Design and Implementation of Image Encryption using Chaos Theory

Veena H N
Assistant Professor,
Department of Information Science & Engineering,
East West Institute of Technology, Bengaluru.
hn.veenagowda@gmail.com

Naveen Chandra Gowda
Assistant Professor,
School of Computing and Information Technology,
REVA University, Bengluru-64
ncgowdru@gmail.com

Abstract:-Due to the rise in the use of internet facility for data/information transmission, the data must be kept secured. The data to be transferred can also be an images. So that images being transmitted through the internet must also be kept much secured for gaining the trust from the users. The image encryption can be performed through many ways. The proposed method of image encryption is by mapping with the chaotic maps provided as chaos theory. The original image will be divided in to different blocks, then permute and diffuse separately at the pixel level of each block. Finally combine and diffuse the permuted image as a cipher image. The proposed method also experimented and tested to reach the current need of image encryption to maintain the security among the users.

Keywords: **Image Encryption, Chaotic Maps, Chaos Theory, Permute, Diffusion.**

1. Introduction

The data or the information to be transferred by numerous connection technologies over an internet must be kept secured. The information can also be sent as in image. So the images being sent must be secured enough to reach to exact destination. This kind of information sharing in the form of images is very much used in military, politics, phone banking and any other policing activities. The well-known way of sending them securely is by using the technique of cryptography. The original image is to be encrypted before it is sent, converting the original data to unreadable format using some key is specified as encryption. Then later the specified receiver can decrypt back using the key then converting to readable format.

Implementation of Image encryption can be done by using the different algorithms proposed [1] such as Rivest-Shamir-Adleman (RSA), data encryption standard (DES) advanced encryption standard (AES) and so on. These methods can be well used only for attack identification but insufficient for protecting the images under transmission. So the image encryption can be made protective using chaotic systems [2][3].

Many researchers started working on image encryption using chaotic theory. The algorithm in [4] has shown this by two approximations as first construct the pixel mapping table then later columns and rows will be altered to modify the pixel value. This entire scenario is presented in two levels using quadratic map and Chebyshev map [4]. The authors in [5] also tried to present chaotic baker map and chaotic Lorenz map for image encryption in two stages which are confusion and diffusion. Few other maps are applied and verified in [6] for better image encryption by splitting the original image into blocks of size 8x8 then a 2D cat map and 2Dcoupled logic is applied to generate the random control parameters. Then later a one-dimension logistic map is generated. The logistic map is actually deployed in [7] to generate the key used for permute the pixels of an entire image. The values of the pixels can also be altered using Rossler attractor.

Here we would like to implement an image encryption is by using four chaotic maps. The plain image is divided in to pieces then later map each part to chaotic maps. The detailed process will be elaborated further. The rest of the paper is organized as, section II gives the detailed description about the proposed encryption algorithm.Section III elaborates the experimentalresults conducted. Section IV overviews the analysis of security elements considered here. Finally section V concludes our algorithm in better way for Image Encryption.

2. Proposed Algorithm For Image Encryption.

We make use of different chaotic maps to accomplish the image encryption. Find the index values for every pixel of an original image then map to chaotic maps based on the key element. The proposed algorithm for image encryption is as follows,

Step 1: Consider an original image of size 128x128 as an input.

Step 2: Divide the original image in to blocks each of size 8x8.

Step 3: Apply Cubic map to permute the pixels with in an image block.

The cubic map for any discrete system in nonlinear in fashion [8] can be defined as,

$$f_r(x) = rx_n^3 + (1-r)x_n,$$

Here n is the number of iterations, 256. r is chaotic factor, 3.99. And initial x0 as 0.0215.

Step 4: Apply the Henon map in order to diffuse the permuted pixels within a block.

The Henon map can be used to produce the random numbers, here we use them to map to index values of an image pixels. The map is defined through the [9] equation,

$$X_{n+1} = 1 - aX_n{}^2 + Y_n,$$

$$Y_{n+1} = bX_n,$$

The (a, b) is a random point, here it can be (1.4, 0.3) with number of iterations as 256. The diffusion is operated as XOR operation.

Step 5: Now apply the Quadratic map to permute the individual block of a complete image. The equation for the same is given in [10] as,

$$X_{n+1} = r - (x_n)^2$$

Here n is the number of iterations, 256. r is chaotic factor, 1.999. And initial x0 as 0.0215.

Step 6: Apply the Logistic map to combine and permute all the pixels related to complete image. In the one dimensional system, the logistic map can be described as [11],

$$X_{n+1} = \lambda X_n(1 - X_n),$$

Here λ the chaotic factor, 3.99 and initial x0 as 0.1234 and n as number of iterations, 16384.

Step 7: finally apply the Henon map to diffuse the combine and permuted image pixels in order to produce the output image in the form of cipher-modified format. The number of iterations this time it will be 16384. The combined and permuted image can be diffused using XOR.

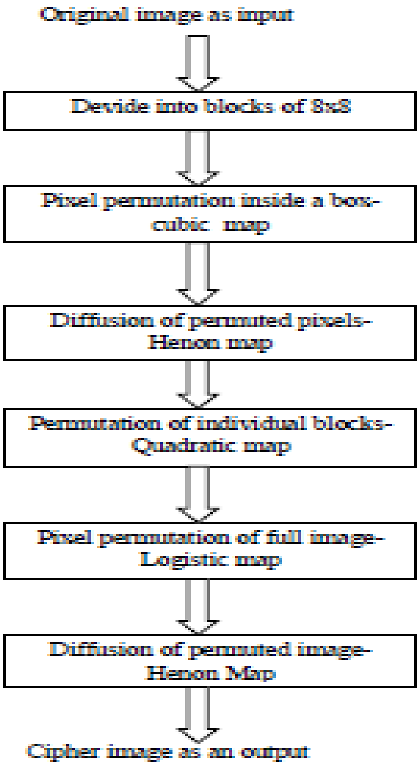
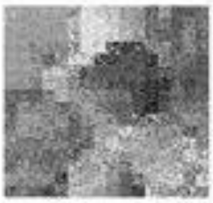
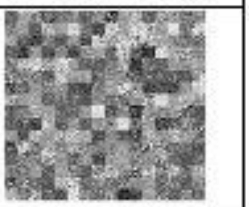

Original image as input
Devide into blocks of 8x8
Pixel permutation inside a box-cubic map
Diffusion of permuted pixels-Henon map
Permutation of individual blocks-Quadratic map
Pixel permutation of full image-Logistic map
Diffusion of permuted image-Henon Map
Cipher image as an output

Figure 1: Proposed Model

3. Experimental Results

The proposed encryption algorithm is carried out in MATLAB workbench. The original input image is considered in the form of gray-scale image. The input image is considered with the size of 128x128 pixels. The following table shows results after every phase of proposed system. The encrypted-decrypted images may be tested for any feature of an image processing, but here we would like to check for security related analysis. So among all the different tests can be made, we tried to test for differential cryptanalysis and sensitivity analysis related to change of key bits.

Table 1: Applying the proposed phases on input image.

Phase	Image
Original Image	
Blocks of permuted pixels	
Diffused permuted pixels	
Permuted blocks	
Permuted pixels with in an image	
Final Cipher image as an output	

4. Analysis Of Security Parameters

a) Differential Cryptanalysis.

The cryptographic analysis is made to identify the occurrence of attacks on the images after encryption. The analysis is on modification of one or more pixels of original image. This can be done in two ways,

I. Avalanche Effect analysis through Mean Square Error: The encrypted image may be altered 50% because of change of single bit the original image. This effect can be best found using mean square error (MSE). The MSE can be found using,

$$\mathrm{MSE} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{\mathrm{i}=0}^{\mathrm{N}-1} \sum_{\mathrm{j}=0}^{\mathrm{M}-1} [\mathrm{C}_1(\mathrm{i},\mathrm{j}) - \mathrm{C}_2(\mathrm{i},\mathrm{j})]^2$$

The equality of images varies when the MSE value is more than 30dB [12]. But the MSE of the proposed model is about 48.45dB.

II. Number of modifying pixel rate: The ratio of the number of pixels modified to total number of pixels can be found using NPCR [13].

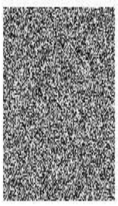
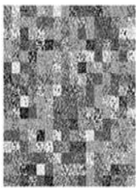
$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

The ratio between numbers of modified pixels to number of original pixels in the original image in the proposed system is about 99.66%, comparatively better than existing methodology [14], where it was 99.12%.

b) Sensitivity Analysis (SA) of Used Key

The key to be used in the encryption is precious, a small change of bits in the key leads to huge variations in the encrypted result. The decrypted image will never be same as original if there exists a small change in the key [15]. Our chaotic maps are well defined to address these kind of control parameters. The following table shows the variations.

Table 2: Sensitivity Analysis

Original Image	**Encrypted Image**	**Decrypted Image with actual key**	**Decrypted Image when one of the bit in key is changed**
			

Conclusion

The way of Image Encryption is designed using different chaotic mapping methodologies. Here the pixel values of an image are permuted and analyzed for different the gray values pixels of an original image. The basic plain image is divided into individual blocks, each of 8×8 size and then the pixels are permuted for every block separately and finally combined together as a cipher image. This complete process is done by using the different chaotic maps. The algorithm is also evaluated for better results compared to existing methodology of image encryption.

This can be enhanced in future to implement and experiment for the time complexity based on the existing Image Encryption Techniques.

References

1. M. R. C. Mansi, "An Audio Multiple Shuffle Encryption Algorithm," International Journal Of Engineering And Computer Science, vol. 4, no. 9, 2015.
2. H. M. I. M. F. S. N.F.Elabady, "Image encryption based on new one-dimensional chaotic map," in Engineering and Technology (ICET), 2014 International Conference, 2014.
3. B. Dr.S.Ramahrishnan, "Image Encryption Using Chaotic Maps in Hybrid Domain," International Journal of Communication and Computer Technologies, vol. 2, no. 5, 2014.
4. H. M. A.-N. A. M. Al-Najjar, "Image Encryption Algorithm Based on Logistic Map and Pixel Mapping Table," in the 12th International Arab Conference on Information Technology, 2011.
5. D. S. A.Anto Steffi, "Modified Algorithm of Encryption and Decryption of Images using Chaotic Mapping," International Journal of Science and Research (IJSR), vol. 2, no. 2, 2013.
6. M. S. A. Musheer Ahmad, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping," International Journal on Computer Science and Engineering, vol. 2, no. 1, 2009.
7. A. M. A.-N. Hazem Mohammad Al-Najjar, "Multi-Chaotic Image Encryption Algorithm Based on One Time Pads Scheme," International Journal of Computer Theory and Engineering, vol. 4, no. 3, 2012.
8. X. Liu, "Analysis and Improvement for Image Encryption Algorithm Based on Multiple Chaotic Mapping,"The Open Automation and Control Systems Journal, vol. 7, 2015.
9. N. S. R. &. A. KUMAR, "IMAGE ENCRYPTION USING HENON CHAOTIC MAP WITH BYTE SEQUENCE," International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), vol. 3, no. 5, 2013.
10. H. E. H. A. S. E. E. F. E. A. E.-S. Noha Ramadan, "Chaos-Based Image Encryption Using an Improved Quadratic ChaoticMap," American Journal of Signal Processing, vol. 6, no. 1, 2016.
11. Y. C. Dongming Chen, "A Novel Image Encryption Algorithm based on Logistic Maps,"Advances in Information Sciences and Service Sciences, vol. 3, no. 7, 2011.
12. S. M. M. S. M. R. M. Benyamin Norouzi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," Multimedia Tools and Applications, vol. 71, no. 3, 2014.
13. S. O. H. A. A. Jawad Ahmad, "An Experimental Comparison of Chaotic and Non-chaotic Image Encryption Schemes," Wireless Personal Communications, vol. 84, no. 2, 2015.

14. F. A. Jawad Ahmad, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes," International Journal ofVideo & Image Processing and Network Security IJVIPNS-IJENS, vol. 12, no. 4, 2012.
15. H. K. Y. Z. J. Z. X. Cao Guanghui, "Chaotic Image Encryption Based on Running-Key Related to Plaintext," Hindawi Publishing Corporation Scientific World Journal, vol. 2014.