Scrambling Based Secure Image Transmission

Narinder Kaur **Kumar Saurabh**

Abstract

An image is a pertinent data because of its visual characteristics. Image should be encrypted appropriately due to sensitivity to changes as well as security perspective. But as of inherent characteristics of image, standard encryption algorithms are not appropriate for image encryption. Recently, research on image encryption using chaos theory has been emerged. In this research, work chaos based encryption technique and prime modulo multiplicative linear congruential generator (PMMLCG) has been proposed to improve the quality of image encryption and to attain the objective of pixel scrambling.

Keywords: Asymmetric key cryptography, Decryption, Encryption, Image encryption, Symmetric key cryptography. Security analysis; Stream cipher

I. Introduction

An escalating amount of information is being transmitted over the Internet, including not only text but also audio, image, and other multimedia files. Images are extensively used in daily life, and, as a result, the security of image data is an important requirement [1]. In addition, when either communication bandwidth or storage is restricted, data are often compacted. Encryption is also performed when it is required to defend user privacy [2].Several reviews have been published on image and video encryption provides overviews, comparisons, and assessments of classical encryption schemes for visual data.

Image encryption schemes have been gradually more studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Conventional image encryption [2] algorithm such as data encryption standard (DES), has the flaw of low-level efficiency when the image is bulky. Cryptography studies how to devise good (secure and fast) whether or not they are vulnerable to some attacks. An encryption scheme is called a cipher (or a cryptosystem). The encryption and decryption procedure of a cipher is depicted in Figure 1.

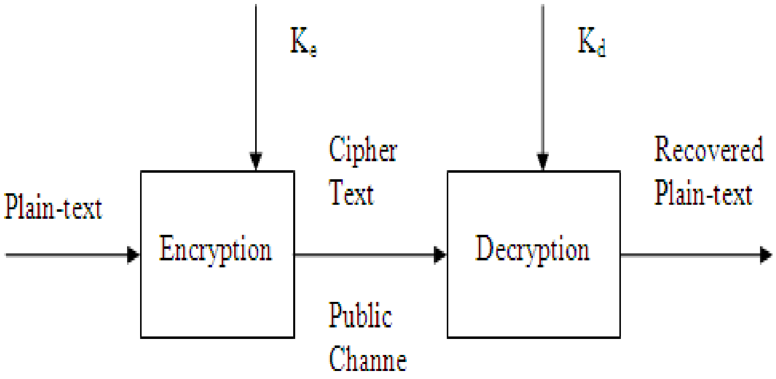

Fig. 1. Encryption and Decryption procedure of a Cipher

The communication for encryption is called plaintext, and the encrypted message is called cipher-text, which is denoted here by P and C, respectively. The encryption procedure of a cipher can be described as C=Eke(P), where Ke is the encryption key and E(.) is the encryption function. Similarly, the decryption procedure is P=Dkd (C), where Kd is the decryption key and D(.) is the decryption function. When Ke=Kd, the cipher is called a private-key cipher or a symmetric cipher.

For private key ciphers, the encryption-decryption key must be transmitted from the sender to the receiver via a separate secret channel. When Ke=!Kd, cipher is called a public-key cipher or an asymmetric cipher. . For public-key ciphers, the encryption key Ke is published, and the decryption key Kd is kept secret, for which no additional secret channel is needed for key transfer. The cryptosystem can be confidential with respect to the structure of encryption algorithm as stream ciphers and block ciphers.

Stream cipher is the way in which a key generator produces a bit stream (the Key stream) which enciphers the plain-text bit stream by simple modulo 2 additions. A stream cipher system therefore hides the plain-text bit by changing the bits of it in a random way. An interceptor, who does not know the key, will not know which bits have been changed (corresponding to the occurrence of “1” in the key stream), or which ones remain unchanged (“0” in the key stream). An idyllic stream cipher would employ a physical (true) random number generator a Key generator. Since its output cannot be reproduced, however, decipherment would be not viable, unless the whole Key stream, with the same length as the plain-text, is transported to the legitimate receiver via a safe channel. This procedure is often not viable. Therefore mostly so-called pseudo-random number generators with unique properties controlled by a relatively short Key have to be used instead as key generators.

Unlike the stream ciphers, where only one bit at a time is ciphered, whole blocks of bits are treated simultaneously. In this case the plain-text information is concealed by the fact that, depending on the key, a cipher-text block can be deciphered to any mixture of plain-text bits or to as many combinations as the keys. If the keys are chosen with equal probability, then to the interceptor observing a cipher text block, all the possible plain-text blocks are equally likely to have occurred.

Cryptography is an eternal field of interest at all time. At present secret communication plays an escalating role in many fields of common life, like banking, industry, commerce, telecommunication etc. Owing to the move ahead in network technology, information security is an increasingly important problem. Popular application of multimedia technology and increasing transmission ability of network steadily leads to us to attain information directly and clearly through images. Hence, data security has become a critical and imperative issue. Encryption is such a way that its content can be reconstructed only by a legal recipient. The technology of encryption is called cryptology. Cryptology is the branch of science dealing with the theory of secure communication algorithms. Cryptography is the process of transforming information (plain-text) into unintelligible form (cipher-text) so that it may be sent over insecure channels or it may be stored in insecure files. Cryptographic procedures can also be used for personal identification, digital signature, access control etc.

II. LITERATURE REVIEW

G. A. Sathish Kumar et al. [3] presented a new method for image encryption by integrated pixel scrambling plus diffusion technique [IISPD]. The algorithm makes use of full chaotic property of logistic map and reduces time complexity. The algorithm calculates the permuting address for row by bit xor'ing the adjoining pixel values of original image. Similarly, the algorithm calculates the permuting address for column by bit xor'ing the adjacent pixel values of original image. Therefore, this technique does not entail the knowledge of probability density function of the chaotic orbits a priory, as a result it reduces the complexity of this technique. The diffusion is performed after scrambling and is based on two chaotic maps. Hence, the key space and security of the algorithm is increased. It also has higher key space and higher degree of scrambling.

Fuyan Sun et al. [4] projected an idea is to encrypt the image in space with spatial chaos map pixel by pixel, and then the pixels are confused in multiple directions of space. Using this process one cycle, the image becomes indistinguishable in space due to inherent properties of spatial chaotic systems.

Hossam El-din H. Ahmed et al.[5] presented an efficient chaos based feedback stream cipher (ECBFSC) for image cryptosystems. The proposed stream cipher is based on the use of a chaotic logistic map and an external secret key of 256-bit. The initial conditions for the chaotic logistic map are derived using the external secret key by providing weightage to its bits corresponding to their position in the key. Further, new features of the proposed stream cipher include the heavy use of data-dependent iterations, data-dependent inputs, and the inclusion of three independent feedback mechanisms. These proposed features are verified to provide high security level.

Linhua Zhang et al.[6] improved the properties of confusion and diffusion in terms of discrete exponential chaotic maps, and design a key scheme for the resistance to statistic attack, differential attack and grey code attack. In this paper implementation of spatial S-box and design of key scheme for the resistance to statistic attack and grey code attack is being done. This scheme can resist to the error function attack (EFA) which be regarded as a very effective attack recently.

Ji Won Yoon et al.[7] proposed a new image encryption algorithm using a large pseudorandom permutation which is combinatorially generated from small permutation matrices based on chaotic maps. The random-like nature of chaos is effectively spread into encrypted images by using the permutation matrix.

G. A. Sathish Kumar et al.[8] proposed a new image encryption algorithm using random pixel permutation based on chaos logistic maps and prime modulo multiplicative linear congurential generators. The random-like nature of chaos is effectively extended into the encrypted image through permutation and transformation of pixels in the plain image. The pixel transformation results in the encryption scheme being resistive to cryptanalytic attacks. Simulation results show high sensitivity to key, plaintext and cipher text changes. From a cryptanalytic point of view, the scheme is highly resistive to known/chosen plaintext and cipher text attacks. The proposed technique gives good parametric and sensitivity results proving itself an eligible candidate for image encryption. Moreover it is a lossless encryption technique and hence use for securing medical and military image.

Jiankun Hu et al.[9] proposed a novel pixel-based scrambling scheme to protect, in an efficient and secure way, the distribution of digital medical images. To endow with an efficient encryption of a bulky capacity of digital medical images, the proposed system uses simple pixel level XOR operation for image scrambling in an pioneering way such that structural parameters of the encryption scheme have become a part of the cryptographic key. The cryptographic key of this operation is a true random number sequence generated from multi-scroll chaotic attractors.

III. CHARACTERISTICS OF PROPOSED IMAGE CRYPTOSYSTEM

The projected information security system is able to not only guard confidential messages in the text form, but also in image form. Three basic characteristics in the information security field are adhered which include: privacy, integrity, and availability.

(1) Privacy: an unauthorized user cannot reveal a message.

(2) Integrity: an unauthorized user cannot amend or corrupt a message.
(3) Availability: messages are made accessible to authorized users authentically.

A perfect image cryptosystem is not only flexible in the security mechanism, but also has high overall performance. Thus, besides the above characteristics, the image security includes the following characteristics:

- The encryption system is computationally secure. It requires an extremely long computation time to break, for example. Unauthorized users are not able to read privileged images.
- Encryption and decryption are fast enough so as to not degrade system performance. The algorithm for encryption and decryption is simple enough to be done by users with a personal computer.
- The security mechanism is elastic.
- Large expansion of the encrypted image data is not there.

IV. Experimental results

Qualitative Analysis and Quantitative Analysis is accomplished using a number of parameters which consist of Histogram Analysis and Entropy

A. Histogram Analysis

After encrypting the image using the proposed encryption technique, the histogram is consistent and all gray levels have same frequency of occurrence with the same probability. The histogram of the cipher image has no statistical relation to the plain image and hence does not provide any clue for a statistical attack on the proposed encryption scheme.

B. Entropy

Entropy 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 perceivable. The average of our results is 7.99. Hence a statistical attack is difficult to make.

The following tables shows the change in parameters by varying the Linear Congruential Generator parameter a, M and seed values (x_0, y_0).

Table 1 Average result for Set 1 Images

a	*m*	*Seed(x_0,y_0)*	*Entropy*
92717	*262139*	*(44,44)*	*7.9617*
118068	*262139*	*(97,44)*	*7.9618*
166972	*262139*	*(44,44)*	*7.9533*
283741	*524287*	*(97,44)*	*7.9641*
37698	*524287*	*(97,44)*	*7.9665*
178	*251*	*(44,44)*	*7.9716*

Table 2 Average result for Set 2 Images

a	*m*	*Seed(x_0,y_0)*	*Entropy*
92717	*262139*	*(44,44)*	*7.9818*
118068	*262139*	*(97,44)*	*7.986*
166972	*262139*	*(44,44)*	*7.9791*
283741	*524287*	*(97,44)*	*7.9857*
37698	*524287*	*(97,44)*	*7.9882*
178	*251*	*(44,44)*	*7.9884*

V. Conclusion

In this research work chaos based encryption technique and prime modulo multiplicative linear congruential generator (PMMLCG) has been projected to improve the quality of image encryption and to accomplish the goal of pixel scrambling. The projected algorithm generates random numbers, which are used in row shuffling, column shuffling and pixel scrambling. Results effectiveness is measured in qualitative and quantitative metrics .In this present research work, the typical structure of chaos-based image encryption schemes has been implemented.

References

[1] H. Hossam El-din, H. M. Kalash, and O. S. Farag Allah, “An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption,” Informatica, vol. 31, no. 1, pp. 121–129, 2007. View at Scopus

[2] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” International Journal of Bifurcation and Chaos in Applied Sciences and Engineering, vol. 8, no. 6, pp. 1259–1284, 1998. View at Scopus

[3] Sathish Kumar, G. A., K. BhoopathyBagan, and V. Vivekanand. "A novel algorithm for image encryption by integrated pixel scrambling plus diffusion [IISPD] utilizing duo chaos mapping applicability in wireless systems." Procedia Computer Science 3. 2011

[4] Sun, Fuyan, Shutang Liu, Zhongqin Li, and ZongwangLü. "A novel image encryption scheme based on spatial chaos map." Chaos, Solitons& Fractals 38, no. 3: 631-640, 2008.

[5] Ahmed, Hossam El-din H., Hamdy M. Kalash, and Osama S. Farag Allah. "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption." INFORMATICA- 31, no. 1,2007

[6] Zhang, Linhua, Xiaofeng Liao, and Xuebing Wang. "An image encryption approach based on chaotic maps." Chaos, Solitons& Fractals 24, no. 3,759-765, 2005.

[7] Yoon, Ji Won, and Hyoungshick Kim. "An image encryption scheme with a pseudorandom permutation based on chaotic maps." Communications in Nonlinear Science and Numerical Simulation 15, no. 12. 2010.

[8] Sathishkumar, G. A., SrinivasRamachandran, and K. BhoopathyBagan. "Image encryption using random pixel permutation by chaotic mapping." In Computers & InformaticsSymposium on, pp. 247-251. IEEE, 2012.

[9] Hu, Jiankun, and Fengling Han. "A pixel-based scrambling scheme for digital medical images protection." Journal of Network and Computer Applications 32, no. 4.2009.

[10] A. B. Campbell, Applied Chaos Theory: A paradigm for complexity, Academic Press Inc., pp. 81-125, 1993.

[11] I.A.Ismail,Mohammed Amin and HossamDiab “An Efficient Image Encryption Scheme Based chaotic Logistic Map”, International Journal of Soft Computing,285-291,2007.

[12] ZhangYiWei, WangYuMin and ShenXuBang “A chaos-based image encryption algorithm using alternate structure”, Springer-Verlag, Science in China Series F: Information Sciences 2007.