Divergent Chaos Vector Rotation Image Cryptography

Sakshi Shrivastava[1], Prof. Lokesh Malviya[2]
[1]*M. Tech. Scholar*, [2]*Research Guide*
Department of Computer Science Engineering, SAM College of Engineering, Bhopal

Abstract - Cryptography of image is the security method to transmit information from one node to another node without being hacked to anyone in the form of image, information is being shared in the form of image can be sensitive to disclose and need to be provided as secure as possible. Previous researches was having 2-3 levels of security layers to encrypt image, and here it is need to maintain that security levels must be increased to make the cryptography 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 0.12933 seconds and decryption time is 0.43444 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

Information that can be read and implicit without any special procedures or method is termed as plaintext or clear text. The technique of concealing plaintext in order to hide its particular material is called encryption. The impression of encryption is to make a message incomprehensible, except to the receiver.

Data encryption technology is used to benefit protection against loss, exploitation or alteration of private information. Encrypting plaintext results in indecipherable rubbish called cipher text. Encryption is used to guarantee the hidden information from anyone of concern not intended to, even those who can comprehend the encrypted data. The procedure of backsliding cipher text to its original plaintext is considered as decryption. Figure 1.1 demonstrated the process of encryption and decryption of information.

The science of consuming the calculation and math behind the procedure to encrypt and decrypt data is called cryptography. Cryptography facilitates to accumulate the sensitive information or pass on it through the insecure networks in order to keep it unreadable from public except the intend receiver.

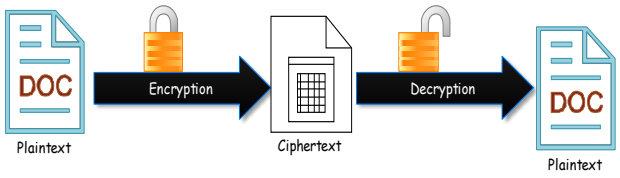

Figure 1.1 Encryption and Decryption.

Although cryptography is the skill or art of securing data, the skill of analyzing and breaking secure communication is considered as cryptanalysis. Classical cryptanalysis implicates a fascinating arrangement of application of mathematical tools, analytical reasoning, tolerance, pattern finding, willpower, and good fortune. Cryptanalysts are also considered as attackers. Cryptology comprises of both cryptography and cryptanalysis.

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 rotate the red, green and blues layers with different angles this is parallel security in a single layer itself. Followed by mixing of layers i.e. RGB layers are mixed each other to make it more difficult to guess. The third level is chaotic operations 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.

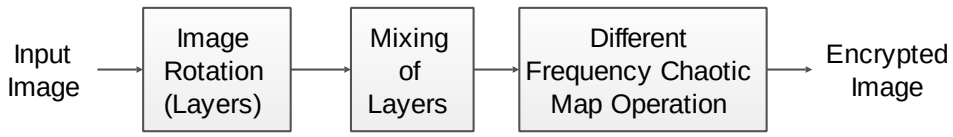

Fig. 2.1 Block Diagram of Encryption Process

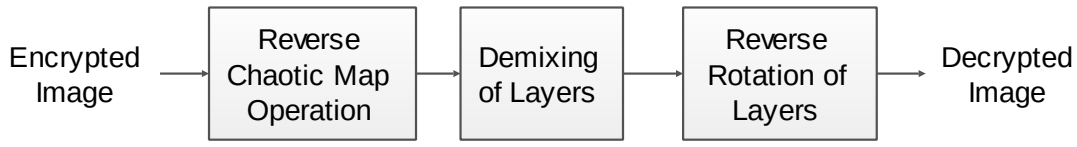

Fig. 2.2 Block Diagram of Decryption Process

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 below.

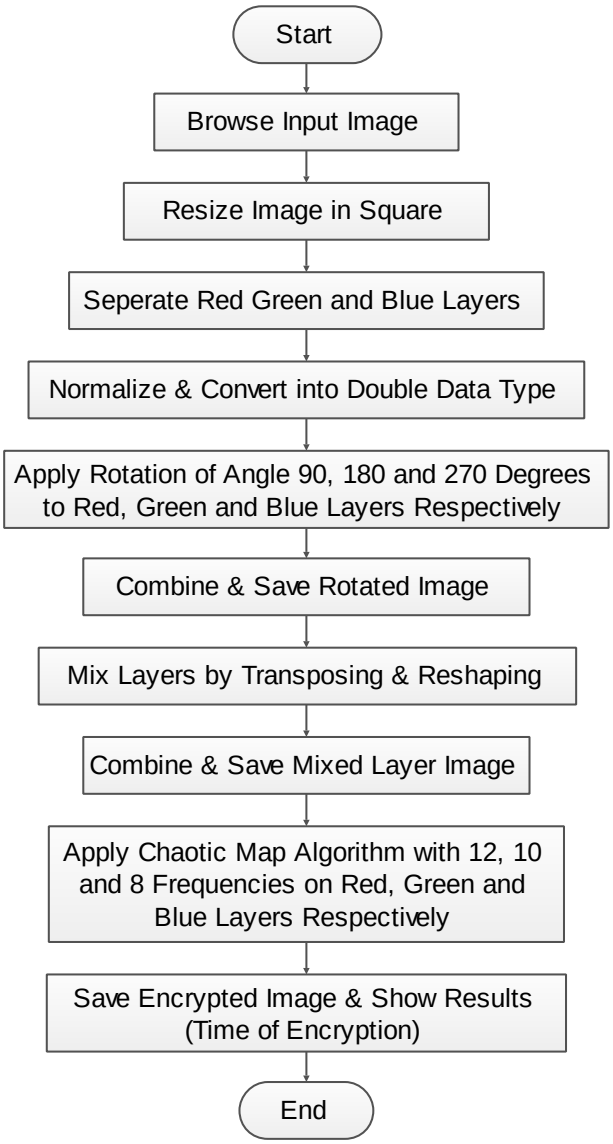

Fig. 2.3 Flow Chart of Encryption Process

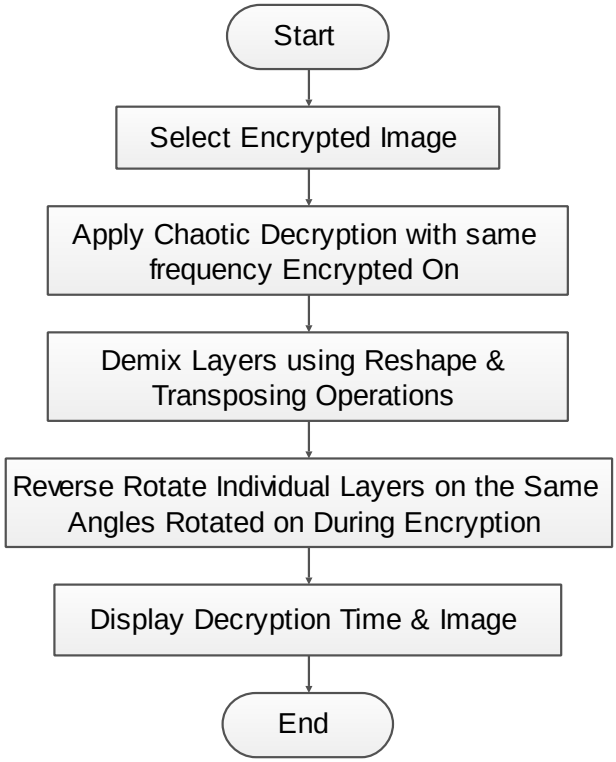

Figure 2.4 Flow Chart of Decryption Process.

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.

Fig. 4.1 Input Images (Towar, SAM_front, SAM_garden, secret)

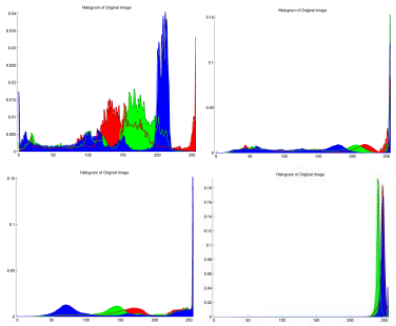

Fig. 4.2 Color Histogram of Respective Input Images

Fig. 4.3 Matrix Rotation of Layers of Respective Previous Stage Outputs

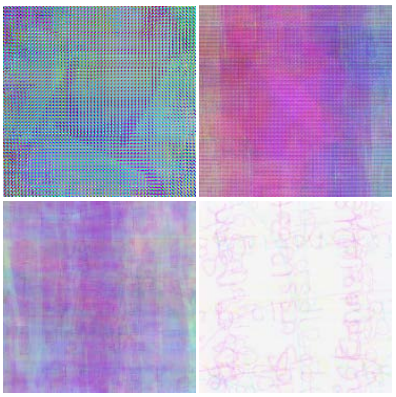

Fig. 4.4 Mixing of Layers of Respective Previous Stage Outputs

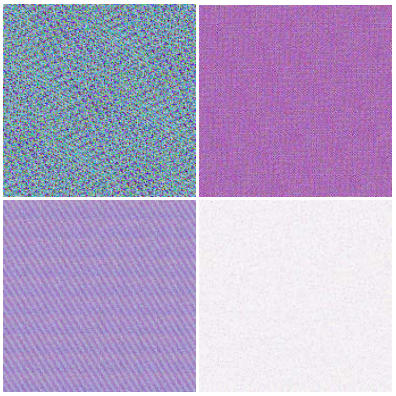

Fig. 4.5 Different Chaotic Frequency Operations on Respective Previous Stage Outputs

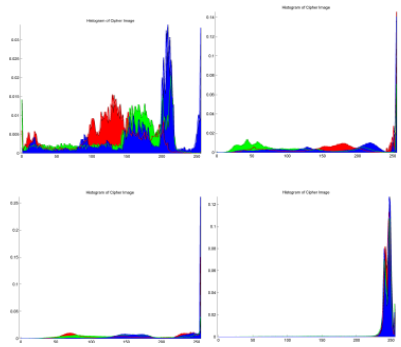

Fig. 4.6 Color Histogram of Respective Previous Stage Images

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

Table 1: Previous System Setup 1 (C++)

Image	Size	NIST Curve	Time for Encryption	Time For Decryption
Tower	170x170	P-192	0.577	10.161
		P-224	0.617	3.343
		P-256	0.575	2.951
		P-384	0.772	5.264
		P-521	1.210	29.786

Table 2: Previous System Setup 2 (java)

Image	Size	NIST Curve	Time for Encryption	Time For Decryption
Tower	170x170	P-192	0.936	3.675
		P-224	0.999	3.993
		P-256	1.087	4.580
		P-384	1.474	3.914
		P-521	1.951	12.622

Table 3: Proposed System

Image	Size	Time for Encryption	Time For Decryption
Tower	170x170	0.17253	0.62163

Table 4: Summary of Images with Respective Encryption and Decryption Time.

Image	Size	Encryption Time (sec.)	Decryption Time (sec.)
Img 1	***170x170***	***0.17584***	***0.61415***

Img 2	***170x170***	0.17514	0.61302
Img 3	***170x170***	0.17519	0.65333
Img 4	***170x170***	0.17556	0.60233
Img 5	***188x188***	0.23414	0.4463

The table: 5 show the comparison of encryption and decryption time between proposed system and existing also.

Table5: Comparison of Encryption and Decryption Time

Methodology	Encryption Time (sec.)	Decryption Time (sec.)
Proposed	***0.17584 (77% Improved)***	***0.61415 (95% Improved)***
Existing [1]	0.577	10.161

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," Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on, Visakhapatnam, 2015, pp. 1-4.

[2] Maryam Savari and Yeoh Eng Thiam, “Comparison of ECC and RSA in Multipurpose Smart Card Application”.

[3] Elsayed Mohammed and A.E Emarah and Kh.El-Shenawwey, “Elliptic Curve Cyrptosystems on Smart Cards”.

[4] 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

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

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

[7] Kamlesh Gupta1, Sanjay Silakari, “ECC over RSA for Asymmetric Encryption: A Review”

[8] http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/2/

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

[10] Santoshi Ketan Pote, Usha Mittal “Elliptic Curve Cryptographic Algorithm”

[11] Christof Paar, Jan Pelzl /’Understanding Cryptography”