International Journal of Computer Science and Business Informatics

IJCSBI.ORG

A Hybrid Cryptosystem for Image using Chaotic Mapping

Nidhi Sethi
Assistant Professor
DIT University
Dehradun-248001

Sandip Vijay
Proffessor
DIT University
Dehradun-248001

ABSTRACT

In this paper, we have proposed a new method to develop a safe image encryption techniques using a Chirikov Standard Map and Modified Logistic Map. Here, Chirikov standard map is used to shuffle the pixels of the image and hence creating the confusion and modified logistic mapping is used for pixel permutation. Since this scheme of encryption is symmetric, so the transportation of key is an issue. This issue is resolved in the proposed work by image steganography using a new proposed algorithm. Hence in all, the proposed technique consists of two steps. In the first step, the original image is encrypted using chaotic mapping. In second step the secret keys used for encryption and authentication are embedded in the encrypted image. The result shows that the proposed method is resistant to statistical attack, differential attack, brute force attack and histogram analysis attack.

Keywords

Chirikov Standard Map, Image encryption, Modified Logistic Map, steganography, symmetric.

1. INTRODUCTION

With the ever increasing need of the communications which is mediated by the technology, and augmented awareness of the importance of interception issues, technology and its compromise are at the heart of the security. Every kind of data like text, image, and video is at stake when it is transmitted over internet. So encryption of data is one of the possible solutions to this problem. Image encryption has its application in internet communication, in areas like multimedia systems, medical imaging, telemedicine, and military communication.

Chaotic maps are nowadays vitally used for image encryption because of their sensitivity towards initial conditions. These initial conditions are incorporated as secret keys for image encryption. The chaotic encryption schemes are used as symmetric encryption algorithm. Hence the problem of transportation of keys is difficult. The proposed had tried to improve the security features of the algorithms and resolve the problem of transmission of secret key.

The proposed encryption technique consists of two phases. In the first the original image is enciphered using chirikov map and modified logistic map. The shuffling of the pixels is done by chirikov map and the pixel permutation is done by modified logistic mapping. In the second phase the secret keys used for encryption and authentication are embedded in the encrypted image. The stego key used for steganography is exchanged by public key cryptography. The proposed algorithm is tested for several images and the results are given in the experimental results section.

2. LITREATURE REVIEW

Information security is the hot topic of research for decades to deal the prevailing security requirements. Traditional encryption schemes such as DES,,T-Des , AES are not suited to build the cryptosystem for digital images , this is due to the inherent features of the images and high redundancy. J. M. Blackedge et al. [2] have proposed a multilevel blocks scrambling is employed to scramble the blocks of coefficients which requires high computation. The control parameters of the scrambling are randomly generated from the secret key dependent. The key stream used to encrypt the scrambled image is extracted from the chaotic map and plain image.

W Puech et al. [10] have explained and reviewed the security, performance and reliability issues, in respect to the combination of various chaos based symmetric key cryptosystems. Logistic, Henon, Tent, Cubic and Cheyshev mappings have been used for the enhancement of the key space. Chengqing Li et al. [11], have reviewed four chaos based image encryption schemes that were proposed .He found that all, the four schemes can be put under one umbrella which comprises of two basic parts: permutation and combination of pixel value with ciphertext feedback function. Hence following security problems were found: 1) the schemes are not sensitive to change of plain-image; 2) the schemes are not sensitive to change of secret key; 3) there exist a serious flaws of diffusion function; 4) the schemes can be broken with no more than $[\log_l(MN)+3]$ chosen images when iteration number is equal to one, where MN is dimension of image. Chong Fu et.al [15] have used , Chirikov standard map , to decor relate the strong relationship among adjacent pixels hence employed to shuffle the pixel positions of the plain image. After the decor relating the pixels, the pixel values are modified sequentially to confuse the relationship between cipher image and plain image.

2.1 Chirikov Map

The Chirikov map ofetly called standard map is an area preserving chaotic map. The equation of this map is as below:

$$Y_{n+1=}(Y_n + K\sin 2\pi\ X_{n+1}/N)\text{mod } N$$

$$X_{n+1=}(X_n + Y_n)\text{mod } N$$

K is dimensionless parameter that influences the degree of chaos. As the K increases the ergodicity also increases. The value of K can be used as a secret key for confusion, N XN is the size of the image. Because of the simple mathematical operation, it is very efficient to shuffle the pixels of the plain image using this map.

2.2 Modified Logistic Map

The 1D logistic map is discrete time analogue of population growth model. It is a non-linear chaotic discrete system that shows random behavior. The equation of logistic map is below:

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

The equation for modified logistic map is derived from the above equation .The equation for modified logistic map is

$$Y_{n+1}=\lambda\ Y_n(1-\ Y_n)(\ 1-\ (Y_n)^2/5)$$

Where Y_n is the intial value which is used as a secret key in this algorithm , λ is the control parameter which affects the randomness and n is the number of rounds .As the value of the λ increases the randomness(number of periods) increases .λ lies in the range.

3. PROPOSED ALGORITHM

The proposed image encryption algorithm has two major steps. Firstly, the image is encrypted and converted into the unreadable form .This level of encryption is achieved by disturbing the correlation among the adjacent pixels as the image data have strong correlations among the neighbouring pixels. For image security and secrecy, it is the primarily requirement. This correlation is disturbed by Chirikov Standard map. The shuffled image now undergoes the process of confusion. The resultant image is divided into blocks and each block employ the specific calculation in which makes every pixel dependent on each other. Then the stage of diffusion comes , where the pixel values of the converted image are changed by employing a modified 1 D Logistic map. The control parameters of logistic map are the control parameters of permutation. The shuffling effect obtained after a number of iterations of Chirikov standard map. In the algorithm, these control parameters are randomly generated through the chaotic sequences obtained from modified 1D Logistic map and Chirikov standard map. The second step is steganography. All secret keys used in the encryption process are embedded in the encrypted image itself. Here also one secret key is incorporated which is exchanged by the help of ElGamal key exchange protocol. The sender encrypts the final key with receiver's public key and receiver decrypts the message using its own private key.researchers should be informed that even if they are writing ideas from other authors in their own words, they should still reference the work [10].

Steps of Proposed Algorithm

Step 1: Input the original image

Step 2: Authentication process using key 5

Step 3: Shuffle the image using chirikov mapping with 'n' iterations .The key used is key1 and key 2.

Step 4: After the shuffling within the image, there is a step is there to shuffle within the block of size 8X8.

Step 5: Create a matrix using modified logistic mapping and perform xoring of the shuffled image with the generated matrix. This is diffusion of pixels. The key used is key3 and key 4.

Step 6: Embed the secret keys in the encrypted image using sender's public key named key 6.

Steps of embedding the keys

Step 1: Divide the cover image into blocks.

Step 2. Calculate the median for each block M.

Step 3. Calculate the square root of median for each block.

S=fix(sqrt(M+stego key))

Step 4. Calculate the difference value for each two consecutive pixels Pi and Pi+1.

Di=Pi-Pi+1

Step 5. If Di>=S then embed the message in Pi.

(go to step 2)

Step 6. Split each pixel Pi into two equal parts.

Step 7. Make the least significant four bits of the pixel to zeros.

Step 8. Split the Message into two equal parts.

Step 9. Make the most significant four bits to the zeros.

Step 10. Apply bitxor operation on the two results.

The recipient uses the extraction algorithm i.e. reverse order of embedding algorithm to extract the secret message from the stego-image using receivers key.

Extraction, Decompression and Decryption: Using the above algorithm in reverse order, the original image can be retrieved. The satisfactory security level with low computational complexity is achieved .Thus we can say, that the proposed algorithm proves to be an appropriate choice for real-time safe and secure image transmission.

SENDER'S SIDE ***RECEIVER'S SIDE***

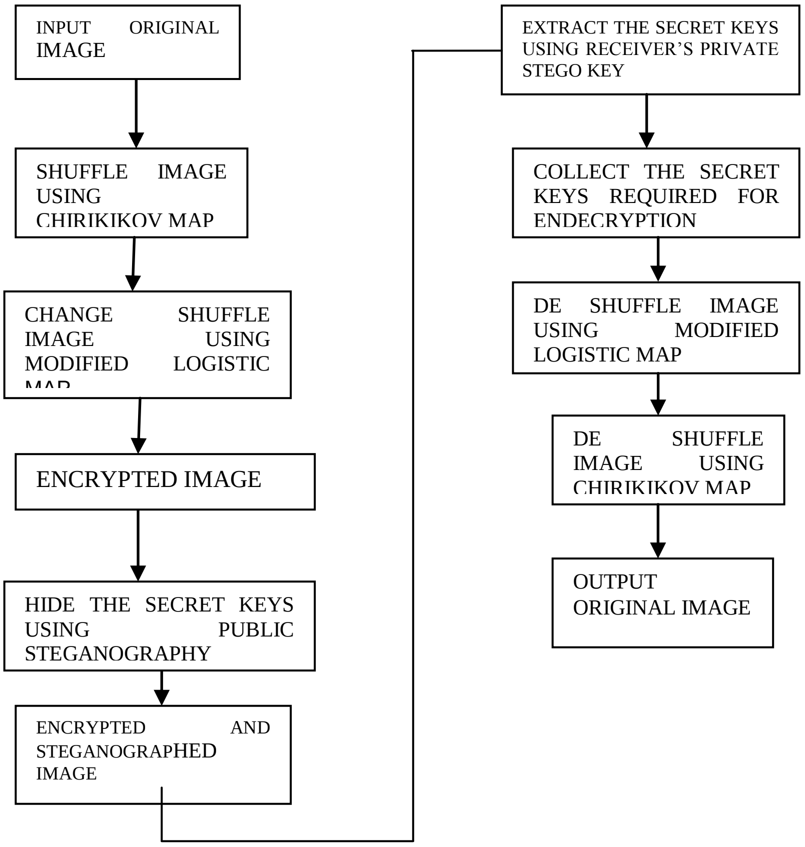

INPUT ORIGINAL IMAGE
SHUFFLE IMAGE USING CHIRIKIKOV MAP
CHANGE SHUFFLE IMAGE USING MODIFIED LOGISTIC MAP
ENCRYPTED IMAGE
HIDE THE SECRET KEYS USING PUBLIC STEGANOGRAPHY
ENCRYPTED AND STEGANOGRAPHED IMAGE
EXTRACT THE SECRET KEYS USING RECEIVER'S PRIVATE STEGO KEY
COLLECT THE SECRET KEYS REQUIRED FOR ENDECRYPTION
DE SHUFFLE IMAGE USING MODIFIED LOGISTIC MAP
DE SHUFFLE IMAGE USING CHIRIKIKOV MAP
OUTPUT ORIGINAL IMAGE

Figure 1: Flowchart of the encryption and decryption process

4. RESULTS AND DISCUSSION

In this proposed work the combination of Chirikov map and Modified Logistic Map has been used. To demonstrate the efficiency of the algorithm ,the results of various tested images is shown below. It is found that this new scheme has resistance to statistical attacks and brute force attack. The resistance to chosen plain text and chosen cipher text is also achieved to an ideal stage.

Total number of Keys: 06;

Key1: A unique number used as initial vector for Chirikov mapping **Key2**: A unique number for number of iterations the map will shuffle. **Key 3**: Fed to random number generator for further processing **Key 4:** Initial parameter for modified logistic mapping ; **Key 5**: lemda:(3<key3<4)**Key 6:** A unique number required for authentication.

4.1 Experimental Results

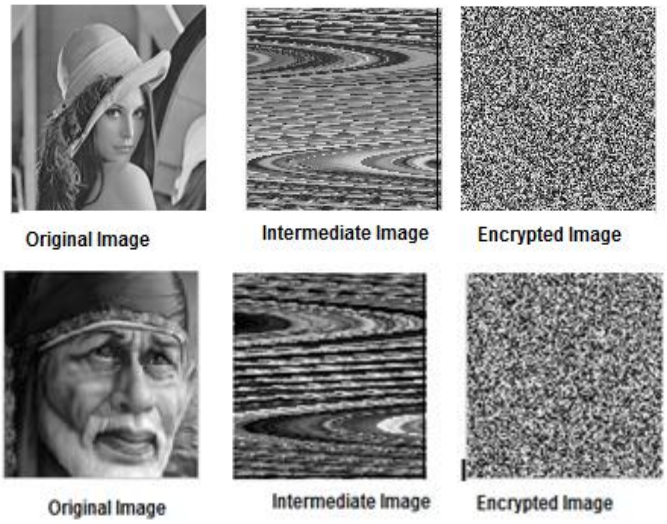


Figure 2: Image after and before encryption

4.1.1 Key Analysis:

- Key Sensitivity **:**A good cryptosystem should be sensitive to a small change in secret keys i.e. a small change in secret keys in decryption process may results into a completely different output image. Our proposed encryption algorithm is sensitive to a very small change in the secret keys. If we change a little (10^{-14}) in any of the initial conditions then the decrypted image is completely different and in un-understandable form

- Key Space: Key space is defined as the total number of different keyset/keys that can be used in the cryptosystem .A cryptographic system should be sensitive to all secret keys. There are total four initial conditions, two of Chirikov map and two of logistic map used in the algorithm .All these four intial conditions are used as secret keys of encryption and decryption. In this situation, the precision of each key is 10^{-14}, the key space size is $(10^{14)8}$ i.e. 10^{112}, which is extensively large enough to resist the exhaustive attack.

4.1.2 Statistical Analysis:

Many attacks can be done which are based on the statistical analysis .Statistical analysis has been performed on the test images to demonstrate the bad correlation among the pixels of the encrypted images. The following test has been performed like PSNR, MSE, MAE, information entropy and Correlation coefficient. The results below show that there is negligible correlation between pixels of the encrypted image in comparison to original image.

- **Mean Squared Error** is the average squared difference between original input image and a encrypted image. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total number of pixels.
- **Peak Signal-to-Noise Rat**io is the ratio between the original image and the encrypted image. PSNR is calculated in decibels.[5] The higher the PSNR, the closer the encrypted image is to the original. For good encryption scheme the PSNR should be as low as possible.
- **MAE** is the Mean absolute error. It is used to measure how close predictions are to the eventual outcomes. The larger the value of MAE better is the image security.
- **Correlation Coefficient Analysis**: To estimate the encryption quality of the proposed encryption algorithm , the correlation is used .For highly correlated image the correlation coefficients are almost 1 and for encrypted images the correlation coefficients is almost 0.
- **Information Entropy**: Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon [14]. Information entropy is defined to express the degree of uncertainties in the system. The formula for calculation entropy *H*(*m*) of a message *m is:*

$$H(s)=-SUM(p(s_i)\log_2 p(s_i))$$

4.1.3 Differntial Attack

Differential attack /cryptanalysis is a common name of attacks/cryptanalysis which is generally done to block ciphers which are working on binary sequences. In this type of attack the dependency of cipher image and input image is analyzed.

- **NPCR:** NPCR is Number of pixel change rate. NPCR concentrates on the absolute number of pixels which changes value in differential attacks.

$$D(i,j)=\begin{cases} 0 \; if \; C^{1}(i,j) = C^{2}(i,j) \\ 1 \; if \;\; C^{1}(i,j) \neq C^{2}(i,j) \end{cases} \qquad \ldots\ldots\ldots..(1)$$

$$NPCR=\frac{\sum_{i,j}D(i,j)X100\ \%}{T} \qquad \ldots\ldots\ldots.(2)$$

Here symbol *T* denotes the total number pixels in the cipher image. Table II shows the values of NPCR during experimentation .If the value of NPCR is near 0.99, it is treated as good.

Table 1: Results of encryption without transformation

	Baba	**Lena**
PSNR	50.117	51.414
MSE	0.6329	0.814
Entropy (Encryp)	7.9894	7.9881
Correlation Coeff.	-0.0164	-0.0115
MAE	89.03	72.794

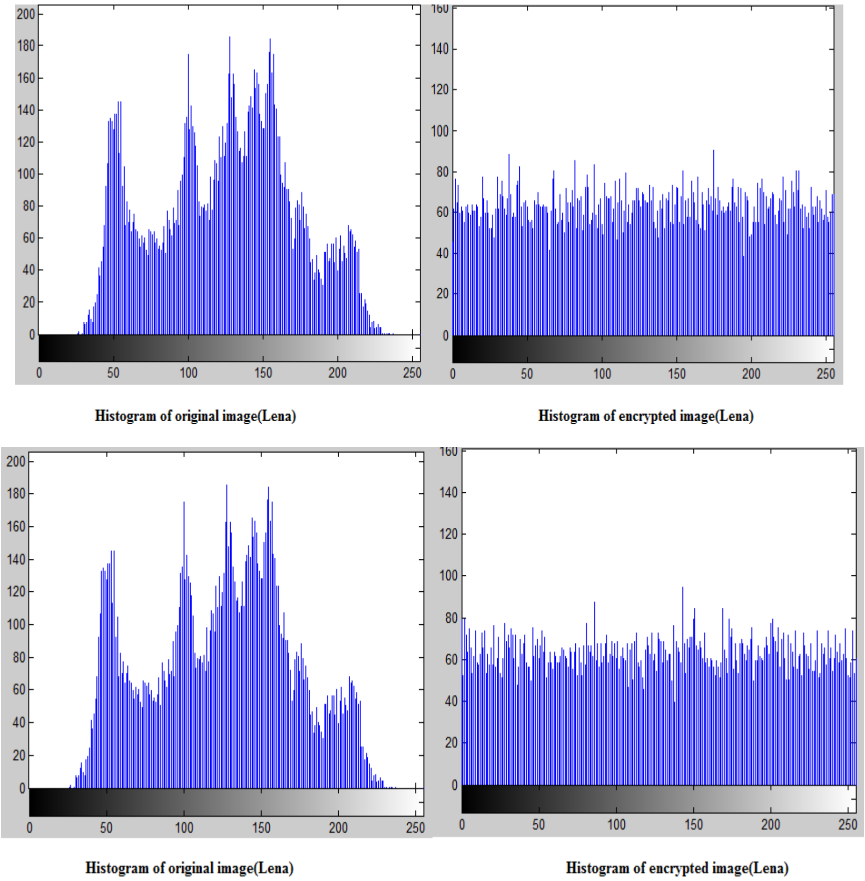
Table 2: Result for NPCR values without transformation

S. No	**Name of Image**	**NPCR value**
1	Lena	0.9954
2	Baba	0.9932

Table 1 shows the effect of transformation on image along with the encryption. The result is calculated in terms of PSNR, MSE, MAE, Correlation and entropy. Table 2 shows the NPCR values for two images Lena & Baba for encrypted image. We can therefore conclude that if there was an additional day in one week, it should be five!

4.1.4 Histogram Analysis

The histograms of enciphered images were analyzed and it was found that the histograms are usually uniform. This property makes statistical attacks difficult in images .The test on lena and baba images are shown below:



Histogram of original image(Lena)

Histogram of encrypted image(Lena)

Histogram of original image(Lena)

Histogram of encrypted image(Lena)

Figure 3: Histogram of original and encrypted image

Figure 3 shows that the histogram of original and encrypted image for image lena and baba. It is clearly seen from the histogram of encrypted image that the intensity of all the pixels is almost same, which means the intruder is unable to identify the image by histogram analysis attack.

5. CONCLUSIONS

The paper aims at developing a secure algorithm for image encryption. The encryption algorithm use two concepts, i.e., confusion and diffusion which is also called substitution and permutation among the pixels of the gray scale image. To perform the confusion in the plain-image's pixels, a Chirikov map is used and finally modified logistic map is used to performing the diffusion. Two different images have been used for test and the results are mentioned above. We concluded that the algorithm is resistant to statistical attacks and brute force attack. The resistance to chosen plain text and chosen cipher text is also to an acceptable limit.

REFERENCES

[1] P. Raviraj and M. Y. Sanavullah, "The modified 2D-Haar Wavelet Transformation in image compression"Middle East Journal of Scientific Research, (2007), Vol: 2, Issue: 2, pp 73-78, ISSN 1990.

[2] Jonathan M. Blackedge, Musheer Ahmed ,Omar Farooq "Chaiotic image encryption algorithm based on frequency domain scrambling", School of Electrical Engineering systems Articles, Dublin Institute of Technology, (2002).

[3] G. K. Kharate, A. A. Ghatol and P.P.Rege "Image Compression Using Wavelet Packet Tree", ICGST-GVIP Journal, (2005), Issue (7).

[4] David F. Walnut, "Wavelet Analysis", Birkhauser, (2002), ISBN-0-8176-3962-4.

[5] Musheer Ahmed, M. Shamsher Alam **"**A new algorithm of encryption and decryption of images using chaotic mapping**"** International Journal on computer science and engineering, (2009), Vol. 2(1), pp 46-50.

[6] J. Fridrich **"S**ymmetric ciphers based on two-dimensional chaotic maps" International Journal of Bifurcation and Chaos. (1998), Vol.8, pp. 1259-1284.

[7] **L**inhua Zhang, Xiaofeng liao , Xuebing Wang "An image encryption approach based on chaotic maps" chaos, solitons and fractals, (2005)vol.24 ,759-765.

[8] **S**higuo Lian , Jinsheng Sun, Zhiquan Wang **"**A block cipher based on a suitable use of the chaotic standard map"chaos solitons and fractals, (2005), Vol.26, ,117-129.

[9] Ahmed T A1-Taani and Abdullah M. AL-Issa "A Novel Steganographic Method For Gray-Level Images". World Academy Of Science, Engineering and Technology,(2009).

[10] Puech, W. and Rodrigues, J. M., "A New Crypto- Watermarking Method for Medical Images Safe Transfer". In The 12th European Signal Processing Conference, (2004), pp. 1481-1484.

[11] Chengqing Li, "On the security of a class of Image Encryption Scheme", IEEE International Symposium on Circuit & System, ISCAS, Department of Electronics Engineering, University of Hong Kong , (2008), pp. 3290-3293.

[12] S. K. Muttoo, Sushil Kumar **"**Data Hiding in JPEG Images**"** BVICAM'S International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi, (2008).

[13] Microslav Dobsicek,"Modern Stegnography" 8th International Student Conference on Electrical Engineering FEE CTU, 2004.

[14] C.E. Shannon"Communication Theory of Secrecy Systems," *Bell Syst Tech J*, (1949)), Vol. 28, pp. 656–715.

[15] Chong Fu, Jun-jie Chen,Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy", (2012) OSA, Vol. 20, No. 3 / OPTICS EXPRESS 2363.