RESEARCH ARTICLE OPEN ACCESS

Symmetric Encryption Scheme Using Logistic Map

K.Saranya [1], AG.Shanmathi [2], N.Suchitra [3], Dr.S.Ramakrishnan M.E. Ph.D [4]
UG Students [1], [2], [3], Professor and Head [4]
Department of Information Technology
Dr. Mahalingam College of Engineering and Technology
Coimbatore – 642003
Tamil Nadu - India

ABSTRACT

With modern technological advancements, multimedia messages overpower the usage of text messages. These messages are usually exchanged using the internet. Security threats are drastically increasing over the internet. In such a scenario, the need for security enhancements during the multimedia exchange becomes unavoidable. Security measures can be taken by collaborating cryptographic techniques with image processing. Grey scale images are dealt here. The original image is first permuted using logistic map. The same is done on a cover image. The permuted pixel values of the original cover image are then substituted with the summation of corresponding pixel values of the resultant permutation pixel values of the original and the cover image. Thus it is difficult for the attackers to decrypt the original image because the attackers have no knowledge about the cover image. The attacker should also know the exact parameters used for the logistic maps to get the original image, which is very difficult to guess. In this proposed approach, grey scale image encryption using logistic maps is immune to attacks. Various result analysis techniques like histogram analysis, entropy analysis, Number of Changing Pixel Rate analysis and correlation coefficient analysis has been proposed to analyse the result. Thus this approach is used for secure transmission of grey scale images in an open network.

Keywords:- Permutation, Substitution, Chaotic Map, Logistic Map, Number of Changing Pixel Rate, Correlation.

I. INTRODUCTION

Cryptography: Cryptography is the art and science of keeping messages secure. This relates to various types of aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation. A cryptographic algorithm, or cipher, is the mathematical function used for encryption/decryption which involves converting the original images into another form, for the purpose of security.

***Encryption and Decryption*:** Based on cryptographic principles, Encryption is the process of translating original data (plaintext) into a random, meaningless data (cipher text). Decryption is the process of converting cipher text back to plaintext. This is usually done with the help of a special knowledge called key.Image Encryption is a notable domain where numerous research activities are carried out these days. Encryption involves converting data or information from its original form to an unpredictable hidden form making it tedious for retrieval. Protecting the image data from Unauthorized access is important. Encryption is employed to increase the image security.

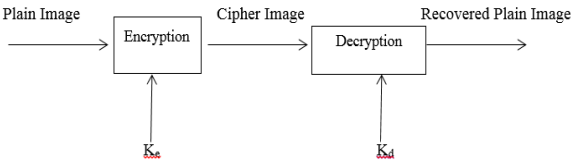


Fig.1. Structure of Image Encryption

***Permutation and Substitution*:** Permutation technique is the one in which the plaintext remains the same, but the shuffling occurs in the order of the characters. It refers to the act of reordering the smallest data unit according to some algorithm. To be effective, any no uniformity of plaintext data units has to be redistributed across the cipher text, making that no uniformity much harder to detect. **Substitution** technique is one in which each character in the plaintext gets substituted for some other character in the cipher text. The receiver inverts the substitution on the cipher

text to recover the plaintext. **Confusion** refers to making the connection that exists between the cipher text and the symmetric key as complex as possible. It means that each character of the cipher text should depend on several parts of the key. **Diffusion** refers to dissipating the statistical structure of plaintext over bulk of cipher text. It means that if we change a character of the plaintext, then there should be a huge change in the characters of the cipher text, vice versa. This complexity is generally implemented through repeated series of substitutions and permutations.

Chaotic Maps: Chaotic maps are considered to be the widely used trend for enhancing the strength of image encryption schemes. Different encryption schemes based on chaotic maps emerge mainly impressed by the chaotic properties of dynamical systems such as high sensitivity in the case of initial conditions, ergodicity, and topological transitivity. It is well known that a good encryption algorithm should have a greater sensitivity to the secret key, and also possess a large key space making brute-force attacks infeasible. Some of the widely used chaotic maps are Logistic Map, Arnold's Cat Map, Hénon Map, Tent Map, Sine Map, Gauss Map, Shift Map, etc.,

***Logistic Map*:** An one dimensional chaotic map with X output and input variable and two initial conditions X_0 and r represents the logistic map that can be mathematically depicted as follows:

$$X_{n+1}=r\ X_n(1-X_n) \qquad (1)$$

Where r lies in the interval of [0,4] in which, the chaotic behaviour is achieved when r is 3.9999. In our encryption algorithm we used logistic map to Shuffle the Pixels Mapping Arrays (PMA) (as shown in Eq.(1)).The relative simplicity of the logistic map makes it a widely used concept of chaos. A chaos can be achieved efficiently when the chaotic systems exhibit a great sensitivity to initial conditions which is the characteristic property of the logistic map for the values of *r* over the range of 3.57 and 4. A common source of such sensitivity to initial conditions is that the map represents a repeated folding and stretching of space where it is defined. The quadratic difference equation describing the logistic map may be thought of as a stretching-and-folding operation on the interval (0, 1).

II. RELATED WORK

There has been a lot of research on the analysis of secure transmission of images over the internet.

A fast chaos-based image encryption system with stream cipher structure using 32-bit precision representation with fixed point arithmetic is used to achieve a fast throughput and facilitate hardware realization. The encryption system is based on a pseudo-random key stream generator on a cascade of chaotic maps, which serves the purpose of sequence generation and random mixing **[1]**. Unlike the other existing generators like chaos-based pseudo-random number generators, the proposed key stream generator not only achieves a very fast throughput, and also passes the statistical tests of up-to-date test suite even under quantization.

The two major differences of the text data and image data are larger size of the image data and the loss on the image data when compression technique is used. An efficient cryptosystem for images is designed based on vector quantization **[2]**. This method can achieve two goals. One is the design of a high security image cryptosystem and the other one is reducing the computational complexity of both the encryption and decryption algorithms.

Chaos is introduced to cryptology and a secret key cryptosystem by iterating a one dimensional chaotic map. It is based on the characteristics of chaos, which are sensitivity of parameters, randomness and sensitivity of initial points of sequences obtained by iterating a chaotic map **[3]**.A cipher text is obtained by the iteration of inverse chaotic map from an initial point, which denotes a plaintext. If the iteration is large, the randomness of the encryption and the decryption function is so large that attackers cannot break the cryptosystem by its statistic characteristics. The cryptosystem is composed by a tent map, which is one of the simplest chaotic maps, by setting a finite computation size avoids a cipher text only attack in addition to the security of the statistical point.

A new image encryption algorithm based on logistic map chaotic function which involves two different replacement approaches to change the value of the pixel without shuffling the image itself. To do that, it is

suggested to use a Pixel Mapping Table (PMT) **[4]**with the random shifting value to increase the uncertainty of the image. After that, the pixels values are modified by using the rows and columns replacement approach. By analysing the algorithm, it is shows that it is strong against different types of attacks and is sensitive to the initial conditions

III. PROPOSED SYSTEM

In this system we have used Logistic maps for pixel permutation of the original and cover images and the pixels of the original permuted image is substituted with the summation of corresponding resultant pixel values of permuted original and cover images.

A. Image Encryption

***Stage 1 - Original and Cover Image Permutation*:** A Logistic Map is generated with a constant value and an initial value which acts as the key. The initial parameters play a major role in greater chaotic behaviour. The range of values to be generated is based on the number of pixels in the image. The generated map is sorted. The whole values are reshaped to the dimension of the image before and after sorting.

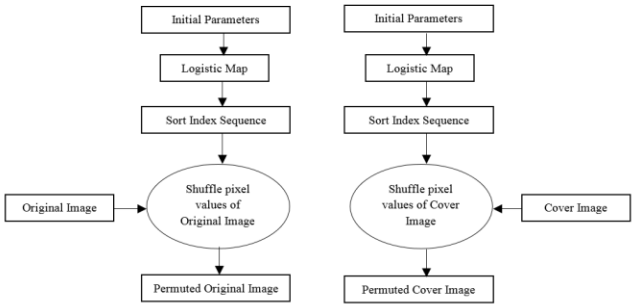


Fig.2. Permuting Original Image and Cover Image

The position change in the values before and after sorting is determined and the same location change is made in the original image in terms of pixels. Thus the permutation is achieved in pixel level. The same step is carried out on another image called cover image. This cover image helps in strengthening the encryption mechanism as the cover image is known only to the receiver using which retrieval of original image is possible.

***Stage 2 – Substitution*:** The permuted pixel values of the original cover image are substituted by the summation of corresponding pixel values of the resultant permuted pixel values of the original and the cover image. This process results in the encrypted image that can be transmitted.

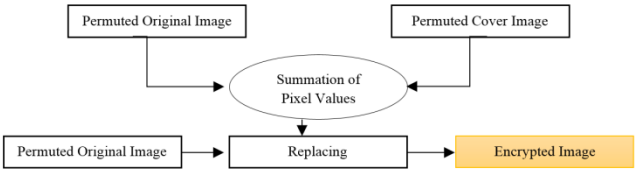


Fig.3. Encryption after substitution

B. Image Decryption

***Stage 1 - Reverse Substitution*:** The receiver holds the cover image and the initial parameters to be fed to the logistic map. The receiver has to remove the cover image from the encrypted image to get the permuted original image. This is possible by generating the permuted cover image at the receiver side and removing the same from the encrypted image resulting in permuted original image.

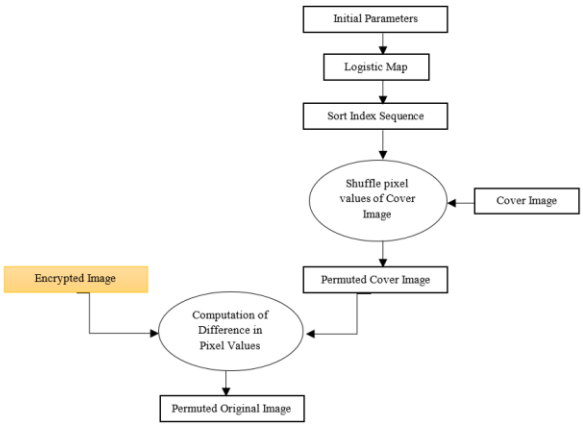


Fig.4. Retrieval of Permuted Original Image

***Stage 2 - Reverse Permutation*:** The logistic map is generated with the same parameters and it is then sorted. The values of original and sorted logistic maps are reshaped to the dimension of the image. Then the permuted original image received is compared with the reversed location of the values in the logistic map arrays. Once they are scrambled then the image would be decrypted and the original image would be obtained.

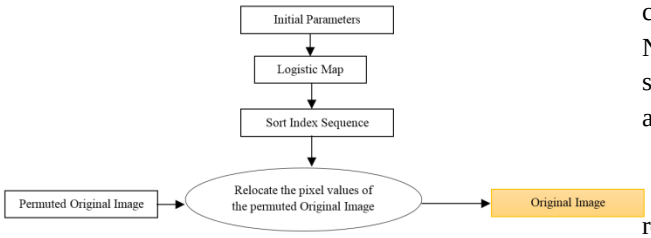
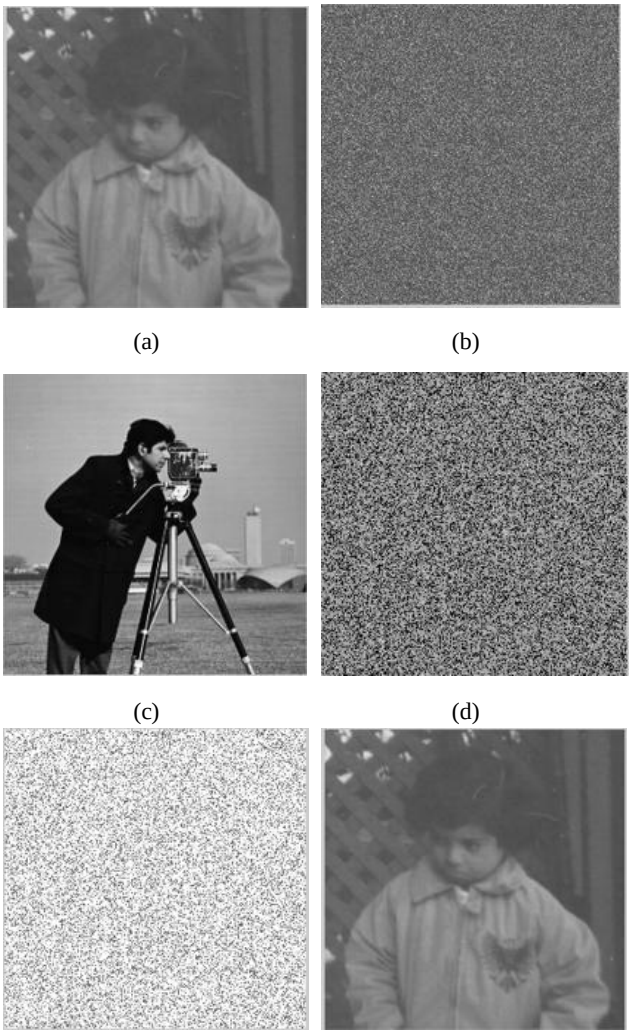


Fig.5. Decryption



(a) (b)

(c) (d)

(e) (f)

Fig.6. (a) Original Image. (b) Original Image after Permutation.
(c) Cover Image. (d) Cover Image after Permutation.
(e) Encrypted Image. (f) Original Image after Decryption.

IV. RESULT ANALYSIS

To secure images from statistical and brute force attacks we are in need of a good encryption techniques. In this section we discussed histogram analysis, correlation coefficient analysis, entropy analysis and NPCR analysis to prove that our proposed encryption system is more secure against most of the known attacks.

***A. Histogram*:** Histogram plays an important role in the security analysis. Histogram illustrates the distribution of pixels in an image. Histogram calculates and displays the distribution of grey values in the active image or selection. The histogram of the encrypted images is significantly different from the histogram of the original images and hence it does not provide any useful information to perform any statistical analysis attack on the encrypted image.

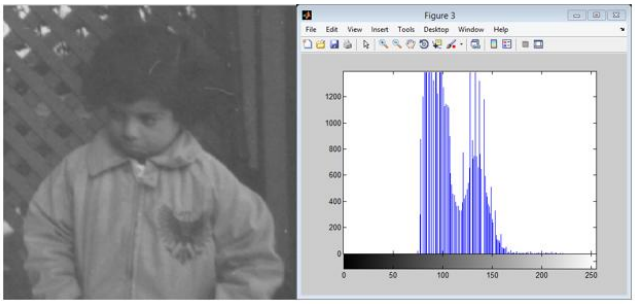


Fig.7. Histogram of Original Image

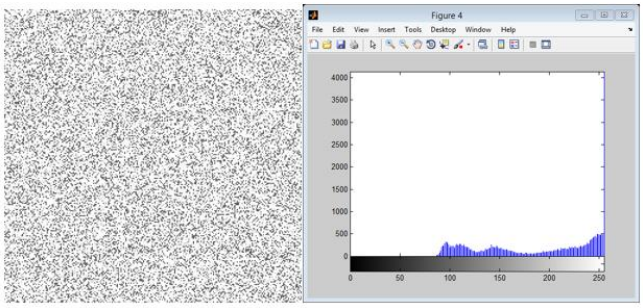


Fig.8. Histogram of Encrypted Image

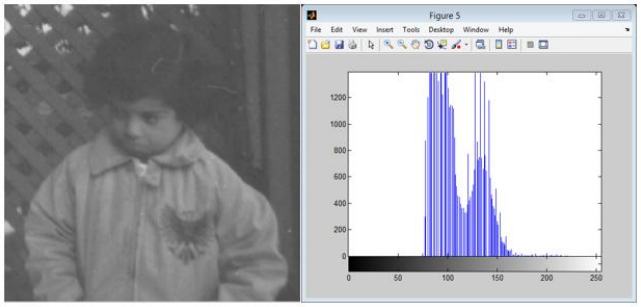


Fig.9. Histogram of Decrypted Image

***B. Correlation Co-efficient*:** Correlation process computes the degree of similarity between two adjacent pixels in an image. Here we compare the correlation coefficients of original image and encrypted image by taking 40,000 selected randomly pairs of horizontally and vertically adjacent pixels using Eq. (2).

Image		Horizontal		Vertical	
Original	Cover	Original	Encrypted	Original	Encrypted
pout	cameraman	0.9893	-0.0025	0.9899	-0.00135
circuit	Pout	0.9752	-0.00093	0.9766	-0.0041
rice	cameraman	0.9107	-0.0035	0.9291	-0.0030

Table 1. Correlation Coefficient Analysis

$$R_{xy} = \mathrm{COV}(x,y)/\sqrt{D(x)}\sqrt{D(y)}, \quad (2)$$

where

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

$$E(x) = \frac{1}{T}\sum_{i=1}^{T}x_i, \quad E(y) = \frac{1}{T}\sum_{j=1}^{T}y_i,$$

$$D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x_i))^2, \quad D(y) = \frac{1}{T}\sum_{i=1}^{T}(y_i - E(y_i))^2,$$

Where x_i and y_i are the adjacent pixels in an image.

***C. Entropy*:** Entropy represents the degree of randomness among the information residing in an image. It describes the distribution of the pixel values present in an image. The entropy of original image, permuted original image and decrypted image should be the same as the encryption process is lossless. The entropy of encrypted image should be lower than that of the original image to ensure high randomness which can be determined using Eq (3)

$$H(s) = -\sum_{i=1}^{2^N-1}\mathbb{P}(s_i)\log_2\mathbb{P}(s_i) \quad (3)$$

Where $P(s_i)$ is the probability of the symbol s_i

	Proposed work			
	Original Image	Permuted Image	Encrypted Image	Decrypted Image
pout	5.7191	5.7191	4.9083	5.7191
rice	6.9712	6.9712	5.0842	6.9712

Table 2. Entropy Analysis

***D. NPCR*:** It is a common measure used to verify the effect of one pixel change over the entire image. This will indicate the percentage of different pixels between two images.

$$\mathrm{NPCR} = \frac{\sum_{i=j=1}^{m,n}D(i,j)}{w \times h} \times 100\%, \quad (4)$$

Where w and h are the image width & height.

$$D(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) = C_2(i,j) \\ 0 & \text{Otherwise} \end{cases}.$$

Where C_1 and C_2 are the two encrypted images corresponding to two original images with a pixel difference. The NPCR value for the proposed system thus obtained is 99.9983 which shows that the proposed encryption algorithm is very efficient (obtained using Eq. (4)).

VI. CONCLUSION

The image encryption is most important for the secure transmission over the internet. A new symmetric encryption scheme using logistic map has been proposed which is immune to attacks like brute force attacks, statistical attacks.

The entropy values of original image and the permuted image shows that the proposed scheme is a lossless one, the NPCR value proves that high pixel change occurs in the encrypted image as a result of a significant change in a pixel and the correlation between the adjacent pixels in the encrypted image is significantly very low when compared with that of the original image. Thus the proposed algorithm is fairly competent. The proposed work can be combined with the Artificial Neural Network which is known for its high perturbation. Better chaotic behaviour can be achieved when combined. This can be applied in the areas where image transmission plays a vital role like Secret Image transmission in Army, Blue print exchange of the Company projects and so on.

REFERENCES

[1] H.S.Kwok, W.K.S.Tang, A fast image encryption system based on chaotic maps with finite precision representation, Chaos Solitons Fractals 32(2007)1518–1529.

[2] C.C.Chang, M.S.Hwang, T.S.Chen, A new encryption algorithm for image crypto systems, J.Syst.Softw.58(2001)83–91.

[3] T. Habutsu, Y. Nishio, I. Sasase, S. Mori, A secret key cryptosystem by iterating a chaotic map, in: Advances in Cryptology, EUROCRYPT'91, in: Lect. Notes Comput. Sci., vol. 547, Springer-Verlag, 1991, pp. 127–140.

[4] HamedRahimov, MajidBabaei, Mohsen Farhadi (2011) 'Cryptographic PRNG Based on Combination of LFSR and Chaotic Logistic Map' Department of Computer Engineering, Shahrood University of Technology, Shahrood, Iran, Applied Mathematics, 2011, 2, 1531-1534.

[5] Mitra, Y. V., Rao, S., & Prasanna, S. R. M. (2006), ' A new image encryption approach using combinational permutation techniques', International Journal of Computer Science, 1, 127–131.

[6] Gonzalez, A.,Woods, A., &Eddins, A. (2004). Digital image processing using MATLAB

[7] William Stallings W. Cryptography and Network Security – Principles and Practice'. New Jersey : Prentice Hall; Fifth edition 2011..

[8] http://in.mathworks.com/help/matlab/examples.html.

[9] http://www.tutorialspoint.com/matlab/.