IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Study on Different Image Encryption Technique

Kalyani Kadukar[1], Prof. R. Krishna[2]

Department of Computer Technology, Rajiv Gandhi College of Engineering, Research & Technology[1,2]

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, and 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 technique, Data Hiding, Decryption.

I. 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. LITERATURE REVIEW

[1] "Md.Billal Hossain, Md.Toufikur Rahman" Multimedia data contains text, audio, video, graphic, images and with the increasing use of multimedia data over internet, here comes a demand of secure multimedia data. Image encryption differs from other multimedia components encryption due to some intrinsic features, such as bulk data capacity and high correlation among pixels the earlier encryption techniques such as AES, DES etc. are not suitable for practical applications. The combination of chaotic theory and cryptography forms an important field of information security. The latest trend in image encryption is chaos based for some unique characteristics such as the sensitivity to initial conditions, non-periodicity, non convergence, and control parameters. There are a lot of image encryption algorithms

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

based on chaotic maps have been proposed some of them are time consuming and complex some have little key space. In this paper we proposed a non-linier 3D chaos based simple encryption technique where for the first time 3D chaos is used for position permutation and value transformation technique. We get average entropy of encrypted image 7.99, NPCR of 99.6% and UACI of 33.5%. We tabulate correlation coefficient value both horizontal and vertical position for cipher and original image and compare performance of our method with some existing methods. We also discuss about different types of attack, key sensitivity, and key space of our proposed approach.

[2] Zhicheng Ni and et.al studied a reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the hidden data have been extracted. This algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. It can embed more data than many of the existing reversible data hiding algorithms. They proved analytically and shown experimentally that the peak signal-to-noise ratio (PSNR) of the marked image generated by this method versus the original image is guaranteed to be above 48 dB. The computation of this technique is quite simple and the execution time is rather short. Although this lossless data hiding technique is applied to still images, it is also applicable to videos which consist of a sequence of images. Instead, the key issue is if the histogram has maximum and minimum points, i.e., if the histogram changes up-and-down enough. An extreme example in which this algorithm does not work is an image having an exactly horizontal histogram .

[3] Chia-Chen Lin et. al propose a DCT-based reversible data hiding scheme. Their proposed layer-1 strategy considers some areas not used by Chang et al.'s scheme, which call layer-2 data embedding. This method applied Tian's pixel expansion method to design their layer-1 data embedding strategy Their experimental results confirm that the hiding capacity provided by combining this strategy with Chang et al.'s is higher than that provided by the Chang et al. approach alone. Moreover, the image quality of stego-images with this scheme remains above 30 dB for most test images, which is better than the best image quality offered by Changet al.'s scheme. Finally, the security and reversibility of Chang et al.'s scheme is unaffected when their layer-2 scheme is combined with our proposed layer-1 scheme.

[4] X. Zhang presented a practical scheme satisfying the requirements. A content owner encrypts the original image using an encryption key, and a data-hider embeds additional data into the encrypted image using a data-hiding key yet he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key.Image encryption involves generation of encryption key and generation of pseudo-random sequence. Encryption key is 128 bit value. It is generated randomly by using the random function. The random function generates the random key in an uniformly distributed function. Instead Pseudo random sequence consists of random bits generated using the encryption key. In our system, RC-4 algorithm is used to create the pseudo- random sequence using the 128-bit encryption key. It is represented as sequence of bytes (An array of bytes). The number of bytes generated should be equal to the number of pixels in the input image provided the pixels are represented as 8-bit values. If the pixels are represented as 16-bit values then the number bytes in pseudo-random sequence should be double the number of pixels.

III. PROPOSED PLAN OF WORK

The main goal of this research work is to secure the data or images by using encryption method. The project is divide into five module which are as follows. Out of which, we are working now on 1st and 2nd module which generate 3D chaos and also gives chaos Histogram Equalization.

- 3D Chaos generation
- Chaos Histogram Equalization.
- Row Rotation.
- Column Rotation.
- XOR operation.

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:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

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

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:-

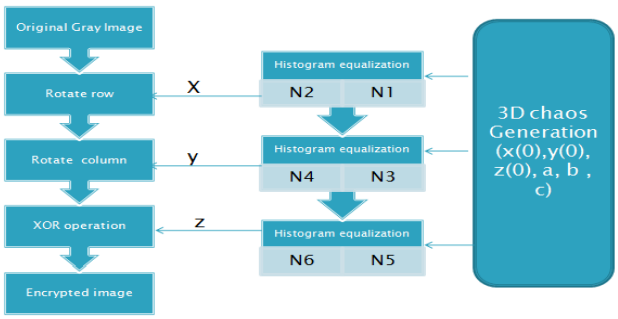

Fig 1: Encryption technique using 3D chaos

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.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

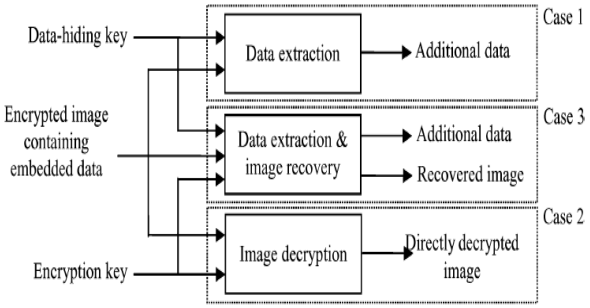

Fig 2: Three cases at receiver side of the proposed separable scheme

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.

IV. PROPOSED PLAN OF WORK

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.

V. CONCLUSION

We proposed a 3D chaos based simple encryption technique with combination of position permutation techniques and value transformation techniques. Though pixel position permutation and XOR operation for value transformation is not a new concept for image encryption but to our knowledge, it is the first time that chaos has been used for position permutation. We can use this algorithm for low, medium and high security purpose by controlling its complexity. We can easily skip any step which reduces key size and complexity. However, we show by experimental results that our algorithm is sensitive to initial conditions and strong against the brute force attacks.

REFERENCES

1. "Md.Billal Hossain, Md.Toufikur Rahman 3rd INTERNATIONAL CONFERENCE ON INFORMATICS, ELECTRONICS & VISION 2014"
2. Xinpeng Zhang "Separable Reversible Data Hiding in Encrypted Image," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012
3. X. Zhang,(2011) "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258..
4. Chia-Chen Lin, Pei-Feng Shiu, "DCT-based Reversible Data Hiding Scheme", JOURNAL OF SOFTWARE, VOL. 5, NO. 2, FEBRUARY 2010.
5. Zhicheng Ni Yun-Qing Shi, Nirwan Ansari, and Wei Su (2011) , "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technology, vol. 16, no. 3, Mar 2006,pp. 354-362.
6. Xinpeng Zhang, (2013) "Separable Reversible Data Hiding in Encrypted Image", IEEE transactions on information forensics and security,vol.7,NO.2,APRIL2012.