²

¹Research Scholar, ²Professor

USICT, Guru Gobind Singh Inderprastha University

Delhi, India

Abstract: Large numbers of image encryption algorithms using chaotic maps have been suggested in literature. Chaotic maps are widely being used due to their features of pseudo randomness and sensitivity to change in initial input conditions. In this paper, logistic chaotic maps based image encryption technique is proposed. An external key is used to generate the initial conditions for chaotic maps used and then various operations for encryption are applied based on chaotic values. The key is also changed after regular intervals to improve the security of overall algorithm. The proposed algorithm is evaluated in terms of resistance to various attacks such as statistical attacks using histogram analysis and correlation analysis, key sensitivity, key space analysis and entropy analysis. The proposed algorithm is also evaluated for its robustness against noise and data loss. The results show that the proposed algorithm provides an effective and secure way for image encryption.

Key words: chaotic map, encryption, attacks

I. Introduction

In recent decades, the rapid growth of multimedia based applications and network technology has encouraged the wide use and transmission of digital images and videos over internet and other transmission media and therefore security of these applications is a big concern. It is required to have fast, reliable and secure methods for transmission of such content. Conventional algorithms like RSA, DES, AES etc. are not suitable for multimedia based encryption as they require large computation. Thus, there is always the demand of more suitable encryption techniques. Chaos is one such paradigm that seems to be promising as these techniques have high sensitivity to the initial conditions i.e. a tiny change in the initial conditions results very different output. Further, they are non-linear, fast and deterministic in nature. A number of chaotic map based image encryption algorithms [1,2,3,4] have been suggested in literature. Authors in [5,6] generalized two dimensional chaotic maps to three dimensional to propose more secure encryption techniques. Pareek, Patidar et.al [7] also proposed image encryption technique using two chaotic logistic maps and applied different operations for encryption to the pixels of input image based on the chaotic value. Chaos is also used in neural network. Authors in [8] used chaos based neural network for image encryption in which weights and biases of the network were computed using chaotic map. Wang, Wong et. al in [9] used the chaos to bring confusion and diffusion in the encryption method. Image was divided into non overlapping blocks and then pixels within block and blocks are shuffled randomly using chaotic values. Authors in [10] suggested overlapping blocks based image encryption technique to increase the confusion and diffusion. In paper [11], an encryption method based on skew tent map and a substitution box is proposed. Authors in [12] used the concept of S_8 symmetric group and two dimensional Henon chaotic map to propose an image encryption and analyzed it against various statistical attacks.

In this paper, a new image encryption technique is proposed using 80 bit external key and logistic chaotic maps. The proposed algorithm has been analyzed in terms of various performance parameters and found to be robust to various attacks. The manuscript is organized as follows. The proposed image encryption algorithm is presented in section II. Security analysis is performed in section III followed by conclusion in section IV.

II. Proposed Image Encryption Method

1. Proposed image encryption algorithm uses two one dimensional chaotic logistic map defined as in (1) and (2) where r is a parameter that controls the chaotic behavior of logistic map. Here the value of r is taken as 3.9999.

$$x_n = rx_n(1 - x_n) \quad (1)$$

$$y_n = ry_n(1 - y_n) \quad (2)$$

2. Algorithm uses 80 bit external key which is used to calculate initial conditions for maps given as

$$K = K_1 K_2 \dots K_{10} \quad (\text{ASCII Mode}) \quad (3)$$

$$K = k_1 k_2 \dots k_{20} \quad (\text{in hexadecimal}) \quad (4)$$

3. To calculate initial condition X_0 for the first logistic map, keys $K_4 K_5 K_6$ and then $k_{13} k_{14} k_{15} k_{16} k_{17} k_{18}$ are used as

$$X_{01} = \frac{K_{41} \times 2^0 + K_{48} \times 2^7 + K_{51} \times 2^8 + K_{58} \times 2^{15} + K_{61} \times 2^{16} + K_{68} \times 2^{23}}{2^{24}} \quad (5)$$

$$X_{02} = \frac{\sum_{i=13}^{18} k_i}{96} \quad (6)$$

$$X_0 = (X_{01} + X_{02}) \bmod 1 \quad (7)$$

where K_{ij} represents j^{th} bit of i^{th} key.

4. Using X_0 obtained from equation(7), calculate 24 real numbers $r_1, r_2, \dots, r_{24}$ and convert them into integer number as

$$I_i = \text{int}(23 \times r_i) + 1 \quad (8)$$

where i varies from 1 to 24.

5. To calculate the initial condition Y_0 for second logistic map, First keys $K_1 K_2 K_3$ are first converted into binary string S as

$$S = K_{11} \dots K_{18} \dots K_{21} \dots K_{28} \dots K_{31} \dots K_{38} \quad (9)$$

6. Now Y_{01} and Y_{02} are calculated using eq. (10) and (11). where $S(I_i)$ is the I_i^{th} bit in S . Finally Y_0 is calculated using (12)

$$Y_{01} = \frac{S_{10}}{2^{24}} \quad (10)$$

$$Y_{02} = \frac{\sum_{i=1}^{24} S(I_i) \times 2^{i-1}}{2^{24}} \quad (11)$$

$$Y_0 = (Y_{01} + Y_{02}) \bmod 1 \quad (12)$$

7. Divide the interval (0, 1) into 24 non overlapping subintervals and form eight groups as shown in table

1. Corresponding to each group the encryption/decryption operation is defined.

8. Read the pixel of input image into RGB component. Now iterate the second logistic map using Y_0 and check in which group subinterval the generated value lies. Corresponding encryption operation is performed on the RGB components of the pixel. Encrypt sixteen pixels repeating the same process.

9. After encrypting the sixteen pixels the external key is changed as

$$\begin{aligned} (K_i)_{10} &= ((K_{i+1})_{10} + (K_{i+2})_{10}) \bmod 256 & i=1 \text{ to } 8 \\ (K_9)_{10} &= ((K_{10})_{10} + (K_1)_{10}) \bmod 256 \\ (K_{10})_{10} &= ((K_1)_{10} + (K_2)_{10}) \bmod 256 \end{aligned} \quad (13)$$

10. Now reset the initial condition $X_0 = r_{24}$ and repeat the step from 4 to 9. This process is repeated till all the input pixels are encrypted.

Decryption process is similar to encryption process except in step 7 where now corresponding decryption operation is chosen from the table instead of encryption operation

III. Security Analysis

Security analysis of the proposed algorithm is done in terms of key space analysis, histogram analysis, correlation analysis, key sensitivity analysis, entropy analysis, noise and block loss. The performance of proposed algorithm is compared with [12] and found to be more effective.

Table 1 Different group of no overlapping subintervals and corresponding operation for encryption/decryption

Group No	Y falls in	Operations for encryption/ decryption
1	0-0.04, 0.33-0.37, 0.66-0.70	NOT operation on R, G, B values
2	0.04 -0.08, 0.37-0.41, 0.70-0.75	XOR operation, $R \oplus K_4, G \oplus K_5, B \oplus K_6$
3	0.08 - 0.12, 0.41 - 0.46, 0.75 - 0.80	Encryption $((R)_{10} + (K_4)_{10} + (K_5)_{10}) \bmod 256$ $((G)_{10} + (K_5)_{10} + (K_6)_{10}) \bmod 256$ $((B)_{10} + (K_6)_{10} + (K_4)_{10}) \bmod 256$ Decryption $((R)_{10} + 256 - (K_4)_{10} - (K_5)_{10}) \bmod 256$ $((G)_{10} + 256 - (K_5)_{10} - (K_6)_{10}) \bmod 256$ $((B)_{10} + 256 - (K_6)_{10} - (K_4)_{10}) \bmod 256$
4	0.12- 0.16, 0.46 - 0.5, 0.80 - 0.84	Encryption $NOT(R \oplus K_4), NOT(G \oplus K_5), NOT(B \oplus K_6)$ Decryption $(NOT(R)) \oplus K_4, (NOT(G)) \oplus K_5, (NOT(B)) \oplus K_6$
5	0.16 - 0.20, 0.5 - 0.54, 0.84 - 0.88	Similar to group 2 except that K_7, K_8, K_9 are used instead of K_4, K_5, K_6 , respectively.
6	0.20 - 0.24, 0.54 - 0.58, 0.88 - 0.92	Similar to group 3 except that K_7, K_8, K_9 are used instead of K_4, K_5, K_6 , respectively.

7	0.24 - 0.28 , 0.58 - 0.62, 0.92 - 0.96	Similar to group 4 except that K_7, K_8, K_9 are used instead of K_4, K_5, K_6 , respectively.
8	0.28 - 0.33, 0.62 - 0.66, 0.96 - 1	No operation on R, G, B values

A. Key Space Analysis

In cryptosystem, larger the key space is, more security is against brute force attack. The proposed algorithm uses 80 bit long external key. It means total no of possible keys are 2^{80} which is satisfactory large for brute force attack.

Table 2. Average Correlation analysis of adjacent pixels using DEFACB142358690700F5

Image name	original image	Encrypted image [12]	Encrypted image (Proposed method)
4.1.03(color)	0.94613	.1516	0.0155
4.2.05 (color)	0.95905	.0764	0.0181
4.2.07 (color)	0.97095	.0826	.00925
Leena512 (color)	0.9206	.0824	.0201
5.1.11(gray)	0.94685	.1898	.00985
5.1.12 (gray)	0.96583	.2007	.00715
Lena (gray)	0.9443	.1045	.0244
Boat.512	0.09547	.0441	.01335

B. Correlation analysis

Correlation between horizontally and vertically adjacent pixels is calculated using eq.(14) where x_i and y_i are the corresponding pixels in two images and N is the no. of pixels in the image used for computation. Table 2 shows the results for different sample images.

$$C_r = \frac{N \sum_{j=1}^N (x_j \times y_j) - \sum_{j=1}^N x_j \times \sum_{j=1}^N y_j}{\sqrt{(N \sum_{j=1}^N x_j^2 - (\sum_{j=1}^N x_j)^2) \times (N \sum_{j=1}^N y_j^2 - (\sum_{j=1}^N y_j)^2)}} \quad (14)$$

C. Histogram Analysis

Histogram is the graphical representation of distribution of pixels as per the intensity values. The histogram of an encrypted image ideally should be uniform. Figure 1.shows that the histogram of encrypted image is almost uniform and completely different from original.

D. Key Sensitivity Analysis

In a good encryption algorithm, a slight change in the secret key should generate entirely different cipher image. To analyze the key sensitivity the different ciphers are generated using key with slight change and then correlation among them is calculated. For analysis *lena* gray image is taken.

Image1-cipher generated after encrypting input image with key DEFACB142358690700F5

Image2-cipher generated after encrypting input image with key CEFACB142358690700F5

Image3-cipher generated after encrypting input image with key DEFACB142358690700F4.

Results in table 3 show that encrypted images have really low correlation between them.

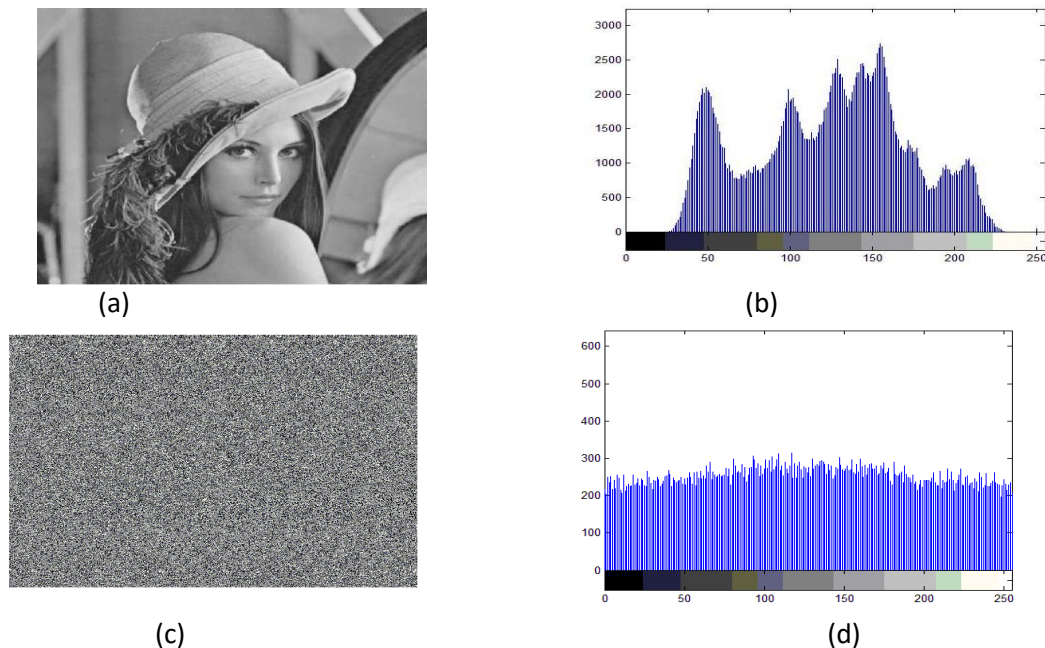


Figure 1. (a) Original image 'Lena' (b) histogram of original image. (c) encrypted image of original image of fig.1 (a) using proposed method (d) histogram of encrypted image in fig1(c).

Table 3. Key Sensitivity Analysis

First Image	Second Image	Correlation Coefficient
Image 1	Image 2	0.0049
Image 2	Image 3	0.0041
Image 1	Image 3	0.0050

Table 4. Entropy analysis

Image name	original image	Encrypted image [12]	Encrypted image (Proposed method)
4.1.03(color)	6.4565	7.9467	7.9553
4.2.05 (color)	6.5769	7.9973	7.9404
4.2.07 (color)	6.7653	7.9502	7.9512
Leena512 (color)	7.2718	7.6792	7.9575
5.1.11(gray)	6.7896	7.5528	7.9256
5.1.12 (gray)	6.7057	7.4788	7.9634
Lena (gray)	7.4455	7.4455	7.9719
Boat.512	7.1918	7.1919	7.9626

Table 5: PSNR (dB) and SSIM index analysis and comparison

Attack Type	PSNR		SSIM	
	[12]	Proposed method	[12]	Proposed Method
Gaussian Noise (Mean 0, Variance 0.01)	27.4366	28.439	0.0167	0.2455
Gaussian Noise (Mean 0, Variance 0.05)	27.3142	27.5123	0.0162	0.1119
Gaussian Noise (Mean 0, Variance 0.1)	27.2671	27.4674	0.0151	0.0751
Salt and Pepper noise (Intensity 0.8)	40.1998	40.4238	0.4526	0.5123
Salt and Pepper noise (Intensity 0.8)	38.1409	38.4086	0.3261	0.3284
Salt and Pepper noise (Intensity 0.8)	37.1224	37.3268	0.2768	0.3284
Block Loss (15 x15 blocks)	40.2976	43.6097	0.9600	0.9715

E. Entropy Analysis

For a message m , consisting of symbols $(a_0, a_1, \dots, a_{l-1})$ with the probability of occurrence of symbol a_i as p_i is defined as

$$H(m) = \sum_{i=1}^{l-1} p_i \log_2 p_i \quad (15)$$

The values of a_i are from 0 to 255. The results are shown in table 4 and it can be observed that the entropies of encrypted images are close to ideal value 8.

F. Noise attack and block loss analysis

Gaussian white noise contamination, paper and salt noise contamination with various parameters and block loss have been used as attacks on the cipher image. For block loss analysis, randomly located blocks of size 15x15 have been removed from the cipher image. Standard boat image of size 512x512 has been used for analysis. Table 5 shows results in terms of peak signal to noise ratio (PSNR) and structural similarity (SSIM) index. MATLAB code of SSIM index available online at <http://www.cns.nyu.edu/lev/ssim/> has been used with its default parameters. It is observed that the PSNR and SSIM for the decrypted image using proposed encryption/decryption method is better than others.

IV. Conclusion

In this paper, an image encryption technique based on a chaotic map has been proposed using 80 bit external key and its performance has been analyzed in terms of resistance to various attacks such as histogram analysis, correlation analysis, Key sensitivity and key space analysis to evaluate its effectiveness for image security. Further, it has also been analyzed for entropy measurement and various attacks on cipher image like block loss and introduction of noise as well. The results show that the proposed algorithm performs better on various attack parameters.

References

- [1] J. Fridrich, "Symmetric ciphers based on two dimensional chaotic maps", J. of Bifurcate Chaos, World Sc. 8 1259–1284,1998.
- [2] C. C. Chang, M. S. Hwang and T. S. Chen, "A new encryption algorithm for image cryptosystems", J. of Sys. Software, vol. 58, pp. 83–91, 2001.

- [3] L. Kocarev, "Chaos based cryptography: a brief overview", IEEE Ckt. Sys. Mag 1, pp. 6–21, 2001.
- [4] S. Li and X. Zheng, "Cryptanalysis of a chaotic image encryption method", Proc. IEEE Int. Symposium Ckt. and Sys, (Scottsdale, AZ, USA), pp. 708–711, 2002.
- [5] Y. B. Mao, G. Chen and S. G. Lian, "A novel fast image encryption scheme based on 3D chaotic baker map", J. of Bifurcate Chaos, World Scientific, vol. 14, pp. 3613–3624, 2004.
- [6] Chen, G., Mao, Y. and Chui, C., "A symmetric image encryption scheme based on 3d chaotic cat maps", *Journal of Chaos, Solitons and Fractals*, vol. 21 : 749–761, 2004.
- [7] Pareek, N. K., Patidar, V. and Sud, K. K., "Image encryption using chaotic logistic map", *Journal of Image and Vision Computing*, vol. 24, 926–934, 2006.
- [8] Jain, A. and Rajpal, , "A two layer chaotic network based image encryption technique", Proc. Of Conference on Computing and Communication System, 2012.
- [9] Wang, Y., Wong, K. W., Liao, X. and Chen, G. , "A new chaos-based fast image encryption algorithm", *Journal of Applied Soft Computing* vol. 11, pp. 514–522, 2011.
- [10] Tang, Z., Zhang, X. and Lan, W. , "Efficient image encryption with block shuffling and chaotic map," *Journal of Multimedia Tools and Applications* DOI = 10.1007/s11042-014- 1861-1 ,2014.
- [11] Hussain, I., Shah, T. and Gondal, M. A. , "Application of s-box and chaotic map for image encryption", *Journal of Mathematical and Computer Modeling* vol. 57, pp. 2576–2579., 2013.
- [12] Khan, M. and Shah, T., "A novel image encryption technique based on henon chaotic map and s_8 symmetric group", *Journal of Neural Computing and Applications*, vol. 25, 1717–1722, 2014.