ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Image Encryption Using Chaotic Map and Prime modulo Multiplicative Linear Congruential Generator

Sukhjeevan Kaur, Shaveta Angurala

Department of Computer Science and Engineering, DAVIET, Jalandhar, India

ABSTRACT: The chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques because of its exceptionally desirable properties of sensitivity to initial condition and parameters of chaotic map. In this study an image encryption algorithm is presented, in which chaos based encryption technique and prime modulo multiplicative linear Congruential generator (PMMLCG) has been used to improve the quality of image encryption and to achieve the goal of pixel scrambling. The proposed algorithm generates random numbers, which are used in row shuffling, column shuffling and pixel scrambling which results in encryption technique highly resistive to cryptanalytic attack. Results and effectiveness is measured in qualitative and quantitative metrics which shows that this encryption algorithm is securefor encryption of images.

KEYWORDS: Linear congruential generator, Logistic map, Encryption, Decryption, PSNR, SC, SSIM.

I.INTRODUCTION

Information security is one of the important issues in the present information age; it involves the confidentiality, integrity, availability and controllability of information.Images are the integral part of the information in engineering, industrial application as well as in medical processes.

Images have intrinsic features such as bulk data capacity and strong correlation among adjacent pixels etc. for which conventional number theory based algorithms do not seem to be appropriate such as RSA,DES, and AES [2]. The theory of chaotic map present many desired cryptographic qualities such as simplicity of implementation that leads to high encryption rates, and excellent security. The chaos based cryptography algorithms have suggested some new and efficient ways to develop secure image encryption techniques for image transmission over communication channels and a lot image encryption algorithms based upon chaotic system have been proposed[4-5], [7], [9], [12-13].In this paper image encryption technique is presented based upon chaotic map. In the proposed algorithm mask operation is applied on original image pixel and generated random sequence by chaotic map and then the pixels are scrambled using generated sequence by PMMLCG and chaotic map. The paper is organised as follows.In the Section II description of the overall framework of the proposed technique is presented and the chaotic map is discussed. Section III evaluates the performance of proposed work. Section IV presents the conclusion of the paper.

II. PROPOSED IMAGE ENCRYPTION TECHNIQUE

The proposed technique first generates a chaos sequence, then prime modulo multiplicative linear congruential generator sequence and at last again generates chaos sequence. The effectiveness of algorithm depends upon the randomness of the generated sequence. The chaotic binary sequence is generated depending on the size of the image, and the predefined value of μ (3.9876543210001, 4) and the PMMLCG sequence is generated depending on the input secret key. The initial seed value for the random sequence generators are derived from the secret key. The generated sequence is then used for 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 is used after row and column shuffling by simple XOR operations between adjacent pixels. By values of both sequences, pixel shuffling is done. The proposed image encryption technique is illustrated in Fig.1 and described below

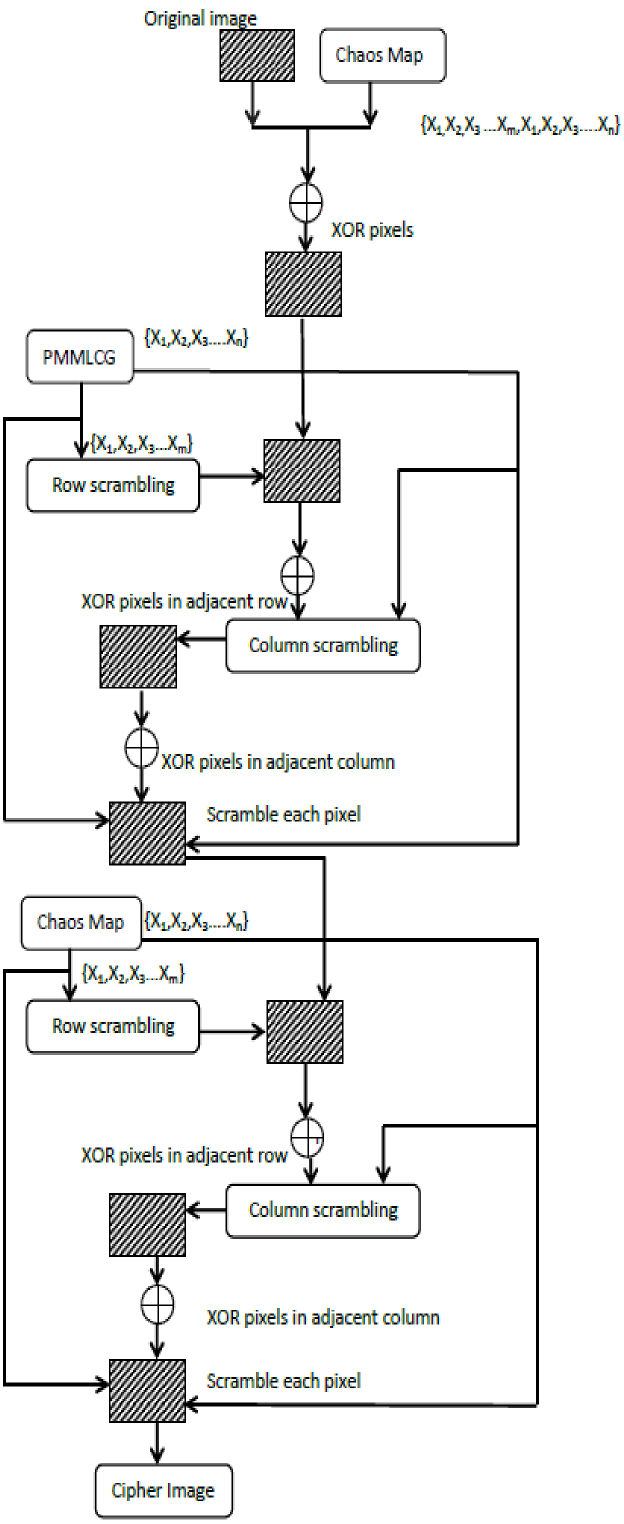

Fig.1 Proposed image encryption technique

A. Algorithm

Step 1:Read an input plain image.

For the Gray scale image I of size M x N pixels, we can generate two chaos sequences of real numbers of lengths M and Nrespectively as given by,

$$x_{n+1} = \mu x_n(1 - x_n) \qquad (1)$$

where µis the control parameter governing the chaotic behaviour, X is the sequence of pseudorandom value; $x_n$is the initial seed value. The initial seed value for one of the sequences is derived from the secret key and the first element of this sequence is used as the initial seed for the second sequence.

Step2:Mask each pixel I(i, j)in the image to a position I(x_i , x_k), with$x_i$taken from one sequence and $x_k$taken from the other by applying XOR operation.

Step3: Read an input plain image.

For the Grayscale image I of size M x Npixels, we can generate two PMMLCG sequences of real numbers of lengths M and Nrespectively as given by,

$$X_{n+1} \equiv (aX_n + c) \text{mod } m \qquad (2)$$

where, ais a multiplier. The initial seed value for one of the sequences is derived from the secret key and the first element of this sequence is used as the initial seed for the second sequence.

Step 4:Permute theIth row of the image *I* with the $x_i$throw and XOR pixel values in adjacent rows. Permute the kth column with $x_k$thcolumn and XOR pixel values in adjacent columns, for all values of *i* from 1 to *M* and *k* from 1 to *N*.

Step 5: If i=M and k = N,end the iteration. Otherwise, increment i and k and Repeat the previous step.

Step 6: Scramble each pixel I(i, j) in the image to a position I(x_i , x_k), with $x_i$taken from one sequence and $x_k$taken from the other.

Step 7*:* Similarly, we can have an arbitrary chaotic iteration second time given by,

$$x_{n+1} = \mu x_n(1 - x_n) \qquad (3)$$

to generate two chaotic sequences of real numbers of lengths M and Nrespectively.

Step 8: Permute the ith row of the image *I* with the x_i throw and XOR pixel values in adjacent rows. Permute thekth column with $x_k$thcolumn and XOR pixel values in adjacent columns, for all values of *i* from 1 to *M* and *k* from 1 to *N*.

Step 9: If i=M and k = N, end the iteration. Otherwise, increment i and k and repeat the previous step.

Step 10: Scramble each pixel I(i, j) in the image to a position I(x_i , x_k), with $x_i$taken from one sequence and $x_k$taken from the other and display the cipher image.

III. SECRUITY ANALYSIS

3.1 Qualitative analysis

(a)Histogram: An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each colour intensity level [3][4].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 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.

3.2 QUANTATIVE ANALYSIS

(a)Entropy: Entropyis a cumulative measure of the frequency of the intensity levels in an image [3].

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

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

(b)Cross-correlation: In addition to the histogram analysis, we have also analysed the cross-correlation. The cross-correlation coefficient [5],[6] and [7] C_{AB}between the plain image A and the cipher image B quantifies the level to which the encrypted image pixels are relatively randomized .The closer it is to zero, this means that the adjacent pixel in the encrypted image are highly uncorrelated to each other.The cross-correlation is measured with the following equation.

$$C_{AB}=\frac{\frac{1}{r*c}\sum_{i}^{r}\sum_{j}^{c}(A_{i,j}-\bar{A})(B_{i,j}-\bar{B})}{\sqrt{\frac{1}{r*c}\sum_{i}^{r}\sum_{j}^{c}(A_{i,j}-\bar{A})^2\frac{1}{r*c}\sum_{i}^{r}\sum_{j}^{c}(B_{i,j}-\bar{B})^2}} \quad \text{Eq.(5)}$$

$A_{i,j}$and $B_{i,j}$are the pixels in the ith row and jth column of A and B respectively and r, c represent the no. of rows and columns in the image.

(d) Horizontal and Vertical Correlation: The horizontal and vertical correlation is used to measure the correlation between two horizontally and vertical adjacent pixels respectively [3][14].The horizontal and vertical correlation measured with our technique is shown in Table 1.

$$r_{xy}= cov(x,y)/(\sqrt{D(x)}\sqrt{D(y)}\ ) \qquad \text{Eq.(6)}$$

(c)PSNR: Peak Signal-to-Noise Ratio is commonly used as a measure of quality of the encryption technique. 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 [4] is presented in Table2. Our results provide a PSNR lower than that of currently existing techniques, thereby showing significant improvement.

(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 [10].The proposed technique gives SC value closer to 1.It can be calculated by using the given formula,

$$SC=(\textstyle\sum_{i,j}^{N-1} C(i,j)^{2})/(\sum_{i,j}^{N-1} \hat{C}(i,j)^{\ 2}) \qquad \text{Eq.(7)}$$

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

(e)Structural Similarity Index (SSIM): SSIM is used to compare luminance, contrast and structure of two images [10]. Two images will have good similarity if SSIM value is 1 and poor if it is lesser than 0.90. This proposed scheme gives SSIM value between 0.0055-0.0997.

$SSIM(x,y)=((2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2))/((\mu_x+\mu_y+c_1)(\sigma_x^2+\sigma_y^2+c_2))$ Eq.(8)

whereμ_x the average of x, μ_y the average of y, σ_x^2 ,σ_y^2 represent the standard deviation of x and y,σ_{xy} the covariance of x and y.c_1 and c_2 represents the two constants used to avoid instability.[10]

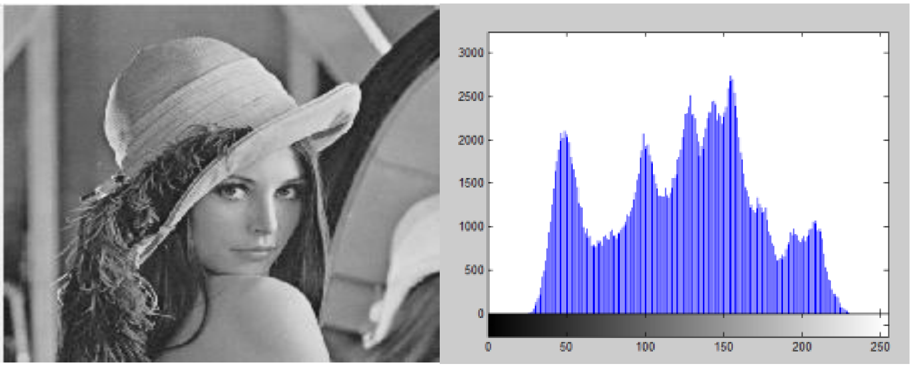

Fig.2 Original Lena image and its histogram

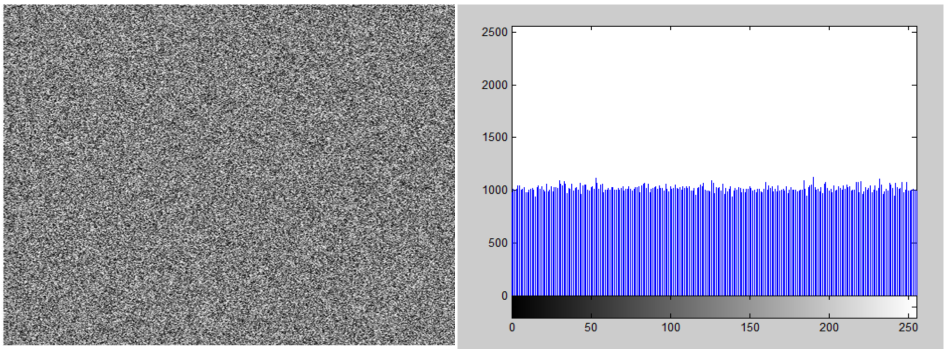

Fig.3 Encrypted image and its histogram

Table1. Correlation coefficient of adjacent pixels in original image and encrypted image

Image Name	Original Image		Encrypted Image		
	Horizontal	Vertical	Horizontal	Vertical	Cross Correlation
Lena	0.9772	0.9755	-0.0018194	-0.0014655	-0.00114881
Pepper	0.97063	0.9829	0.00231818	0.0049123	0.000296285

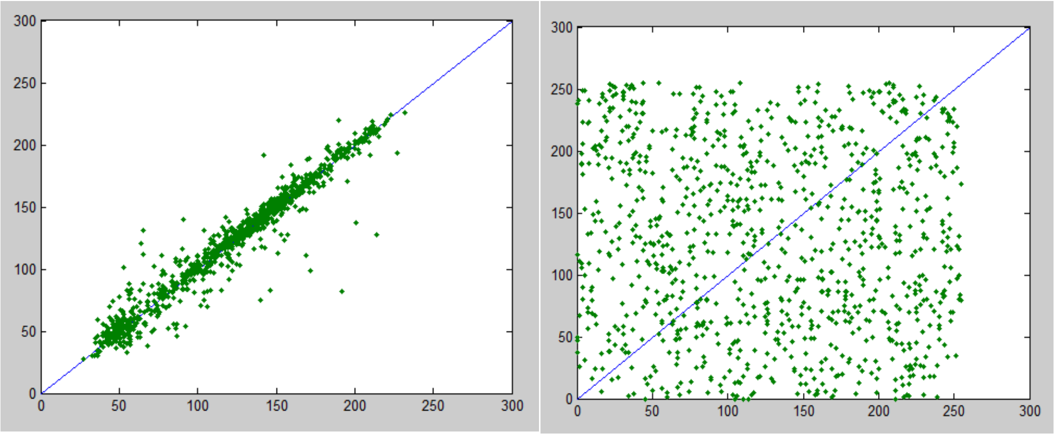

Fig4. Horizontally correlation of two adjacent pixels in plain image/encrypted image (Lena)

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

Image Name	Our Technique	Previous Technique[4]
Lena	9.22	14.87
Pepper	8.88	12.93

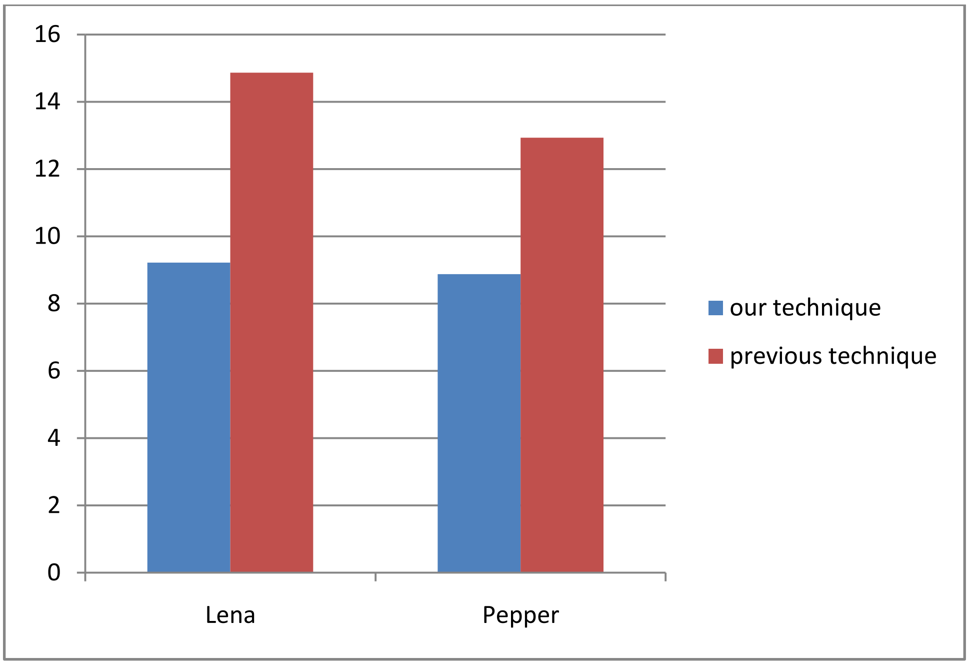

Fig5.Comparison of PSNR result

Image Name	SSIM
Lena	0.00645012
Pepper	0.00721883

Table3. SSIM values of different images

3.3 Key Space

Key space size is the total number of different keys that can be used in the encryption. A good encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible. In this proposed algorithm, the initial conditions and parameters can be used as keys. The proposed encryption algorithm uses three different chaotic map, chaotic maps with different initial values. One map is for row scrambling, one map for column scrambling and another for XOR operation. Similarly two different PMMLCG sequences are used for row and column scrambling. So, this scheme provides a choice of using different keys. It provides a larger keys spaceof iterations to skip before the actual encryption/decryption starts.

IV. CONCLUSION

In this paper a new algorithm of encryption is presented based upon Chaos logistic map and PMMLCG. In quantitative analysis metric, our proposed work decreased the Peak Signal to Noise Ratio (PSNR) value from 23.78% to 37.52 % with mean of 30.87%, which implies that the cipher image is more noise like, i.e. the amount of significant signal information available is very less in the cipher image. 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 SSIM are better when the proposed technique is applied. All comparisonoftheresults obtainedfrom proposed algorithmandprevious techniqueshowthat the proposed algorithm ismoreefficientin terms of performance.

REFRENCES

[1]Behrouz A. Forouzan "Cryptography and Network Security".
[2]B. Schneier, "Applied Cryptography: protocols, algorithms, and source code in C", 2nd ed.

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

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

[5] V. Patidar, N. Pareek, and K. Sud, “Modified substitution-diffusion image cipher using chaotic standard and logistic maps”, Communications in Nonlinear Science and Numerical Simulation, Vol. 15, No 10, pp 2755-2765, 2010.

[6] Chang C, Hwang M, Chen T, “A new encryption algorithm for image cryptosystems.”JSyst Software;58:83–91, science, vol. 809, Springer, Berlin; 1993. p. 71–82, 2001.

[7] Sun F, Liu S, Li Z, Lu Z. “A novel image encryption scheme based on spatial chaos map”. Chaos SolitonFract 2008;38(3):631–40.

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

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

10 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.

[11]Kocarev L, Jakimoski G. “Logistic map as a block encryption algorithm”. PhysLett A 2001;289(4–5):199–206.

[12]VinodPatidar, 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.

[13]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

[14] MusheerAhmad,M. ShamsherAlam, “A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping” ,International Journal on Computer Science and Engineering,Vol.2,pp.46-50,2009.