International Journal of Engineering Research in Computer Science and Engineering
(IJERCSE)
Vol 4, Issue 8 , August 2017

“Hybrid technique of Image Encryption to Enhance Security”

[1] Kalyani D. Kadukar, [2] Prof.R. Krishna
[1] Student Of M.Tech.(CSE), R.C.E.R.T, Chandrapur, India
[2] Department (CSE),R.C.E.R.T, Chandrapur, India

***Abstract*— The aim of this project is related to novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery ,3D chaos generation,3D histogram equalization, row rotation, column rotation and XOR operation phases. Additional message are embed into some cover media, such as military or medical images, in a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message is called reversible data hiding. Separable reversible data hiding, the name its self indicates that it is a separable reversible data technique .That is it is reversible data technique but which is separable. The separable means which is able to separate .The separation of activities i.e. extraction of original cover image and extraction of payload is done in this method. This separation requires some basic cause to occur. In separable data hiding key explained by Xinpeng Zhang the separation exists according to keys. Digital images has increased rapidly on the Internet. Security becomes increasingly important for many applications, confidential transmission, video surveillance, military and medical applications. The transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks.**

***Keywords*— Encryption,3D chaos method ,Data embedding ,Decryption.**

INTRODUCTION

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors. The purpose of encryption is to ensure that only somebody who is authorized to access data (e.g. a text message or a file), will be able to read it, using the decryption key. Somebody who is not authorized can be excluded, because he or she does not have the required key, without which it is impossible to read the encrypted information.

Encryption has long been used by military and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage. Encryption can be used to protect data "at rest", such as information stored on computers and storage devices (e.g. USB flash drives). In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail. Digital rights management systems, which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering, is another somewhat different example of using encryption on data at rest.

Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Data should also be encrypted when transmitted across networks in order to protect against eavesdropping of network traffic by unauthorized users.

II. PROPOSED SYSTEM

1.Implementation and calculation, in the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data.

2.In Data Embedding phase, some parameters are embedded into a small number of encrypted pixels. Then extract it to original image.

3.We give extract image is an input for next step(phase) i.e 3D generation chaos method then further.

4.At the end XOR will be done on an image.

5.Comparison of this algorithm with different algorithms.

6. Both encryption and decryption will be done in the project.

III. DESIGN MODULES

1. Encryption module :

3D Chaos generation:-

The logistic map is the simplest process of chaos generation given by an equation:-

$$x_{n+1} = \mu x_n(1 - x_n)$$

For 0< X n<1 and μ= 4 is the condition to make this equation chaotic. Hongjuan Liu. et al proposed the 2D logistic map by using quadratic coupling for enhanced security and its extended 3D version are proposed given by following formula:

$$x_{n+1} = \gamma x_n(1 - x_n) + \beta y_n^2 x_n + \alpha z_n^3$$

$$y_{n+1} = \gamma y_n(1 - y_n) + \beta z_n^2 y_n + \alpha x_n^3$$

$$z_{n+1} = \gamma z_n(1 - z_n) + \beta x_n^2 z_n + \alpha y_n^2$$

Chaos Histogram Equalization:-

For higher security we need to equalize the histogram . If a gray image with M x N dimensions where M is the number of row and N is the number of columns then equalize histogram by following formula:-

$$x = \big(integer(x \times N2)\big) mod\ N$$

$$y = \big(integer(y \times N4)\big) mod\ M$$

$$z = \big(integer(z \times N6)\big) mod\ 256$$

N2, N4, N6 are a large random number generally greater than 10000. For the simplicity we also consider N2,N4 and N6 are equal. Fig. shows equalized histogram by using N2=N4=N6=100000,M=256,N=256.

Row Rotation:-

This rotation is same like as a combination lock of a briefcase .For rotation of row of a gray image have a dimension of M x N we need to select M number of chaos sequence.

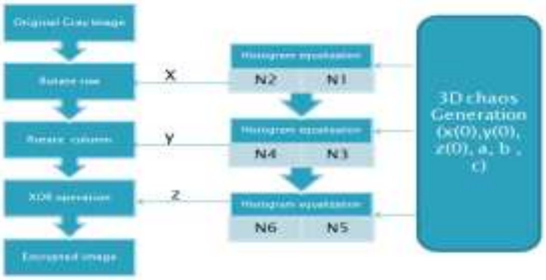
Column Rotation:-

Column rotation is same like as row rotation. For the rotation of row a gray image have a dimension M x N we need to select N number of chaos sequence.

XOR Operation:-

The last step of this encryption process is XOR opration.XOR operation change the pixel value into new value and can't reverse without knowing chaos key.

The representation of modules diagrammatically is as below:-



Encryption technique using 3D chaos

Image Encryption:-

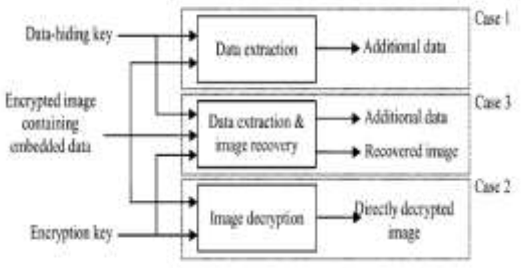
The original image in uncompressed design and each pixel with gray value coming under[0,255], denoted by 8 bits. In encryption stage, the XOR results of the original bits and pseudo-random bits are calculated.

Data Embedding:-

In the data embedding stage, some parameters are embedded into a small number of encrypted pixels and the LSB of the other encrypted pixel are compressed to create a space for inserting additional data and the original data at the location occupied by the parameters.

Data Extraction and Image Recovery:-

In this stage, the three cases are taken into account that a receiver has only the data-hiding key, only encryption key, and both the data hiding and encryption keys, respectively.



Three cases at receiver side of the proposed separable scheme

In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data.

2. Decryption module :

This will be done in next module. The reverse process will be done.

IV. RESULT

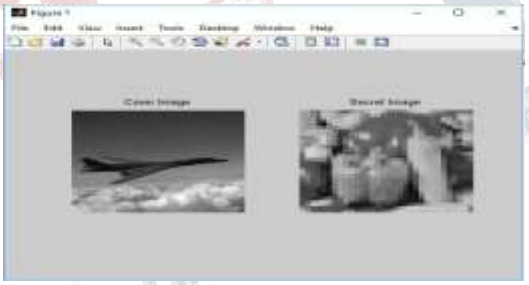


Fig 1: cover image and secret image

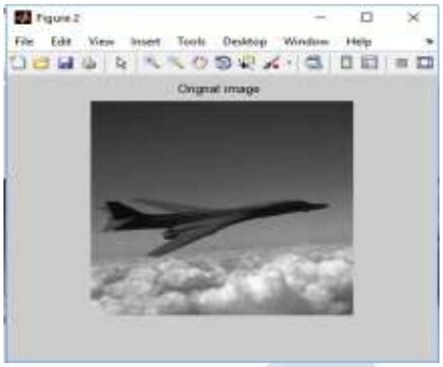


Fig 2: original image

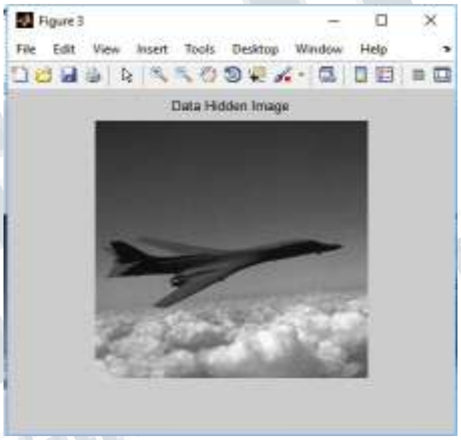


Fig 3:Data hidden image

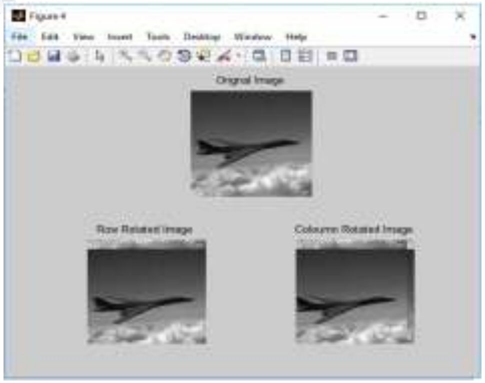


Fig 4:Row & column rotated image

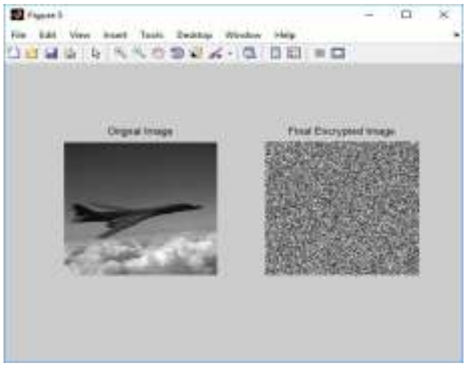


Fig 5:Final encrypted image

V. CONCLUSION

The project is divided into two parts(modules).The first modules will be of encryption in which fig 1.shows that the cover image and secret image is extracted ,fig 2 the original will be extracted, fig 3 the data will be hidden at this point, fig 4 the hidden image will be rotated as row wise and column wise and at last step i.e. fig 5 we will get encrypted image.

In this paper encryption is done.

REFERENCES

[1] X. Zhang,(2011) "Reversible data hiding in encrypted image," IEEE Signa Process. Lett., vol. 18, no. 4, pp. 255–258..

[2] Chia-Chen Lin, Pei-Feng Shiu, "DCT-based Reversible Data Hiding Scheme" , JOURNAL OF SOFTWARE, VOL. 5, NO. 2, FEBRUARY 2010

[3] Zhicheng Ni Yun-Qing Shi, Nirwan Ansari, and Wei Su (2011) , "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol, vol. 16, no. 3, Mar 2006,pp. 354-362.

[4] Xinpeng Zhang, (2013) "Separable Reversible Data Hiding in Encrypted Image", IEEE transactions on information forensics and security, vol. 7, NO. 2, APRIL 2012.

[5] Srivastava, A., "A survey report on Different Techniques of Image Encryption". International Journal of Emerging Technology and Advanced engineering. Vol. 2, pp. 163-167. 2012

[6] S. Lian., "A Block Cipher Based on Chaotic Neural Networks".Elsevier, Neurocomputing, vol. 72, pp. 1296-1301, 2009.

[7] Bhatnagar, G., & Wu, Q., "Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission". Instrumentation and Measurement, IEEE Transactions on, 61(4), 876-887. 2012.

[8] Chang, C. C., Hwang, M. S., Chen, T. S., "A new encryption algorithm for image cryptosystems". Journal of Systems and Software, 58(2), 83-91. 2001

[9] Schneier B., "Applied Cryptography: Protocols, Algorithms, and Source Code in C", John Wileyand Sons, New York, 1996. 2002.

[10] Kwok H. and Tang W., "A Fast Image Encryption System Based on Chaotic Maps With Finite Precision Representation," Chaos, Solitons and Fractals, vol. 32, no. 4, pp. 1518-1529, 2007.

[11] L. Kocarev., "Chaos-Based Cryptography: A Brief Overview". IEEE Circuits and Systems, 1(3):6–21, 200.

[12] J. C. Yen and J. I. Guo, "A new image encryption algorithm and its VLSI architecture." in Proceedings of IEEE workshop on signal processing systems, pp. 430–437, 1999.

[13] J. C. Yen and J. I. Guo, "A new chaotic key-based design for image encryption and decryption." in Proceedings of IEEE International Symposium on Circuits and Systems, Vol.4, pp. 49–52, 2000.

[14] L. Zhang, X. Liao, X. Wang, "An image encryption approach based on chaotic maps." Chaos, Solitons and Fractals, vol. 24, no. 3, pp. 759–765, 2005.

[15] C. Dongming, Z. zhiliang, Y. Guangming, "An Improved Image Encryption Algorithm Based on Chaos." in Proceedings of IEEE International Conference for Young Computer Scientists, pp. 2792-2796, 2008.

[16] A. N. Pisarchik, N. J. Flores-Carmona and M. Carpio-Valadez, "Encryption and decryption of images

with chaotic map lattices." Chaos Journal, American Institute of Physics, vol. 16, no. 3, pp. 033118-033118-6, 2006.

[17] Li Xiongjun , Peng Jianhua , Xv Nin, "A Image Encryption Algorithm Based on Two-dimensional Chaotic Sequence", Journal of Image and Graphics , 2003 , 8(10) : pp. 1172-1177.

[18] N. K. Pareek, V. Patidar, K. K. Sud, "Image encryption using chaotic logistic map." Image and Vision Computing, vol. 24, no. 9, pp. 926–934, 2006.

[19] Pawan N. Khade and Prof. Manish Narnaware, "3D Chaotic Functions for Image Encryption", International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, PP 323-328, May 2012.

[20] Y. Mao, S. Lian, and G. Chen, "A novel fast image encryption scheme based on 3D chaotic Baker maps." International Journal of Bifurcation and Chaos, vol. 14, no. 10, pp. 3616–3624, 2004.

[21] G. Y. Chen, Y. B. Mao, C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps." Chaos Solitons and Fractals, vol. 21, no. 3, pp. 749-761, 2004.

[22] Zhou Zhe, Yang Haibing, Zhu Yu, Pan Wenjie, Zhang Yunpeng, "A Block Encryption Scheme Based on 3D Chaotic Arnold Maps", International Asia Symposium on Intelligent Interaction and AffectiveComputing, 2009.

[23] Hongjuan Liu, Zhiliang Zhu, Huiyan Jiang, Beilei Wang, "A Novel Image Encryption Algorithm Based on Improved 3D Chaotic Cat Map",The 9th International Conference for Young Computer Scientists, 2008.