Development of Multi-Layer Secure Image Cryptography

Tarendra Rahadave[1], Dr. Vikas Gupta[2]

[1]M-Tech Research Scolar, [2]Research Guide

Department of Electronics & Communication Engg. TIT, Bhopal

Abstract - Image Encryption or ciphering of images are the scheme of protecting image from unauthorized access during transmission. Such methods are applied to secure information during transmission from sender to receiver end which is sensitive to disclose and need to be kept as secure as possible. There is various security algorithms exist to secure image by image encryption, but still protection of information remains challenging task. In this work a promising approach introduced to increase the security of image data better as compared to existing methods. There is always a need to maintain that levels of security to make the ciphering more robust and reliable. This is the major concern to develop a strong system to achieve strong image encryption algorithm. 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 0.041444seconds and decryption time is 0.30793 seconds and this is around 92.8% reduction in encryption time and 96.6% reduction in decryption time.

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

I. INTRODUCTION

Cryptology is the branch of science that arrangements with the hiding of data and insurance of vital data from the interloper. In World War II, there was a need to secure the data on weapons, methodology and development of military from the enemy. Directly in the period of data innovation the security of data has turned out to be progressively critical. Since data is sent from sender to collector through open communication channel, it is important to secure the data from different gatherings. Besides, well known utilization of sight and sound innovation and expanding transmission capacity of system continuously lead us to get data specifically and plainly through images which ought to be shielded from open. As e-administration is the present pattern of organization and administration, encryption of information has turned into a need. Image encryption has far reaching applications including Government, military, money related organization, healing centers and private business.

Image encryption is one of the tools of protecting the digital images. It is a process of realigning the original image into an incomprehensible one that is not recognizable in appearance. Traditional data encryption algorithms such as DES, triple DES, RSA, IDEA or AES are not suitable for image encryption due to some intrinsic properties of image such as high redundancy and strong correlation among pixels. Shannon suggested that confusion and diffusion are the two basic techniques to overcome high redundancies and strong correlations.

There have been many suggested image encryption techniques that use chaotic functions. In a number of chaotic cryptosystems that have been proposed, the chaotic pseudorandom key streams play a central role, including generating cryptographic keys and initializing variables in cryptographic protocols randomly. With researches of chaotic cryptology going more thorough, some fatal defects have been discovered, which discourage practical applications of these cryptosystems. For example, the equivalence between the initial condition and the chaotic symbolic trajectory makes cryptosystems very weak.

The primary thought in the image encryption is to transmit the image safely over the system so no unapproved client can ready to decode the image. The image information have uncommon properties, for example, mass limit, high severance and high association among the pixels that forces exceptional prerequisites on any encryption procedure [1]. The most well-known system of secure the advanced pictures is to scramble the computerized information such that unique message of the archives ought not to be identified. There are a few methodologies to accomplish this for instance steganography, packing, advanced watermarking and cryptography. Here the emphasis is on the encryption methods of advanced digital images focused around the chaos mapping. Fundamentally image encryption is the methodology of changing data utilizing a algorithm to make it ambiguous to anybody with the exception of those having exceptional learning, normally alluded to as a key and the changing data utilizing "encryption algorithm" into a structure that can't be deciphered without a key of decryption.

From the other point of view, decryption of image recovers the genuine data from the encrypted structure image. There are more than a few computerized image encryption

frameworks to encode and decode the image information, and there is no single encryption calculation accessible that fulfills the distinctive image sorts. The encryption strategies focused around the chaos mapping gives the encoded advanced images to hold the multilevel encryption strategy furthermore diminishes the computational difficulty of the encryption process. A large portion of the algorithms particularly intended to scramble or encrypt computerized images are proposed in the mid-1990s. There are two significant assemblies of image encryption algorithms: (a) non-chaos selective methods and (b) Chaos-based selective or non-selective methods.

II. CHAOTIC IMAGE CRYPTOSYSTEMS

A distinctive structural design of prevailing chaos-based image cryptosystems is presented in Fig.2.1 It comprises of two phases, namely; confusion and diffusion phases. In the confusion phase, permutations of image pixels are prepared in a secret demand, deprived of varying their values. The purpose of the diffusion phase is to alter the pixel values in sequence so that a small alteration in one pixel is blowout out to several pixels, with looking forward to the whole image.

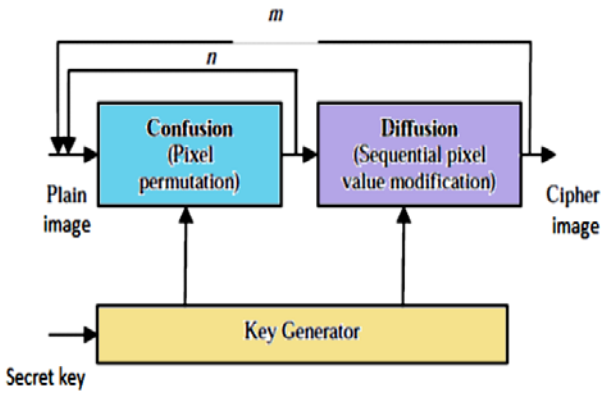


Figure 2.1 Typical Architecture of Chaos based image Cryptosystem.

To disassociate the affiliation among adjacent pixels, the confusion phase is performed n times, where n is usually larger than 1, monitored by the diffusion phase. The comprehensive n-round confusion and single round diffusion replicate from times, with m typically higher than 1, so as to acquire a satisfactory level of security. The constraints of the chaotic maps primary to the permutation and the diffusion should better be unrelated in diverse rounds. This is achieved by a round key generator with a seed secret key as input.

III. PROPOSED METHODOLOGY

The cryptographic technique is based on multilayer chaos system has been proposed in this work which is implemented and simulated on Mtalab Image processing toolbox and Simulink simulation environment. The block diagram of proposed system has shown in figure 3.1.

In proposed algorithm as shown in figure 3.1the system is explained with main blocks where the system is divided among multiple security layers. The first block layer separation of original image has done in this block image is separated in three distinct image of three layers i.e. RGB (Red, Green, Blue). In second block normalization of layers has done in this block various operations are performed on individual layers of images in this block. The third and most important block is a Twisting operation block where twisting operation is performed on processing image. Followed by fourth block blending of layers, blending of layers i.e. RGB layers are mixed each other to make it more difficult to recover. The fifth level is chaotic mapping are also performed over RGB layer with different frequencies which will further complicate the encryption algorithm for enhancement of security. At the end of the entire process an encrypted image is obtained which is most secured image ever. This work is succeeding to significantly to achieve desired security against privacy protection and loss of information. The process flow of encryption and decryption has shown in figure 3.2 and figure 3.3 subsequently.

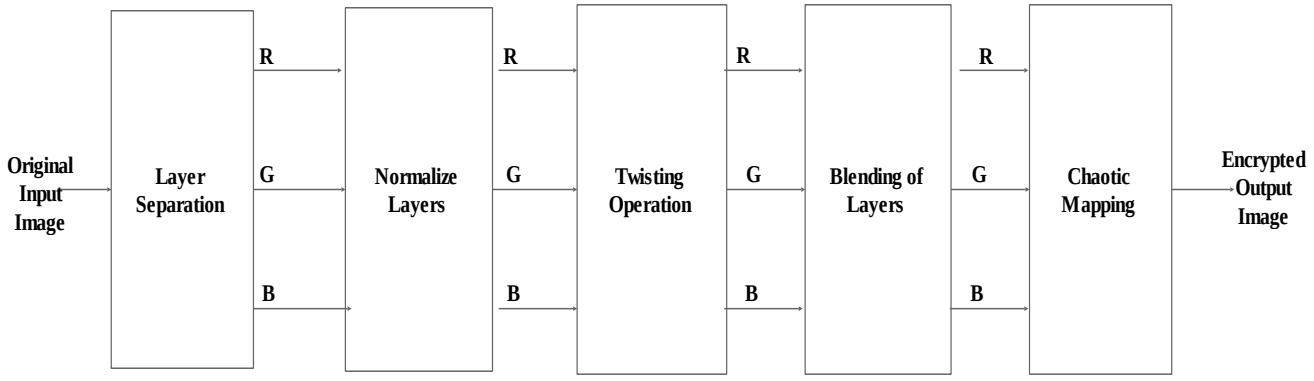


Figure 3.1 Basic Block Diagram of Encryption Decryption Process.

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.

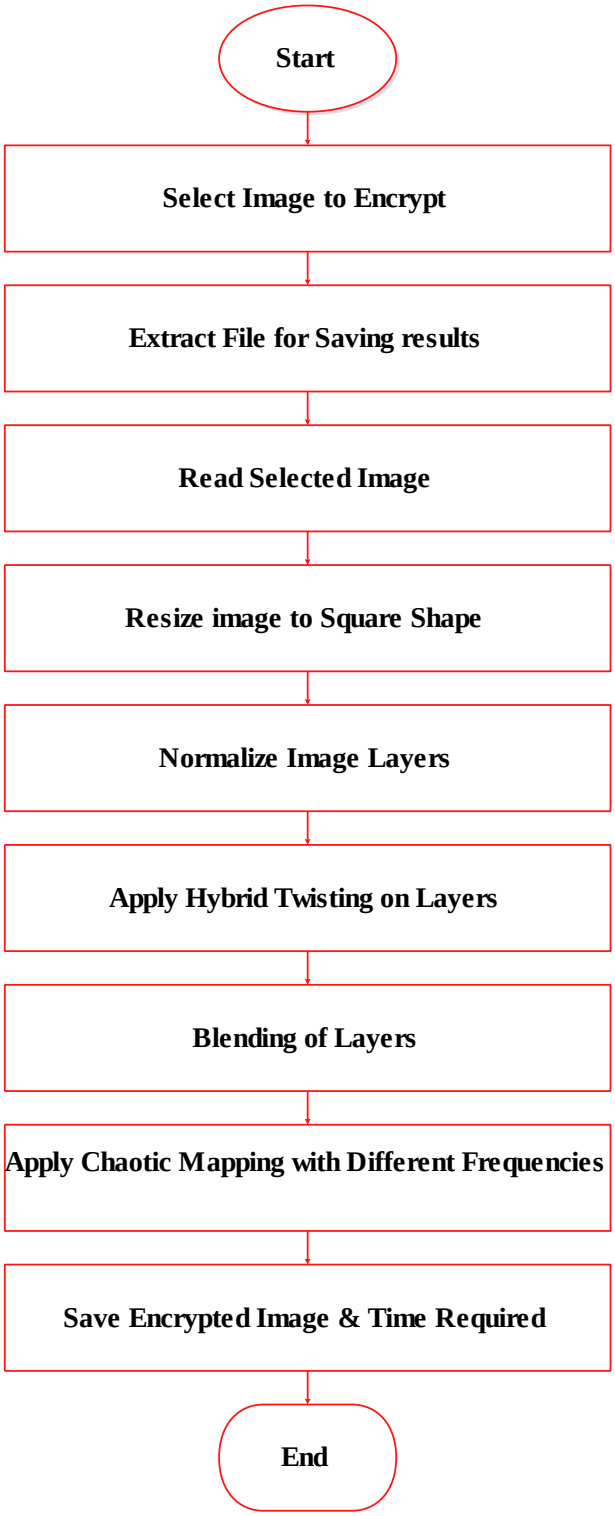


Figure 3.2 Flow Chart of Encryption Process.

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

A. Proposed Encryption

Figure 3.2 shows the encryption process flow. In encryption process fist select the image to be used 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.

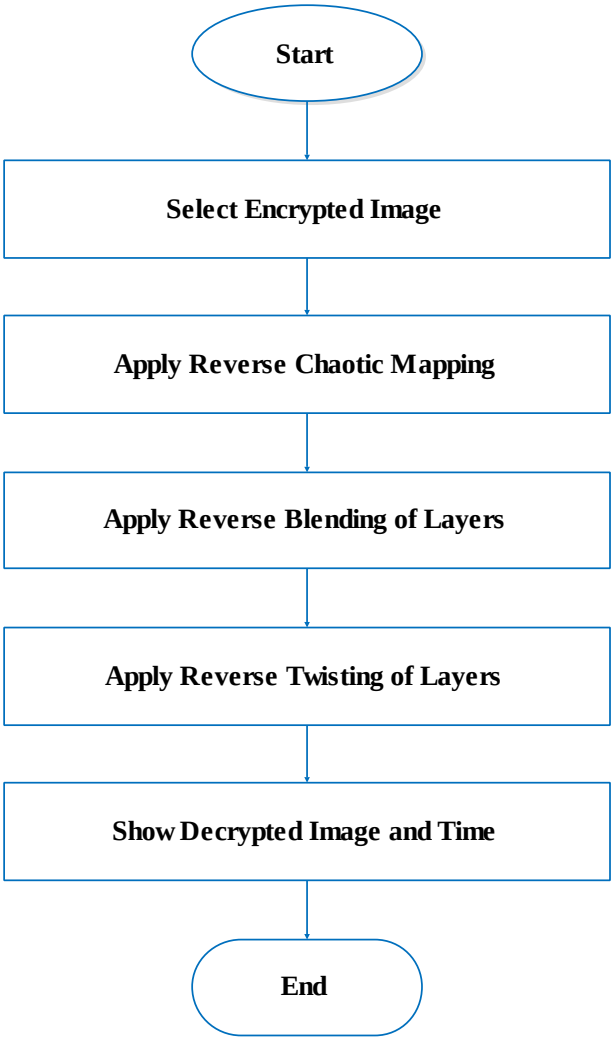


Figure 3.3 Flow Chart of Decryption Process.

B. Proposed Decryption

Figure 3.3 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.

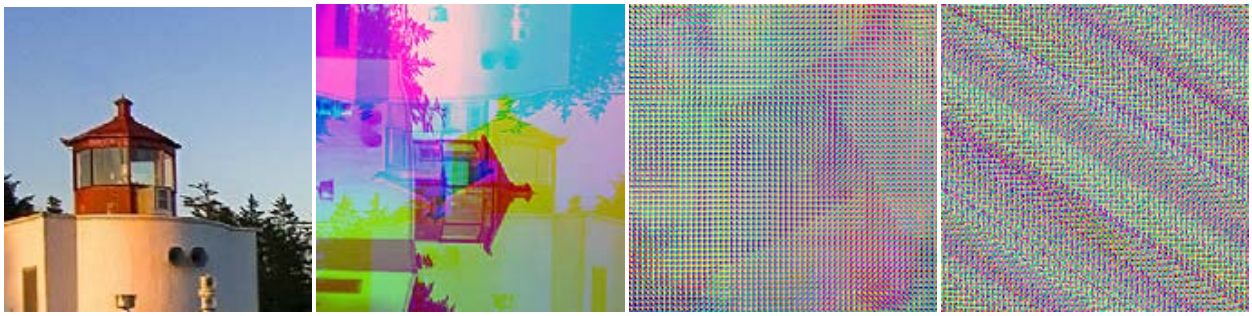
IV. SIMULATION RESULTS

The execution of the proposed multi-layer secure image cryptography has completed on MATLAB Image processing tool. The simulation tool MATLAB SIMULINK is used to perform simulation on various images. It is tested over proposed system and some of the simulation results are explained here. It is clearly visible that during the execution the security of input image are enhancing during various steps of simulation.

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.

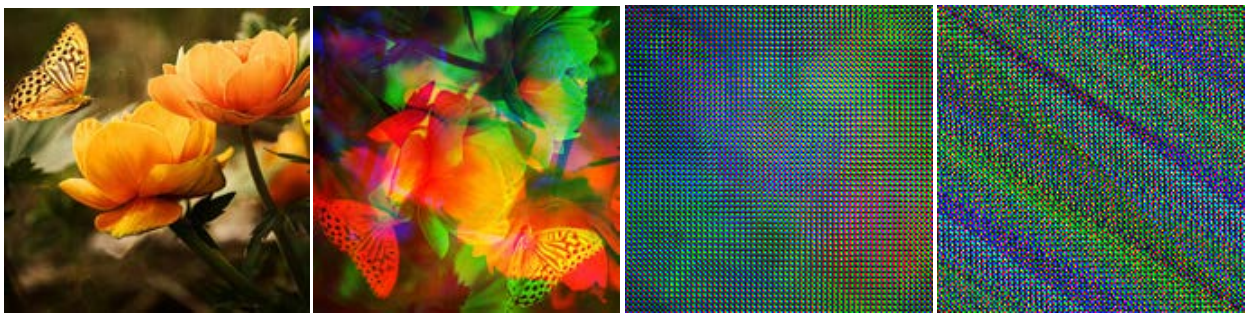
The table 2 shows the summary of images with respective Encryption and Decryption time and size of particular images where comparison has done based on the size deference between images and encryption and decryption time which is in second.

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



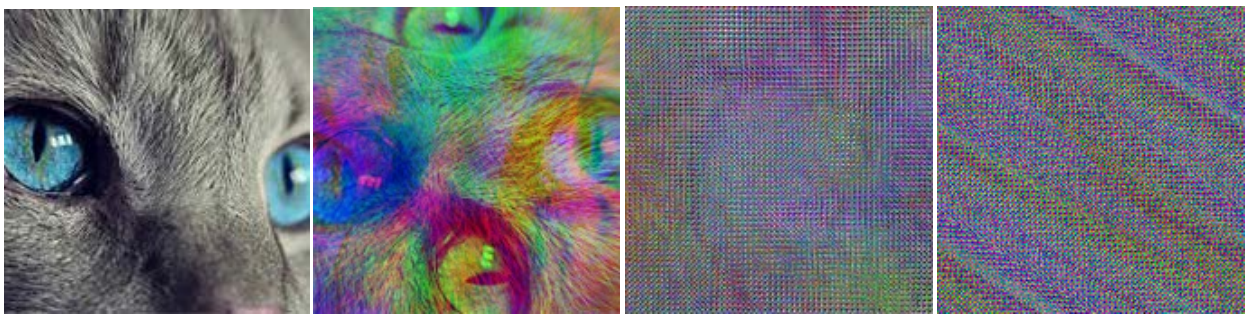
(a) (b) (c) (d)

Figure 4.1 Towar Image (a) Input Image, (b) Hybrid Twisting, (c) Blended Version and (d) Chaotic Version



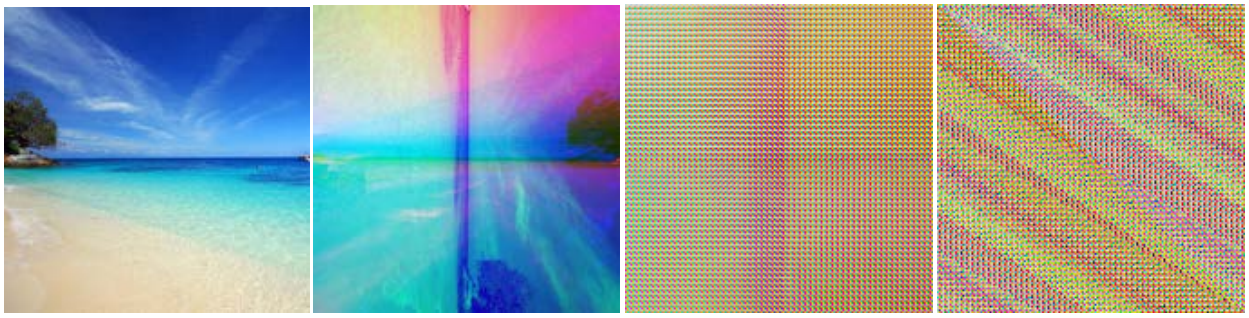
(a) (b) (c) (d)

Figure 4.2 Flower Image (a) Input Image, (b) Hybrid Twisting, (c) Blended Version and (d) Chaotic Version



(a) (b) (c) (d)

Figure 4.3 CatEye Image (a) Input Image, (b) Hybrid Twisting, (c) Blended Version and (d) Chaotic Version



(a) (b) (c) (d)

Figure 4.4 Beach Image (a) Input Image, (b) Hybrid Twisting, (c) Blended Version and (d) Chaotic Version

Table 1: Comparison of Encryption and Decryption Time

Methodology	***Image Dimension***	***Encryption Time (sec.)***	***Decryption Time (sec.)***
Proposed	170x170	***0.041444 Sec.****(92.80% Improved)*	***0.30793 Sec.*** *(96.96% Improved)*
Existing [1]	170x170	0.575 Seconds	10.161 Seconds

Figure 4.5 shows the graphical representation of comparison chart of tower image having dimension 170x170 and Figure 4.6 shows the graphical representation of Performance comparison of other images having dimension 170x170.

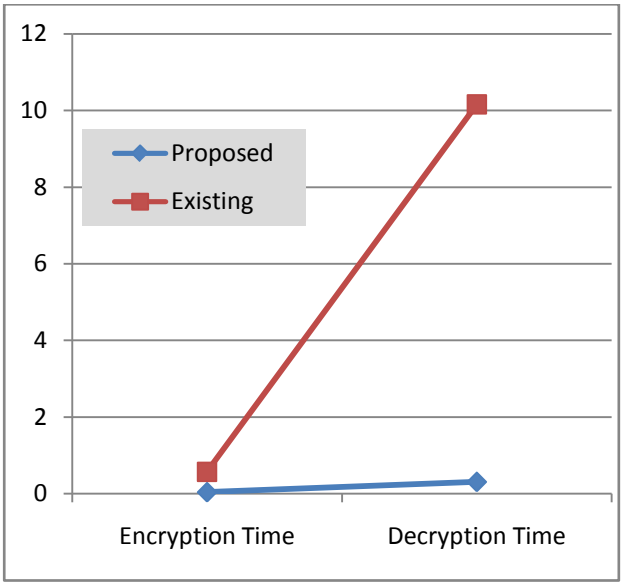


Figure 4.5 Comparison Chart of Tower Image having Dimension 170x170.

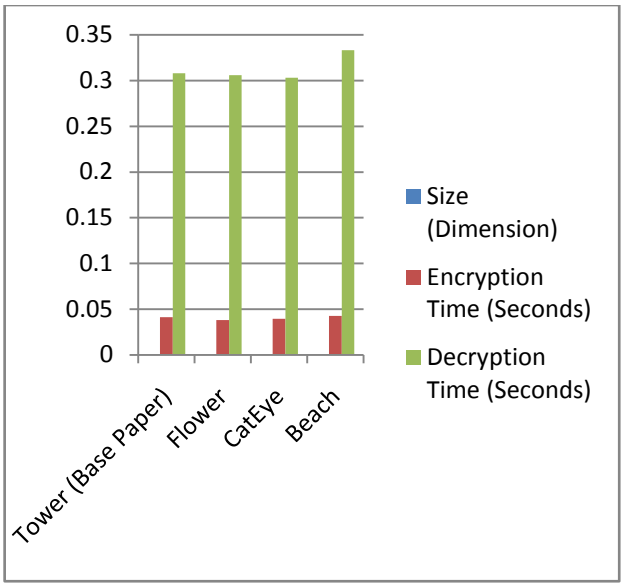


Figure 4.6 Performance Comparison of Other Images having Dimension 170x170.

Table 2: Individual Encryption and Decryption Timings in Seconds

Image	***Size (Dimension)***	***Encryption Time (Seconds)***	***Decryption Time (Seconds)***
Tower (Base Paper)	170x170	0.041444	0.30793
Flower	170x170	0.038247	0.3058
CatEye	170x170	0.039644	0.30299
Beach	170x170	0.042692	0.33312

V. CONCLUSION AND FUTURE SCOPE

In this work development of multi-layer secure image cryptography technique has reported. The existing previous work has discussed about the image stegocrypto cryptography scheme which is based on 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. There is a 2 level of

security in existing methodology to encrypt image. The level of security in previous existing work was also need to maintain with taking into considerations that security levels must be increased to make the encryption more robust and free of crack. This will make system and encrypted image is not even unreadable even untraceable, without the knowledge of security levels and algorithm. The encryption levels in proposed work are divided in parallel security also means all the layers RGB are encrypted individually unequal. 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] Litasari and B. Rahadjo, "Design and implementation stegocrypto based on elgamal elliptic curve," 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, 2017, pp. 95-99.

[2] O. Reyad, M. A. Mofaddel, W. M. Abd-Elhafiez and M. Fathy, "A novel image encryption scheme based on different block sizes for grayscale and color images," 2017 12th International Conference on Computer Engineering and Systems (ICCES), Cairo, 2017, pp. 455-461.

[3] V. Sawant and A. Bhise, "Cryptographic turbo code for image transmission over mobile networks," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, 2016, pp. 844-850.

[4] P. Tobin, L. Tobin, M. Mc Keever and J. Blackledge, "Chaos-based cryptography for cloud computing," 2016 27th Irish Signals and Systems Conference (ISSC), Londonderry, 2016, pp. 1-6.

[5] Gupta, N.; Kundu, V.; Kurra, N.; Sharma, S.; Pal, B., "Elliptic Curve Cryptography for ciphering images," in Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on., pp.1-4, 24-25 Jan. 2015.

[6] Sowmya, S.; Sathyanarayana, S.V., "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)," in Contemporary Computing and Informatics (IC3I), 2014 International Conference on , pp.1345-1350, 27-29 Nov. 2014.

[7] Baheti, A.; Singh, L.; Khan, A.U., "Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System, and Authentication Using Neural Network," in Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on , pp.664-668, 7-9 April 2014.

[8] Soleymani, A.; Nordin, M.J.; Md Ali, Z.; Golafshan, L., "A binary grouping approach for image encryption based on elliptic curves over prime group field," in Communications (MICC), 2013 IEEE Malaysia International Conference on., pp.373-378, 26-28 Nov. 2013.

[9] Xiangqian Wu; Ning Qi; Kuanquan Wang; Zhang, D., "A Novel Cryptosystem Based on Iris Key Generation," in Natural Computation, 2008. ICNC '08. Fourth International Conference on , vol.4, pp.53-56, 18-20 Oct. 2008.

[10] Zhang Yun-Peng; Liu Wei; Cao Shui-ping; ZhaiZheng-jun; NieXuan; Dai Wei-di, "Digital image encryption algorithm based on chaos and improved DES," in Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on, pp.474-479, 11-14 Oct. 2009.