Efficient Image Cryptography using Modified Chaotic Map with Matrix Operations

Priyangi Trivedi[1], Prof. Rishi Sharma[2]

[1]*M. Tech. Scholar,* [2]*Research Guide*

Department of Electronics and Communication, OIST, Bhopal

Abstract - The image cryptography is the technique to hide the sensitive information present in the images. Several techniques has been proposed to do the same thing. In this paper to achieve the encrypted image form an image we have implemented modified chaotic map and the matrix operation. The proposed algorithm has multi-level cryptography stages and it will significantly enhance the security of the cryptographic system. The whole algorithm works faster than the previous work and the works in both ways to get encrypted image as well as original image from encrypted image. The optimum time achieved for encryption process is 0.05570 seconds and for decryption process it takes about 0.3335 seconds for image size of 100x100.

Keywords - Chaotic Map, Matrix Operations, Cipher Image, Cryptography.

I. INTRODUCTION

Cryptography is the science of hiding information which can be revealed only by legitimate users. It is used to ensure the secrecy of the transmitted data over an unsecure channel and prevent eavesdropping and data tampering. Another field called 'cryptanalysis' concerns with attacking and decrypting these ciphers.

Many cryptography schemes were proposed and used for securing data, some use the shared key cryptography, while some others use the public key cryptography (PKC). The shared key cryptography is a system which uses only one key by both sender and receiver for the purpose of encrypting and decrypting messages. On the other hand, public key cryptography uses two keys, namely private-key and public-key. To encrypt a message in the public key scheme, the public-key is used, while the private-key is used to decrypt it.

As compared to the shared key cryptography, the public key cryptography is rather slow. However, the public-key cryptography can be used with the shared key cryptography to get the best of both. In particular, the public key cryptography has many advantages over the shared key; among others, it increases the security and convenience where distributing the private key to other party is not required.

Cryptography Basics

Cryptography is based on hard mathematical problems like prime number factorization, Elliptic curve discrete logarithm problem and discrete logarithm problem. The idea behind these problems is the computation can be easily done in one direction, but it is very difficult in the opposite direction. It is not difficult to find the result of multiplying two numbers, but it is extremely challenging to find prime factors of a number. Thus, cryptography is concerned with the design and the analysis of mathematical techniques which can offer secure communications in the presence of malicious adversaries. It is an area which is concerned with the transformation of data for security reasons.

Before moving further, these are a number of terms which are commonly associated with cryptography:

Plaintext: The message which is transmitted to the recipient.

Encryption: The procedure of changing the content of a message in a way that it conceals the real message.

Cipher text: The output which is produced after encrypting the plaintext.

Decryption: The reverse function of encryption. It is the process of retrieving the plaintext from the cipher text.

Security Requirements

There must be some security services to secure the communications, to prevent some security issues such as eavesdropping.

Cryptography provides the following security services:

Confidentiality: A service which keeps information accessible only to those who are authorized to access this information. The service contains both protection of all user data which are being transmitted between points and likewise, the protection of the traffic flow analysis.

Integrity: A service which ensures that only authorized users who are capable of writing, deleting of the transmitted information.

Authentication: A service which a receiver determines its source to confirm the sender's identity by using something that you have or you know. Normally, it is done by using the sender public key. It is the same integrity provided by digital signature.

Non-repudiation: It ensures the sender and receiver from denying the sending or receiving of a message and the authenticity of their signature. Typically, it is provided by digital signature.

II. PROPOSED METHODOLOGY

In below figure the proposed system is explained in major blocks in which the system is divided. The major blocks are in the sequence i.e. Separate Layers, Matrix Operation on Layers, Mixing Layers, Applying Chaotic map, Combining Layers these are the major functional blocks performing for the process of Encryption.

Fig. 2.1 Block Diagram of Encryption Process

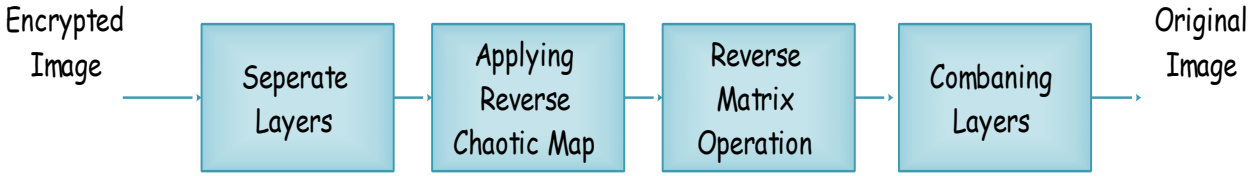


Fig. 2.2 Block Diagram of Decryption Process

Now the below figure proposed system is explained in major blocks also. The major blocks are Separate Layers, Applying reverse chaotic map, reverse matrix operation, combining layers shows the Decryption process of system where we take encrypted image file and performed decryption process and got the original image file.

The below system is implemented on simulation tool and the flow of execution of algorithm is shown in below figure.

Flow Chart- Encryption Process

The flowchart of proposed Encryption approach is given in the figure below. The steps are as follows:

a. *Start of simulation*
b. *The system need an original image to Encrypt*
c. *For further process separate Layers of Image*
d. *After separation process apply Row and Column shift*
e. *Now mixing layers of image*
f. *Applying Modified Chaotic map*
g. *Then combine the layers and save them*
h. *Calculate the encryption time*
i. *End the process*

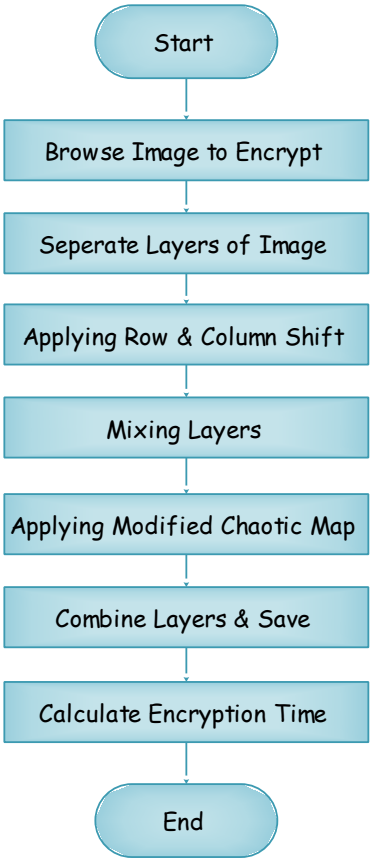


Fig. 2.3 Flow Chart of Encryption Process

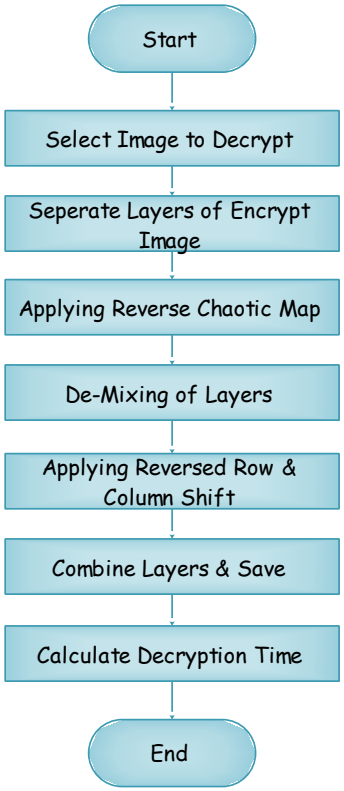


Fig. 2.4 Flow Chart of Decryption Process

After performing encryption process we proceed to next decryption process.

The flowchart of proposed Decryption process is given in the figure below. The steps are as follows:

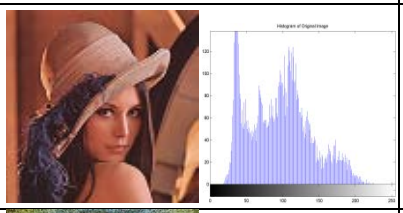
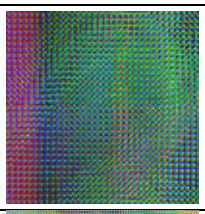
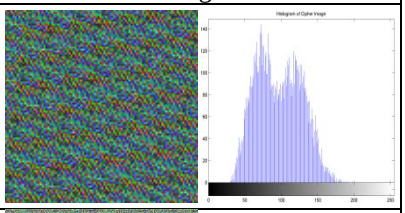
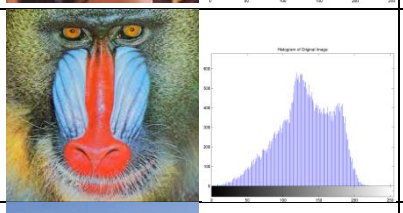
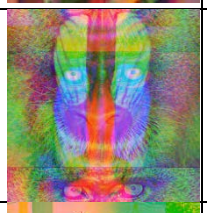
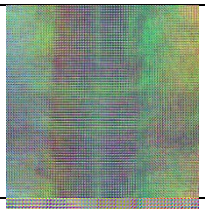
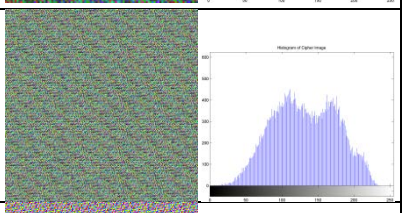
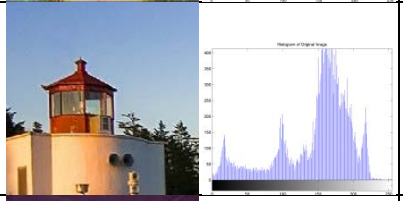
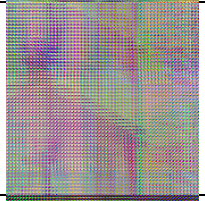
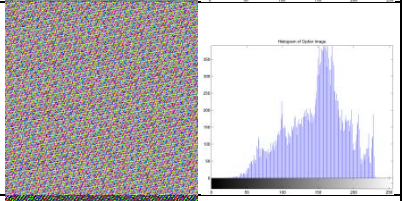
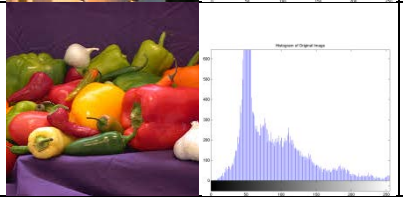
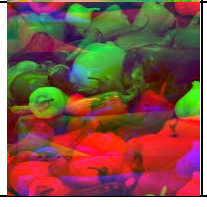
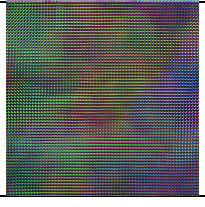
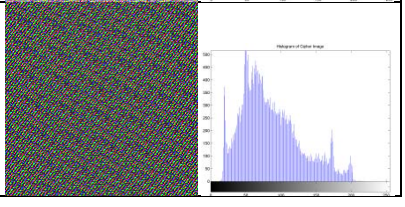
Flow Chart- Decryption Process

a. *Start of simulation*
b. *The system need an Encrypted image to Decrypt*
c. *In this step separate Layers of Encrypt Image*
d. *Now applying Reverse Chaotic Map*
e. *Then apply de-mixing of layers*
f. *And applying reversed Row and Column shift*
g. *combine the layers and save them*
h. *Calculate the Decryption time*
i. *End the process*

III. SIMULATION RESULTS

The proposed system is explained in the previous system implemented with the help of simulation tool and outcomes of the methodology are shown in below table. We have taken different images and shows original images and histogram of these original images. In the blow represented table the column shows different operations of the process and we can see the effect on that particular image of that operation such as matrix operation, mixing layers, encrypted Image (Chaotic Map) and their Histogram.

Table 1: Cryptography Stages and respective outputs of proposed methodology

Image	Original Image& Histogram	Matrix Operation	Mixing Layers	Encrypted Image (Chaotic Map) & Histogram
Lena				
Baboon				
Tower [1]				
Peppers				

The table: 2 shows the summary of images with respective Encryption and Decryption time and size of particular images where we can compare the size deference between images and encryption and decryption time which is in second.

Comparison Table

Table2: Summary of Images with Respective Encryption and Decryption Time

Image	Size	Encryption Time (sec.)	Decryption Time (sec.)
Lena	100x100	0.05570	0.3335
Baboon	225x225	0.21077	3.2639
Tower [1]	***170x170***	***0.11823***	***0.5322***
Peppers	194x194	0.14825	2.3686

The table: 3 show the comparison of encryption and decryption time between proposed system and existing also.

Table3: Comparison of Encryption and Decryption Time

Methodology	Encryption Time (sec.)	Decryption Time (sec.)
Proposed	***0.11823***	***0.5322***
Existing [1]	0.577	10.161

IV. CONCLUSION AND FUTURE SCOPE

The proposed image cryptographic technique is having better speed and performance as compared to the previous [1] technique and even better for bigger images also. The proposed technique has less complexity than the existing work and robustness is better. From the outcomes it can be conclude that the encrypted image is not even unreadable even untraceable also without the knowledge of cryptography algorithm. For advancement in the future methodologies this technique can be integrated with other techniques in a series manner because it takes less time to encrypt image and results would be having higher level of security and robust in several manner.

REFERENCES

[1] N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal, "Elliptic Curve Cryptography for ciphering images," Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on, Visakhapatnam, 2015, pp. 1-4.

[2] L. Chen, X. Chen and Z. Peng, "A Novel Public Key Encryption Scheme for Large Image," 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, 2014, pp. 955-960.

[3] S. Sowmya and S. V. Sathyanarayana, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)," Contemporary Computing and Informatics (IC3I), 2014 International Conference on, Mysore, 2014, pp. 1345-1350.

[4] N. Padmapriya, P. Elamathi and P. Kanimozhi, "Multi image hiding using joint transform digital holography," Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on, Ramanathapuram, 2014, pp. 1497-1501.

[5] Baheti, L. Singh and A. U. Khan, "Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System, and Authentication Using Neural Network," Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, Bhopal, 2014, pp. 664-668.

[6] D. E. M. Ahmed and O. O. Khalifa, "Robust and Secure Image Steganography Based on Elliptic Curve Cryptography," Computer and Communication Engineering (ICCCE), 2014 International Conference on, Kuala Lumpur, 2014, pp. 288-291.

[7] S. Maria Celestin Vigila and K. Muneeswaran, "Elliptic curve based key generation for symmetric encryption," Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on, Thuckafay, 2011, pp. 824-829.

[8] K. Gupta, S. Silakari, R. Gupta and S. A. Khan, "An Ethical Way of Image Encryption Using ECC," Computational Intelligence, Communication Systems and Networks, 2009.CICSYN '09. First International Conference on, Indore, 2009, pp. 342-345.

[9] V. Mehan, R. Dhir and Y. S. Brar, "Secure electronic passport certification using re-water marking," Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, 2013, pp. 371-375.

[10] T. N. Shankar, G. Sahoo and S. Niranjan, "Image Encryption for mobile devices," Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on, Ramanathapuram, 2010, pp. 612-616.

[11] Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang and Mengmeng Wang, "Digital image encryption algorithm based on pixels," Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on, Xiamen, 2010, pp. 769-772.