Multistage Ciphering for Enhanced Security Image Encryption

Mansingh Mali[1], Prof. Kailash Patidar[2]

[1]*M. Tech. Scholar,* [2]*Guide and HOD*

Department of Computer Science Engineering, SSSIST, Sehore

Abstract - Image Encryption or ciphering of images are the methods to protect image being hacked or damaged while transmitting. Such security method applied on transmits information from one node to another node which is sensitive to disclose and need to be kept as secure as possible. Previous researches was having different security algorithms to encrypt image, and here this work promises to increase the security better than previous methods need to maintain that security levels must be increased to make the ciphering more robust and reliable. Above idea is making strong system and encrypted image is not able to guess. In the proposed encryption system security levels are here divided in parallel security also, which multiplies the security means all the layers RGB are encrypted divergently. The simulation steps will clearly shows the robustness of proposed methodology and encryption time is for tower image is 0.095252 seconds and decryption time is 0.454 seconds and this is around 77% reduction in encryption time and 95% reduction in decryption time.

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

I. INTRODUCTION

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.

Rapid evolution of the internet in the digital world today has led to the security of digital images a very important feature attracting considerable attention in different image encryption methods. For example, medical diagnostic information in form of EEG, ECG, MRI, Sonograph of a particular patient have to be stored confidentially in the hospital. It is highly illegal to disclose the diagnostic data of a person to unauthorized person. There are various image encryption systems to encrypt and decrypt data. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data. In most of the natural images, the neighboring pixels are highly correlated. In order to dissipate the high correlation among pixels and increase the entropy, complex and efficient image encryption algorithm is necessary [1].

Protection of image data from unauthorized access is very important. Image encryption plays a significant role in the field of information hiding. Generally there are two levels of security for digital image encryption: low level and high level. In low level security encryption, the encrypted image has a degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high level security, the content is completely scrambled and the image appears as random noise. In such case, the visual characteristic of the image is not understandable to the viewers [2]. The proposed techniques of image encryption in this thesis can be categorised under high-level security encryption.

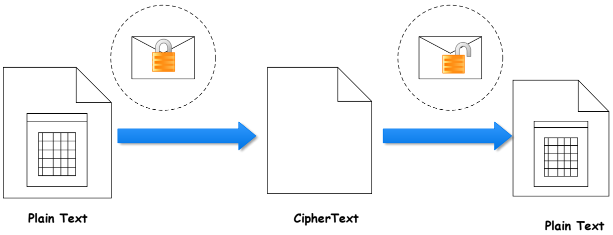

Figure 1.1 Basic Encryption Decryption of information.

A cryptosystem involves mapping of information from one domain to the same domain. The algorithm of mapping is called encryption and its inverse is called decryption. The messages are enciphered by applying mathematical operations and the resulting messages are known as cipher texts. So the symbols that are encrypted will have the same kind of mathematical structure as the encrypted symbols. Since the number of symbols is finite, symbols must belong to finite group, ring or field. The algebraic manipulation of the symbols belonging to finite group, ring or field is used for encryption. Hence, it is also called algebraic cryptosystem. Specifically, the principle of linear algebra can be applied over the finite field, ring or group.

Figure 1.1 demonstrate the concept of encryption and decryption of information.

ECC is a huge field and many different variants of cryptography based on Elliptic Curves (ECs) exist. It does not provide a single best solution for all cryptographic problems but a wide range of possibilities. This makes ECC highly versatile as it allows customization of a variety of parameters to find an optimal solution for a specific application.

II. PROPOSED METHODOLOGY

The cryptographic technique is being discussed in this work is explained here and the different parts of the proposed encryption system is explained below. The working of system is also explained with the help of flow charts after block diagrams.

In below figure the proposed system is explained with main blocks where the system is divided among multiple security layers. The first block is to twisting of red, green and blues layers with different flipping operation this is parallel security in a single layer itself. Followed by blending of layers i.e. RGB layers are mixed each other to make it more difficult to recover. The third level is chaotic mapping are also performed over RGB layer with different frequencies which will further complicate the encryption algorithm for enhancement of security. In the end of this we will get the encrypted image which is most secured image ever.

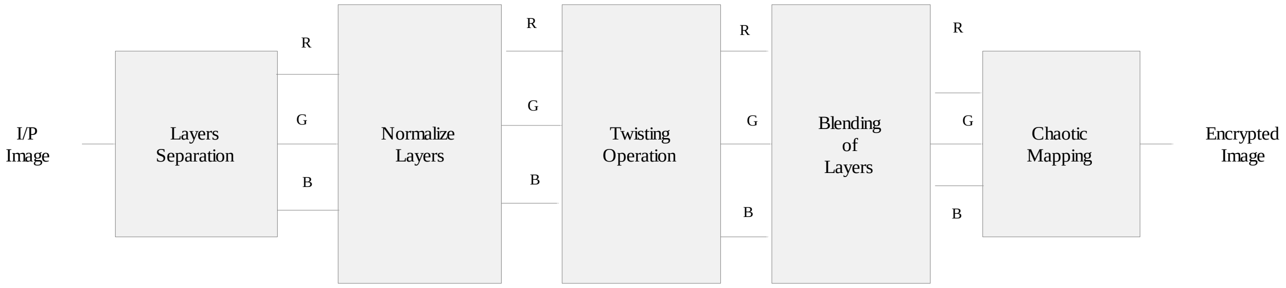

Fig. 2.1 Basic Block Diagram of Encryption Decryption Process

The decryption process is the reverse operation of encryption process and the steps are chaotic decryption of RGB layers with the specified frequencies followed by de-mixing of RGB layers and at the last reverse rotation of layers as it done on the angles.

The above system is implemented on image processing simulation tool and the flow of execution of algorithm is shown in below figures.

The flowchart of proposed Encryption and Decryption approach are given in the figure 2.3.

A. Proposed Encryption

Select the image you want to use for the image ciphering purpose extract file for saving results read the selected image resize image to square shape and normalize layers of image and apply hybrid twisting on each layer blend the layers and apply chaotic image mapping with different frequencies. save encrypted image and time required.

B. Proposed Decryption

Figure 2.3 demonstrated the flow of the proposed decryption system. To decrypt select the encrypted image which is to be decrypt. Decryption process is just a reverse of the encryption process after selecting image apply reverse chaotic mapping and apply reverse blending of layers after reverse blending of layers reverse twisting of layers applied to image after that it shows decrypted image and time take during the process of encryption and decryption .

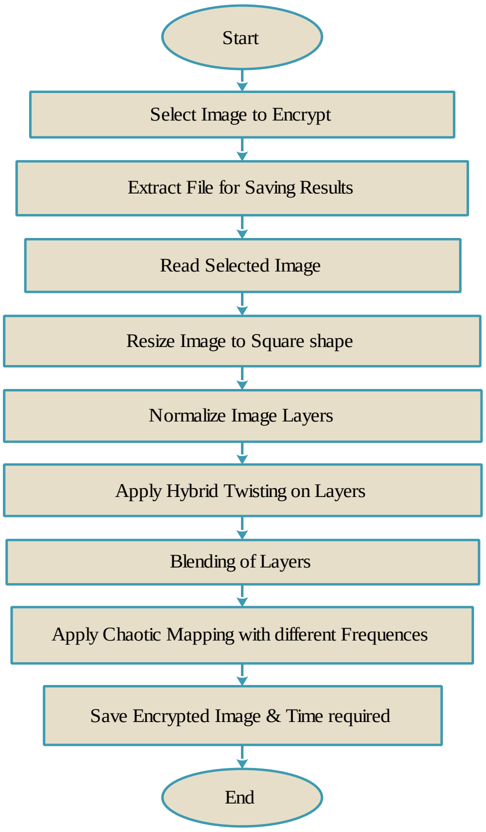
Start
Select Image to Encrypt
Extract File for Saving Results
Read Selected Image
Resize Image to Square shape
Normalize Image Layers
Apply Hybrid Twisting on Layers
Blending of Layers
Apply Chaotic Mapping with different Frequences
Save Encrypted Image & Time required
End

Fig. 2.2 Flow Chart of Encryption Process

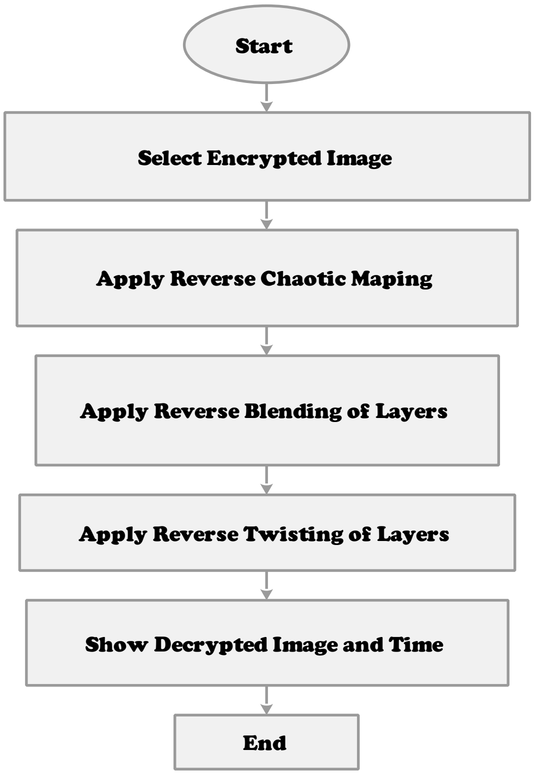
Start
Select Encrypted Image
Apply Reverse Chaotic Maping
Apply Reverse Blending of Layers
Apply Reverse Twisting of Layers
Show Decrypted Image and Time
End

Figure 2.3 Flow Chart of Decryption Process.

III. SIMULATION RESULTS

The execution of the system explained previously is performed on the simulation tool and the various images is tested over proposed system and some of the simulation results are explained here. We can see the effect on input image of that during different steps of simulation.

The simulation of the proposed system has done on the MATLAB the simulation out come and comparison table has give in comparison table 1 and table 2 with result comparing to existing system the proposed system is less time consuming and more secure as compare to existing system.

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.

The Table 1 shows the comparison of encryption and decryption time between proposed system and existing also.

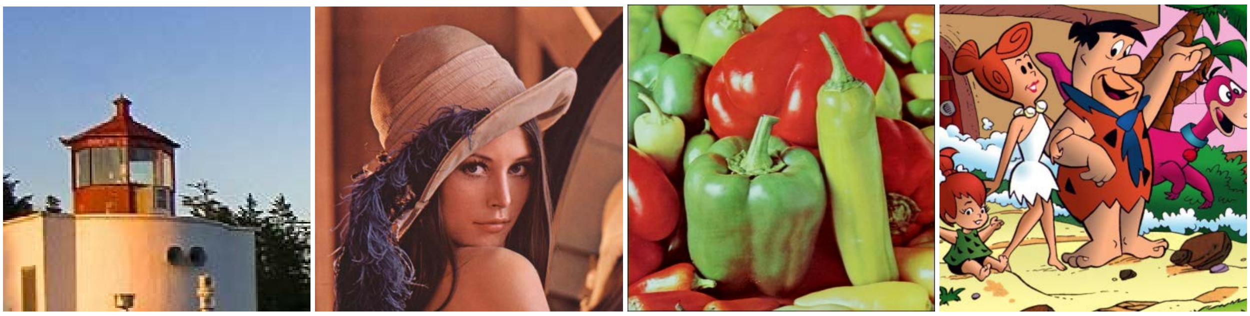

Fig. 4.1 Step 1: Input Images (Towar, lena, peppers and flinstone)

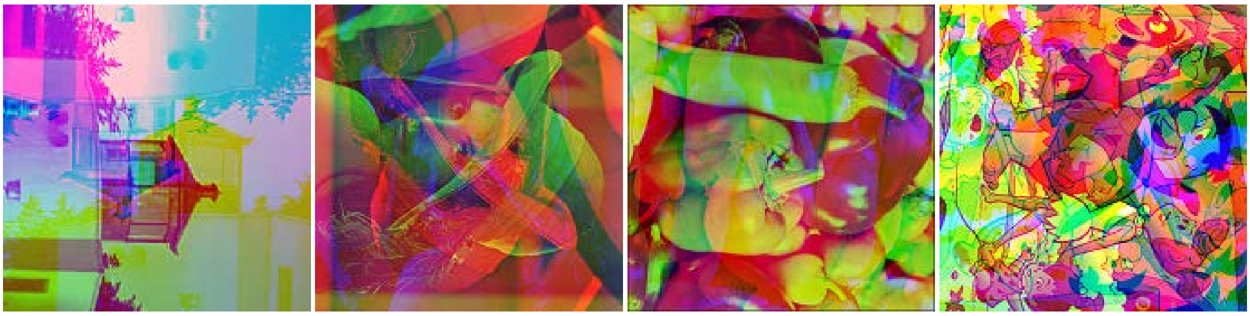

Fig. 4.2 Step 2: Hybrid Twisting of Layers of Respective Previous Stage Outputs

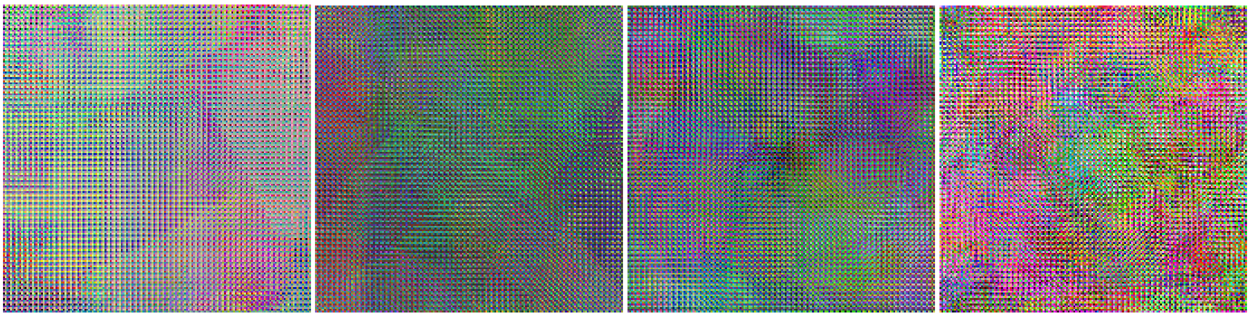

Fig. 4.3 Step 3: Blending of Layers of Respective Previous Stage Outputs

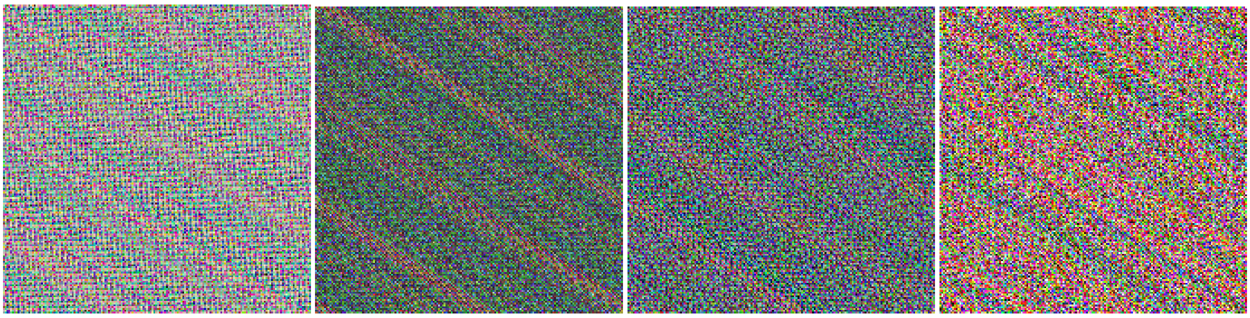

Fig. 4.4 Step 4: Chaotic Mapping Operations on Respective Previous Stage Outputs

Table 1: Comparison of Encryption and Decryption Time

Methodology	***Image Dimension***	***Encryption Time (sec.)***	***Decryption Time (sec.)***
Proposed	170x170	***0.095252 Sec.*** *(83.49% Improved)*	***0.45533 Sec.*** *(95.52% Improved)*
Existing [1]	170x170	0.575 Seconds	10.161 Seconds

Table 2: Individual Encryption and Decryption Timings in Seconds

Image	***Size (Dimension)***	***Encryption Time (Seconds)***	***Decryption Time (Seconds)***
Tower (Base Paper)	170x170	0.095252	0.45533
Lena	170x170	0.10475	0.4613
Peppers	170x170	0.09978	0.45499
Flinstone	170x170	0.09991	0.4452

IV. CONCLUSION AND FUTURE SCOPE

Simulation of cryptographic technique is worth implanting if it works faster when encrypting and decrypting also. The existing work [1] has discussed about the image cryptography which was named elliptical curve method and has better encryption and decryption time. The challenge was to improve the speed i.e. reduction in encryption and decryption time. Existing methodology has 2 level of security to encrypt image and which was also need to maintain with taking into considerations that security levels must be increased to make the encryption more robust and crack free. This will make system and encrypted image is not even unreadable even untraceable, without the knowledge of security levels and algorithm. The encryption levels are here divided in parallel security also, means all the layers RGB are not encrypted equally. This idea makes future encryption algorithms more secure even some of the old robust cryptography algorithms can modified with this concept to increase the shield of old systems and can facilitates the high end modern encryption systems.

REFERENCES

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

[2] B. Aissa, D. Nadir and M. Ammar, "An approach using stream cipher algorithm for image encryption and decryption," 2014 15th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), Hammamet, 2014, pp. 498-503.

[3] Ranjith Kumar R. and Saranraj B., "A novel chaotic color image encryption / decryption based on triangular confusion," 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, 2014, pp. 94-100.

[4] A.N. Borodzhieva and P. K. Manoilov, "MATLAB-based module for encryption and decryption using bifid ciphers applied in cryptosystems," 2014 IEEE 20th International Symposium for Design and Technology in Electronic Packaging (SIITME), Bucharest, 2014, pp. 287-291.

[5] R. U. Ginting and R. Y. Dillak, "Digital color image encryption using RC4 stream cipher and chaotic logistic map," 2013 International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, 2013, pp. 101-105.

[6] (M. Savari, M. Montazerolzohour and Y. E. Thiam, "Comparison of ECC and RSA algorithm in multipurpose smart card application," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, 2012, pp. 49-53.

[7] Padma Bh, D.Chandravathi, P.prapoorna Roja: “Encoding and decoding Of a message in the implementation of Elliptic Curve Cryptography using Koblitz Method”. International Journal on Computer Science and Engineering (IJCSE) Vol. 02, No. 05, 2010, 1904-1907

[8] Hankerson, Menezes, Vanstone. “Guide to elliptic curve cryptography” Springer, 2004 ISBN 038795273X 332s_CsCr

[9] http://www.nsa.gov/business/programs/elliptic_curve.shtml

[10] Santoshi Ketan Pote, Usha Mittal “Elliptic Curve Cryptographic Algorithm” Christof Paar, Jan Pelzl /’Understanding Cryptography”.