ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

An Efficient Image Encryption System

Narinder Kaur, Kumar Saurabh

Abstract: ***In current era, the defence of multimedia data is becoming very significant. The security of this multimedia information can be done with encryption. There are a number of diverse procedures used to shield confidential image data from illicit access. In this paper, we analyze on existing work which is used different techniques for image encryption and propose our image encryption algorithm.***

***Keywords*—Asymmetric key cryptography, Decryption, Encryption, Image encryption, Symmetric key cryptography.**

I. INTRODUCTION

A) IMAGE ENCRYPTION

With the ever-increasing escalation of multimedia applications, security is a significant concern regarding communication and storage of images, and encryption is one the ways to guarantee security. Image encryption run through in transform original image to another image that is tough to understand; to keep the image confidential between users, in other word, it is essential that nobody could acquire the content without a key for decryption. According to Kirchhoff's principle of secure cryptosystem [1], the protection should depend on the secrecy of the key, not the secrecy of the encryption/decryption algorithm that was used. In other words, it is supposed that the algorithm is publicly known, yet decryption of message is infeasible on the basis of the cipher text in addition to acquaintance of the algorithm. Every cipher text block is affected by many plaintext blocks. Typically, it is also unfeasible to search for relationship between the keys without the knowledge of some added information.

B) CATEGORIES OF CRYPTOGRAPHY

There are two chief categories of cryptography:

Secret key cryptography: Secret key cryptography is also recognized as *symmetric key* cryptography. Through this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender by means of the key and decrypted by the receiver using the identical key.

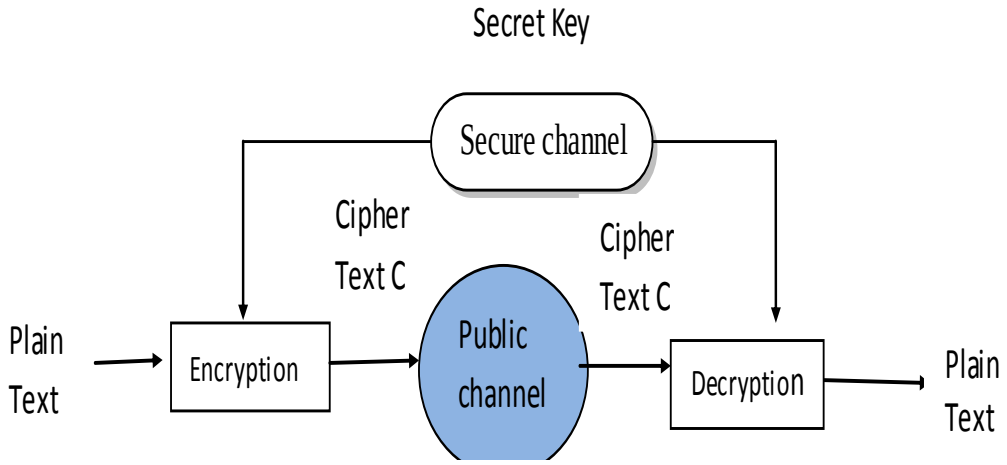

Fig 1: Symmetric Key Cryptography

Public key cryptography: Public key cryptography is also recognized as *asymmetric key cryptography*, uses a pair of keys for encryption and decryption. By means of public key cryptography, keys work in pairs of matched public and private keys.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

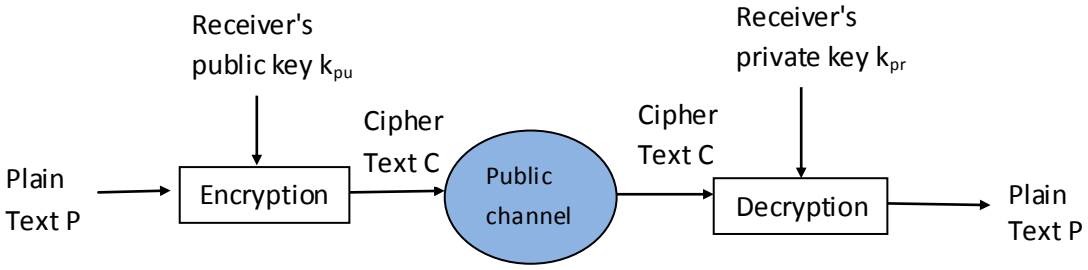

Fig 2: Asymmetric Key Cryptography

Cryptography practice is used when secret messages are transferred from one party to another over a communication line. Cryptography technique desires some algorithm for encryption of data. At the present time when more and additional sensitive information is stored on computers and transmitted over the Internet, we require to certify information security and safety. Image is also vital part of our information. Thus, it's extremely significant to protect our image from illicit access. There are several algorithms existing to protect image from unauthorized access which is described in next section.

II. LITERATURE REVIEW

To attain a fast encryption, image encryption schemes are frequently designed not to encrypt the intact images completely, but a segment only. In this approach, the amount of computation is reduced and this approach is regarded as selective image encryption [2]. Gray level images are generally composed of eight bit planes. The higher-order bit planes include the majority of visually significant and strong correlation information of the plain image, whereas the residual contributes to more restrained details in the image. Based on this observation, a selective bit plane encryption scheme is projected [3].

A formal language (SCAN) is proposed to describe and generate multiple of two-dimensional (2D) spatial accessing order from a short set of simple ones [4]. It is first employed for image encryption [5]. The plain image is originally serialized to one dimensional data stream which is then described by the SCAN language.

In entropy coding, the statistical model is used to decode the compressed bit stream. It is hence recommended that multiple statistical models are used alternately in certain secret order to encode the input symbol stream [5]. Through security analyses, this scheme is proved to be applied effectively on both multiple Huffman coding tables of Huffman coder and multiple state indices of QM coder. However, it should be distinguished that the original image can be accurately reconstructed only if its input is alike to the output of the encoder. There is also a anxiety about codec dependence of such kind of scheme [6].

A direct and evident way to protect the information from illicit eavesdropping is to use an encryption algorithm to pretence the information, which has led to the expansion of a variety of theories based encryption techniques. [7-8].Chaos theory has been recognized by many different research areas, such as physics, mathematics, engineering, and biology [7].

A symmetric encryption scheme based on two-dimensional chaotic maps is projected [9]. A two or higher dimensional discretized chaotic map is adopted for pixel permutation collectively with another one-dimensional (1-D) map for dissemination.

In Pareek et al. [8], an image encryption scheme utilizing two chaotic logistic maps along with an external key of 80-bit.The primary circumstances for both logistic maps were derived from the external secret key.

Chen et al. [10] have anticipated a symmetric image encryption in which a two-dimensional chaotic map is generalized to three-dimension for scheming a real time secure image encryption scheme. This approach employs the three-dimensional cat map to jumble up the positions of the image pixels and uses another chaotic map to mystify the relationship between the encrypted and its original image.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

III. PROPOSED ALGORITHM

Random numbers are generated by chaotic map and PMMLCG. In this projected technique, the following steps are evolved:

1. First the pixels are jumbled according to pseudo random numbers, generated through chaotic map. This is called substitution process.

2. Following scrambling the pixels row and column shuffling is being done by using random numbers, generated through chaotic map and PMMLCG.

3. Masking operation is applied on scrambled pixels. Masking is done from bitwise XORed operation. The selection of XOR operation is based on its properties.

4. Substitution and Transposition of row pixels and column pixels are done alternatively

5. Using chaotic map pixels are jumbled after applying the masking operation.

6. To retrieve the original image back the whole process is reversed.

The competence and efficacy of the algorithm is calculated by doing Quantitative and Qualitative analysis. MATLAB is used to execute the anticipated algorithm. MATLAB has predefined classes to carry out action on images. MATLAB is a numerical computing environment and fourth generation programming language. MATLAB allows matrix operation, intrigues of functions and data, execution of algorithm, construction of user interface, and interfacing with programs written in other languages, including C, C++ and java.

IV. EXPERIMENTAL RESULTS

Qualitative Analysis and Quantitative Analysis is accomplished using a number of parameters which consist of Histogram Analysis, Entropy and Cross Correlation.
Analysis of histogram is a qualitative analysis which takes account of perception of the images. After encrypting the image by means of the proposed encryption technique, the histogram is instituted to be uniform and all gray levels have equivalent frequency of occurrence with the similar probability. The histogram of the cipher image has no statistical relation to the plain image and hence does not provide any evidence for a statistical attack on the projected encryption scheme.

Entropy [26] h is a cumulative measure of the frequency of the intensity levels in an image. Due to the characteristics of the human eye, which is insensitive to high frequency components, an image of high entropy is not visually observable. Entropy is given by:

$$h = -\Sigma(p_i \log_2 p_i)$$

Where p_i is the frequency of intensity level in the image. The maximum h an 8–bit image can attain is 8. The average of our results is 7.9973. Hence a statistical attack is hard to formulate.
The cross–correlation coefficient among the plain image A and the cipher image B quantifies the level to which the encrypted image pixels are somewhat randomized. The nearer it is to zero, the superior. Our proposed algorithm has formed cipher images with cross correlation values that are minor than other chaos-based image encryption schemes.

V. CONCLUSION

The projected algorithm is a good amalgamation of exchange and transposition by means of chaotic maps and pseudorandom numbers. Due to characteristics of both chaotic maps and pseudorandom numbers, we can affirm that this system is both protected and proficient for ciphering an image. In response to the aforesaid challenges in protecting multimedia content, the intention of this research work is especially oriented towards analyzing chaos-based and Prime Modulo Multiplicative Linear Congruential Generator (PMMLCG) image encryption schemes. Many existing schemes under this class are found to merely attain moderate or even stumpy security. Only a few of them promises to achieve adequate security, but without maintaining a pleasing speed

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

performance. Our work is to amend and optimize some existing chaotic image encryption schemes so as to uplift the efficiency necessary for real-time operation purpose. In this regards, two enhancement methods in the system efficiency have been projected to the main components of typical chaos-based image cryptosystems: logistics chaotic map and Prime Modulo Multiplicative Linear Congruential Generator, used to produce random numbers. The higher results of qualitative and quantitative analysis justify the feasibility of such proposed schemes in real-time communication environment.

REFERENCES

[1] B. Furht, D. Socek, A.M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques", in B. Furht and D. Kirovski (Eds.), Multimedia Security Handbook, Ch. 3, CRC Press, 2005.

[2] M. Podesser, H.-P. Schmidt, A. Uhl, "Selective Bit plane Encryption Scheme for Secure Transmission of Image Data in Mobile Environments" ,Proc. of the 5th IEEE Nordic Signal Processing Symposium (NORSIG'02), Trondheim, Norway, October 2002.

[3] Kachris, Christophoros. "Design and FPGA implementation of the SCAN encryption algorithm." PhD diss., Technical University of Crete, 2003.

[4] Chen, Chao-Shen, and Rong-Jian Chen." Image encryption and decryption using SCAN methodology" In Parallel and Distributed Computing, Applications and Technologies, Seventh International Conference on, pp.61-66 IEEE, 2006

[5] C.P. Wu, C.C. Kuo, "Design of Integrated Multimedia Compression and Encryption Systems", IEEE Trans. Multimedia 7(5), pp. 828-839, 2005.

[6] Cheng, Howard, and Xiaobo Li. "Partial encryption of compressed images and videos." Signal Processing, IEEE Transactions on 48, no. 8, 2439-2451, 2000.

[7] Shubo Liu, Jing Sun, ZhengquanXu,"An Improved Image Encryption Algorithm based on Chaotic System" Journal of Computers, Vol. 4, No. 11, 2009.

[8] VinodPatidar, N.K. Pareek , K.K. Sud,"A new substitution–diffusion based image cipher using chaotic standard and logistic maps" "ELSEVIER , Communications in Nonlinear Science and Numerical Simulations 14, 3056–3075, 2009.

[9] Fridrich Jiri, "Symmetric ciphers based on two dimensional chaotic maps", Int. J. Bifurcat Chaos 8, (6), pp. 1259–1284, 1998.

[10] G. Chen, Y. Mao and C.K. Chui, "A symmetric image encryption based on 3D chaotic maps", Chaos Solitons Fractals 21, pp. 749–761, 2004.