Ch. Seetha Devi* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.5, Issue No.3, April – May 2017, 6514-6516.

A Novel Approach Image Encryption Based On Logistic Map

CH.SEETHA DEVI
M.Tech Student, Department Of CSE,
Gudlavalleru Engineering College

Dr. M. BABU RAO, M.Tech, Ph.D
Professor & HOD Of CSE, Department Of CSE,
Gudlavalleru Engineering College

Abstract: **The paper present s a novel approach image encryption based on logistic map. Present days, multimedia messages are exchanged based on internet. Security threats are drastically increasing over the internet. So, security messages are handling by different cryptographic methods in digital image processing. In the paper, proposed method follows 4 steps. Firstly, apply logistic map to the original image and cover image. The original image pixel values are subtract with the summation of corresponding pixel values of the resultant of original and cover image pixel values. The attackers are difficult to decrypt the original image from encode image because of the exact parameter pixels used for the logistic maps to get the original image, which is difficult to guess the parameters. The proposed method has analysis the results and different measurement analysis as shown in experimental section**.

Keywords:- **Cryptographic; Chaotic Map; Logistic Map;**

I. INTRODUCTION

In recent years, more and more consumer electronic services and devices, such as mobile phones and PDA (personal digital assistant), have also started to provide additional functions of saving and exchanging multimedia messages [2], [3], [4]. The prevalence of multimedia technology in our society has promoted digital images and videos to play a more significant role than the traditional dull texts, which demands a serious protection of users' privacy. To full fill such security and privacy needs in various applications, encryption of images and videos is very important to frustrate malicious attacks from unauthorized parties. Due to the tight relationship between chaos theory[6],[5] and cryptography, chaotic cryptography have been extended to design image and video encryption schemes. Chaos theory [1], [5], [6] describes the behavior of certain nonlinear dynamic system that under specific conditions exhibit dynamics that are sensitive to initial conditions. The two basic properties of chaotic systems are the sensitivity to initial conditions and Mixing Property. In this paper, 1 D [7] chaotic map is used to produce the chaotic sequence and used to control the encryption process. The chaos streams are generated by using various chaotic maps. Among the various maps, four maps are investigated and their characteristics are analyzed. In the real world, text-based identities are quite common for identity representation. Nevertheless, there are some limitations with a text-based approach. For example, the identity information is quite long that they can be hard to remember.

The identity information could be created in a different combination order in encryption and key generation, such that the descriptor has to apply a new private key for it. Biometric traits such as fingerprint, face, iris and hand geometry can be also used to represent the identities of users due to their unique biological features. In contrast to traditional text-based identities, people do not need to remember their biometric identities. With the advance of technology, biometrics readers have been rapidly developed and deployed.

II. EXISTING METHOD

Fuchun Guo [8] introduce a new encryption notion called distance-based encryption (DBE) to apply biometrics in identity based encryption. The adopted distance measurement is called Mahalanobis distance, which is a generalization of Euclidean distance. This novel distance is a useful recognition approach in the pattern recognition and image processing community. The primary application of this new encryption notion is to incorporate biometric identities, such as face, as the public identity in an identity-based encryption.

In such an application, usually the input biometric identity associated with a private key will not be exactly the same as the input biometric identity in the encryption phase, even though they are from the same user. The introduced DBE addresses this problem well as the decryption condition does not require identities to be identical but having small distance. The closest encryption notion to DBE is the fuzzy identity-based encryption, but it measures biometric identities using a different distance called an overlap distance (a variant of Hamming distance) that is not widely accepted by the pattern recognition community, due to its long binary representations.

III. PROPOSED METHOD

The block diagram of proposed method as shown in fig.1 and 2.

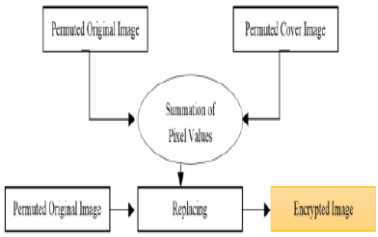


Fig.1. Encrypted image of proposed method

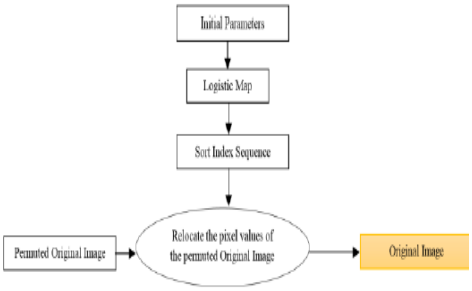


Fig.2. decrypted image of proposed method

The proposed method used logistic map to original image pixel values and then subtract with the summation of corresponding pixel values of the resultant of original and cover image pixel values. The logistic map that can be mathematically represented as follows:

$$Xn+1=r\ Xn(1-Xn) \quad (1)$$

Where Xn is the logistic map of input image pixel value and output pixel value , r is the radiur and lies between the interval of [0,4] in which, the chaotic behavior is achieved when r is 3.9999. In our encryption algorithm we used the Pixels Mapping Arrays (PMA) to Shuffle the logistic map .The concept of logistic map is chaos map. A chaos map can be achieved more efficiently when the chaotic systems exhibit a more sensitivity to initial conditions , where chaos map characteristic of the logistic map for the range values of 3.57 and 4.32 . A common source of such sensitivity to initial conditions is that the map represents a repeated folding and stretching of space where it is defined. The quadratic difference equation describing the logistic map may be thought of as a stretching-and-folding operation on the interval (0, 1).

A fast logistic map-based on image encryption system using 32-bit precision representation with variable point arithmetic is used to get a better throughput and facilitate hardware equipment. The data encryption system is based on a pseudo-random key stream generator on a cascade of chaotic maps, because of sequence generation and random mixing . Unlike the other existing methods like chaos-based methods, the proposed key stream generator not only achieves a very fast throughput, and also passes the statistical tests of up-to-date test suite even under quantization.

a) Encrypted image

Logistic Map is generated keys that is a fixed value and an initial value .The initial parameters important role in chaotic techniques. The range of initial parameters values to be generated is based on the original image pixel values and then logistic map is sorted. The parameter values are reshaped to the 2D dimension of the image before and after sorting. The current position change in the parameter values before and after sorting is determined and the same location of pixel values is changed. Thus the permutation values is achieved in image pixel level. The similar step is carried out on another cover image. This cover image is strengthening the encryption mechanism as the cover image is known only to the receiver using which retrieval of original image is possible. The image permuted parameter values of the cover and original are subtract with the summation of corresponding pixel values of the resultant of original and cover image pixel values. This process steps in the image encrypted that can be transmitted.

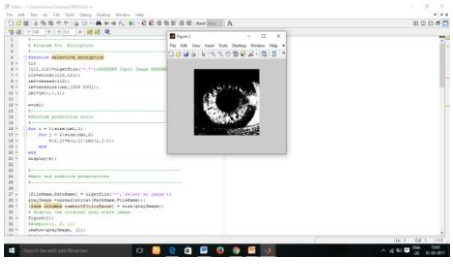
b) Decrypted image

At the receiver receive the cover image and parameters to be fed to the logistic map. The receiver has to retrieve the cover image from the encrypted image using logistic map.

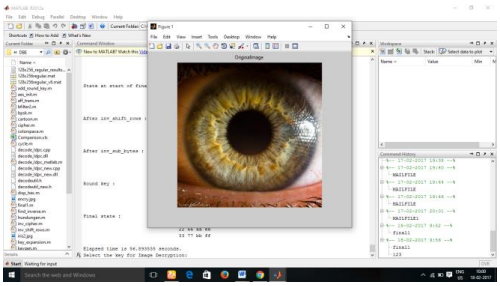
The logistic map is generated with the same parameters and it is then sorted. The pixel values of original image and sorted logistic maps values are reshaped to the 2D dimension of the image. After that, we receive the permuted original image and compared with the logistic map arrays pixels. Once they are scrambled then the image would be decrypted and the original image would be obtained.

IV. EXPERIMENTAL RESULTS

The construction of DBE from IPE with reasonable sized private keys and cipher texts. A new IPE scheme with the shortest private key. Speedup the process.



Decrypted iris image.



The original image of iris.

V. CONCLUSION

The image encryption and decryption is most important for the secure transmission over the internet. A new symmetric encryption scheme based on logistic map has been proposed. In the work the original image pixel values are subtract with the summation of corresponding pixel values of the resultant of original and cover image pixel values. The proposed method has better results and accurate measurements compare to exiting method [8].

VI. REFERENCES

[1]. D. Van De Ville., W. Philips., R. Van de Walle.,I. Lemahieu., : Image scrambling without bandwidth expansion. IEEE Transactions Circuits and Systems for Video Technology, vol. 14, pp. 892-897, (2004)

[2]. M. Yang., N. Bourbakis., L. Shujun. : Data-image-video encryption. Potentials, IEEE, vol. 23, pp. 28-34, (2004)

[3]. Yi, C. H. Tan., C. K. Siew., R. Syed.,: Fast encryption for multimedia. IEEE Transactions on Consumer Electronics, vol. 47, no. 1, pp. 101–107 (2001)

[4]. J. Kuo., M. S. Chen.,: A new signal encryption technique and its attack study. in Proc. IEEE International Carnahan Conference On Security Technology, pp. 149–153, Taipei, Taiwan (1991)

[5]. M. Macq .,J.-J. Quisquater., : Cryptology for digital TV broadcasting. Proceedings of the IEEE, vol. 83, no. 6, pp. 944–957 (1995)

[6]. S. Parker., L. O. Chua., :Chaos: a tutorial for engineers. Proceedings of the IEEE, vol. 75, no. 8, pp. 982–1008 (1995)

[7]. W.Wu .,N. F. Rulkov., :Studying chaos via 1-Dmaps—a tutorial. IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications, vol. 40, no. 10, pp. 707–721 (1993)

[8] Fuchun Guo, Willy Susilo: Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 2, FEBRUARY 2016

