Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Image Encryption Technique Using Random Pixel Permutation by Chaotic Map and Linear Congruential Generator

Sukhjeevan Kaur
M.Tech Scholar
Dept of CSE, DAVIET,
Jalandhar, Punjab, India

Shaveta Angurala
Assistant Professor
Dept of C.S.E, DAVIET,
Jalandhar, Punjab, India

Abstract: ***The chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. In the field of chaos, this paper proposed the technique based on pixel permutation by using chaos logistic map and linear congruential generator. To provide an efficient encryption of images, the proposed technique generates random numbers which are used as index for shuffling of rows, columns and pixels of an image. Several test images are used for inspecting the security of the proposed technique. The proposed technique is simulated using Matlab and the experimental results demonstrate that the encrypted images have good information entropy; the distribution of gray values of an encrypted image is uniform and the encrypted image provides less significant information. The experimental result gives good qualitative and quantitative analysis which shows that this technique is secure for image encryption.***

Keywords: Linear congruential generator, Logistic map, Encryption, Decryption,PSNR,SC

I. INTRODUCTION

Confidential communication has long been a common practice in the social life. However, as information can be communicated electronically, it is exposedin public domain and unavoidably resulted in interceptions. The growth of [1] electronic commerce (e-commerce) and the emphasis of privacy have intensified the need to find a fast and secure cryptographic method. An image is an important data which is communicated electronically because of its visual characteristics [2]. Image should be encrypted properly due to sensitivity to changes as well as security perspective. But because of inherent characteristics of image, standard encryption algorithms are not suitable for image encryption [3].

II. LITERATURE SURVEY

This section provides a brief overview of the work done in the same field.

Chaotic Image Encryption

Chaos theory has been established by many different research areas, such as physics, mathematics, engineering, and biology [4]. Since last decade, many researchers have noticed that there exists the close relationship between chaos and cryptography [5]. The distinct properties of chaos, such as ergodicity, quasi-randomness, sensitivity dependence on initial conditions and system parameters, have granted chaotic dynamics as a promising alternative for the conventional cryptographic algorithms. Chaos-based cryptography is relied on the complex dynamics of nonlinear systems or maps which are deterministic but simple. Therefore, it can provide a fast and secure means for data protection, which is crucial for Multimedia data transmission over fast communication channels, such as the broadband internet communication. Chaos seems to be a good approach due to its ergodicity and complex dynamics.

Yen et al. [6] also proposed an encryption method called CKBA (Chaotic Key Based Algorithm) in which a binary sequence as a key is generated using a chaotic system. The image pixels are rearranged according to the generated binary sequence and then XORed and XORed with the selected key.

Hossam El-din H. Ahmed et al. [1] presented an efficient chaos based feedback stream cipher (ECBFSC) for image cryptosystems. The proposed stream cipher is based on the use of a chaotic logistic map and an external secret key of 256-bit. The initial conditions for the chaotic logistic map are derived using the external secret key by providing weightage to its bits corresponding to their position in the key. Further, new features of the proposed stream cipher include the heavy use of data-dependent iterations, data-dependent inputs, and the inclusion of three independent feedback mechanisms. These proposed features are verified to provide high security level.

G.A. Sathish Kumar et al.[7] proposed a new image encryption algorithm using random pixel permutation based on chaos logistic maps and prime modulo multiplicative linear congruential generators. The random-like nature of chaos is effectively spread into the encrypted image through permutation and transformation of pixels in the plain image. The pixel transformation results in the encryption scheme being resistive to cryptanalytic attacks. Simulation results show high sensitivity to key, plaintext and cipher text changes. From a cryptanalytic point of view, the scheme is highly resistive to known/chosen plaintext and cipher text attacks. The proposed technique gives good parametric and sensitivity results proving itself an eligible candidate for image encryption. Moreover it is a lossless encryption technique and hence

use for securing medical and military image.

Jiankun Hu et al [8] proposed a novel pixel-based scrambling scheme to protect, in an efficient and secure way, the distribution of digital medical images. To provide an efficient encryption of a large volume of digital medical images, the proposed system uses simple pixel level XOR operation for image scrambling in an innovative way such that structural parameters of the encryption scheme have become a part of the cryptographic key. The cryptographic key of this operation is a true random number sequence generated from multi-scroll chaotic attractors.

Ji Won Yoon et al [15] proposed a new image encryption algorithm using a large pseudorandom permutation which is combinatorially generated from small permutation matrices based on chaotic maps. The random-like nature of chaos is effectively spread into encrypted images by using the permutation matrix.

III. SIMULATIONENVIRONMENT

MATLAB stands for Matrix Laboratory developed by the Mathworks. We have used MATLAB platform to implement the proposed algorithm. MATLAB has predefined classes to perform operation on images. MATLAB is a numerical computing environment and fourth generation programming language.

3.1 Proposed technique

A. Image Encryption Using Linear Congruential Generator

It is most commonly used method for pseudo number generation [13], defined by following equation:

$Xn+1 = (aXn+c) \bmod m$ ..... (1)

Where a- multiplier, m- Modulus, c- Constant

An arbitrary starting seed value(Xn) is needed in equation(1) with above mentioned parameters for generation of random numbers which have range up to the value of modulus (m).In this scheme, two random numbers sequences are generated based on equation(1), by choosing appropriate parameters and seed value. Then by using values of these random numbers, image permutation occurs by shuffling of rows, columns and pixels of image. One sequence is used for row shuffling and another is used for column shuffling. A masking operation [3] is used after row and column shuffling by simple XOR operations between adjacent rows and columns. By values of both sequences, pixel shuffling is done.

B. Image Encryption Using Chaotic Logistic Map

Logistic map is a mathematical iterative system used for generating random numbers, defined by following iterative equation:

$Xn+1 = r*Xn*(1-Xn)$ ..... (3)

Where r is growth rate parameter. By choosing appropriate seed value (Xn) and growth rate (r), equation (4) can be used to generate random number sequence [13] [3] [14] which have long period value. In this scheme, two random numbers sequences are generated based on chaotic logistic map. One sequence is used for row shuffling, another for column shuffling. Pixel shuffling is done by taking both sequences together, same as scheme (A). A masking operation [5] is used after row and column shuffling by simple XOR operations between adjacent rows and columns.

3.2 Performance Parameters

(a) **Histogram**: An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each colour intensity level [1][7]. In graph the horizontal axis represents the tonal variations (colour value variation), while the vertical axis represents the number of pixels in that particular tone. The left side of the horizontal axis represents the black and dark areas, the middle represents medium grey and the right hand side represents light and pure white areas.

(b) **Entropy**:Entropyis a cumulative measure of the frequency of the intensity levels in an image [1].

$H(s) = -\sum_{i=0}^{N-1} p(s_i) \log_2 p(s_i)$ (4)

Where $p(s_i)$represents the probability of symbol (s,i).

(c) **Peak Signal-to-Noise Ratio**(**PSNR)**: Peak Signal-to-Noise Ratio is commonly used as a measure of quality of the encryption technique. In image encryption high value of PSNR means the amount of significant signal information present is very much[7], but to protect ciphered image from attack PSNR value must be low.

(d)**Structural Content (SC)**:SC is an effective way of comparing two images based on their weights. Reconstructed image is of good quality if SC value lies near 1, greater values indicate poor quality image [11]. It can be calculated by using the given formula,

$SC=(\sum_{i,j}^{N-1} C(i,j)^2)/(\sum_{i,j}^{N-1} \hat{C}(i,j)^2)$

WhereC(i,j) represents original image and Ĉ(i,j) represents reconstructed image.

IV. RESULTS ANALYSIS

4.1 Qualitative analysis

We have calculated and analysed the histogram of the several encrypted images as well as its original images. One typical example is shown in Fig.2. The histogram of plain image contains large spikes. These spikes correspond to colour values that appear more often in the plain image. The histogram of the cipher image is shown in the Fig.3 by using proposed technique is more uniform, significantly different from that of the original image and bears no statistical resemblance to the plain image which means it does not provide any clue to employ any statistical attack on the proposed technique.

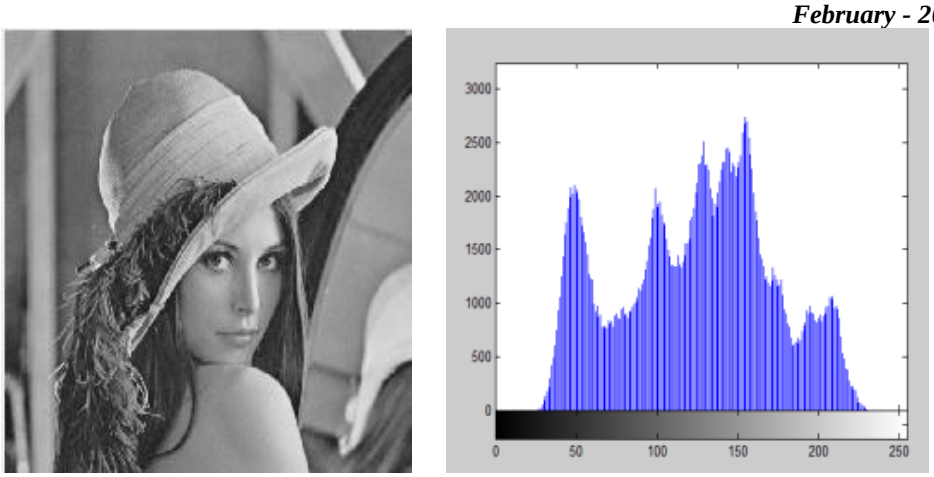

Fig.1 Original Lena image and its histogram

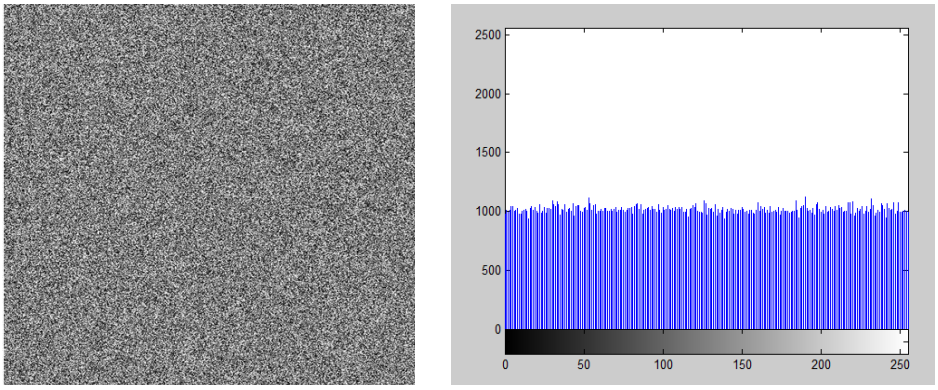

Fig.2 Encrypted image and its histogram

4.2 Quantative Analysis

(a)**Entropy** : Information entropy of an encrypted image can show the distribution of gray value. The more the distribution of gray value is uniform, the greater the information entropy. If the value of entropy of an encrypted image is less than ideal value 8,then there is possibility that encrypted image would be predicted which threatens the image security. The values of information entropy for encrypted images by applying proposed algorithm is very close to ideal value 8. This means that the information leakage in the proposed encryption process is negligible and the image encryption system is secure against the entropy attack. The entropy value of different encrypted images is shown in Table 1.

Table1. Information Entropy of different ciphered images

Image Name	**Entropy**
Lena	7.999
Pepper	7.999
Baboon	7.999

(b)**Peak Signal-to-Noise Ratio(PSNR):**In image encryption, a low value of PSNR for the cipher image implies that the cipher image is noise-like, i.e., the amount of significant signal information available is very less in the cipher image. The PSNR results obtained by encrypting sample images with our proposed technique, in comparison to the PSNR obtained in earlier chaos-based techniques[7], [9], [10] is presented in Table 2. Our results provide a PSNR lower than that of currently existing techniques, thereby showing significant improvement.

Table 2. Quantitative analysis (PSNR values of different ciphered images)

Image Name	**Our Technique**	**Previous Technique [7],[9],[10]**
Lena	9.22	14.87
Pepper	8.88	12.93
Baboon	9.47	9.88

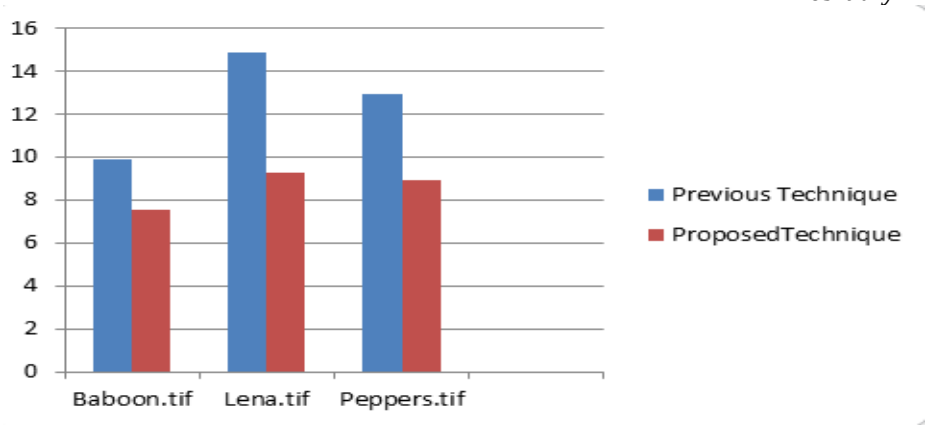

Fig 3. Comparison of PSNR result

(c)**Structural Content (SC):** This measure effectively compares the total weight of an original signal to that of a coded or given. It is therefore a global metric, and if it is spread at 1, then the converted image is of better quality and large value of SC means that the image is poor quality [16].The SC result obtained by applying our proposed technique is shown in Table 3.

Table 3. SC values of ciphered images

Image	Structural Content
Lena	0.814453
Pepper	0.80069
Baboon	0.769703

V. CONCLUSION

In this paper a new algorithm of encryption is presented based upon Chaos logistic map and linear congruential generator. This technique is based on therandom numbers which are generated by using Chaos map and linear congruential generator. Random numbers generated by prime modulo multiplicative linear congruential generatorand chaos map are used as index for shuffling of rows, columns and pixels of an imageIn this paper, review of some chaotic based image encryption is done that describes different ways to improve the performance of image encryption.. The maximum entropy h in an 8–bit image can attain is 8. The average of our results is 7.99. Hence a statistical attack is difficult to make. Also results for PSNR values are better when the proposed technique is applied.Allthe abovequantative and qualitative analysisshow the effectiveness of proposed algorithm which means that proposed technique provides good security against statistical attack and can be used for encryption of images. To show the effectiveness of proposed technique correlation parameter will be taken in another paper.

REFRENCES

[1] Hossam El-din H. Ahmed, HamdyM.Kalash, and Osama S. Farag Allah, “An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption”, Informatica,pp.121–129,2007.

[2] Vinod Patidar, N.K. Pareek , K.K. Sud, “A new substitution–diffusion based image cipher using chaotic standard and logistic maps”, Communications in Nonlinear Science and Numerical Simulation ,Elsevier, vol.14,no.7,pp. 3056–3075,2009.

[3] Guanrong Chen, Yaobin Mao, Charles K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps”, Chaos, Solitons and Fractals 21,Vol.21,No.3,Elsevier, pp.749–761,2004

[4] Shubo Liu, Jing Sun, ZhengquanXu,”An Improved Image Encryption Algorithm based on Chaotic System” Journal of Computers, Vol. 4, No. 11, 2009.

[5] LIU Xiangdong, Zhang Junxing, Zhang Jinhai, He Xiqin,” Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation”, International Journal of Computer Science and Network Security, VOL.8 No.1, 2008.

[6] J.C. Yen, J.I. Guo, "A new chaotic key based design for image encryption and decryption", Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, pp. 49–52, 2000.

[7] G.A.Sathishkumar, Srinivas Ramachandran, Dr.K.BhoopathyBagan,“Image Encryption Using Random Pixel Permutation by Chaotic Mapping”, Symposium on computers and informatics(ISCI), IEEE,pp.247-251,2012.

[8] Hu, Jiankun, and Fengling Han. "A pixel-based scrambling scheme for digital medical images protection." Journal of Network and Computer Applications 32, no. 4. 2009.

[9] G.A.Sathish Kumar et al./Procedia Computer Science 3 (2011) 378-387.

[10] I.A.Ismail,Mohammed Amin and HossamDiab "An Efficient Image Encryption Scheme Based chaotic Logistic Map", International .Journal of Soft Computing,285-291,2007.

[11] Vibha Tiwari1, P.P. Bansod and AbhayKumar, "Performance Evaluation of Various Compression Techniques on Medical Images", International journal of advanced electronics and communication system, No.2, 2012.

[12] Kocarev L, Jakimoski G. "Logistic map as a block encryption algorithm". Phys Lett A 2001;289(4–5):199–206.

[13] C.E. Shannon, "Communication Theory of Secrecy System" , Bell Syst. Tech. J. 28, pp. 656-715, 1949.

[14] Y.B. Mao, G. Chen, S.G. Lian, "A Novel Fast Image Encryption Scheme Based on the 3D Chaotic Baker Map", Int. J. Bifurcat. Chaos 14(10), pp. 3613-3624, 2004.

[15] Yoon, Ji Won, and Hyoungshick Kim. "An image encryption scheme with a pseudorandom permutation based on chaotic maps." Communications in Nonlinear Science and Numerical Simulation 15, no. 12. 2010.

[16] K.Berlin ,A.Padmapriya," Performance Analysis of Threshold based Image Encryption" International Journal of Computer Applications (0975 – 8887) Volume 99– No.12,pp. 30-33, 2014 .

