A NOVEL SURVEY ON IMAGE ENCRYPTION

Vaishali D. Kamble [1], Prof. Kanchan Doke [2]

[1,2]Bharati Vidyapeeth College of Engineering, University of Mumbai

---

Abstract - *Encryption consist of finite set of instructions which converts plain text into cipher text. Plain text is the readable data and cipher text is the unreadable data. Therefore, the encryption is nothing but the encoding of data from readable to unreadable format. For encryption algorithm requires a set of characters known as key to encrypt or decrypt data. By using key we can encrypt or decrypt the plaintext into cipher text and then cipher text into plain text. Encryption is a part of cryptographic techniques. Only the authorized person can access the data. Cryptography deals with Confidentiality, Integrity, Non-repudiation, Authentication, Cryptography.*

Key Words*: *Image encryption, Image decryption, Chaos based image encryption, Security analysis.

1. INTRODUCTION

Nowadays, securing information becomes more important. Images are widely used for different process. Therefore, securing of image data from unauthorized users become more important. Image encryption is very important part in hiding of information. In image encryption method the information is prepared as unreadable so that not any hacker or eavesdropper including server administrators and others have access to original data. Encryption can be used in various places such as corporate, military and personal information. The cryptography consist of two types symmetric and asymmetric. The symmetric system consist of same key means secret key to encrypt and decrypt data. The asymmetric system consist of one key means public key to encrypt the data and private key to decrypt the data.

1.1 LITERATURE SURVEY

1. Secure image encryption technique for wireless network.

In this paper, the image encryption is done using threshold technique. The threshold technique is used to share the images. This technique is used to produce two or more shares of any images. After this process, the block transformation is used for encryption of the shares and then they concatenate the shares to produce a single image. The block transfer is used for the high level of security. In this technique, the image is divided into two shares and the segments into blocks. A new key generation technique is used for symmetric key generation and then the bit shifting method used for encryption. When the two images is produce using encrypted transform then the concatenation of these image is performed to produce a single image which will be transfer through wireless media. In the receiver side the reverse process is been applied.

2. New image encryption algorithm based in diffie hellman and singular value decomposition.

In this paper, a new technique is been used known as diffie hellman and singular value decomposition for image encryption. There are three various steps for image encryption such as scrambling the values of image by using Fibonacci series, to generate public key and private using diffie hellman key exchange, keys are used to encrypt the diagonal of matrix which is used to make singular value decomposition. The decryption process is the inverse of encryption.

3. Medical image encryption based on multiple chaotic mapping and wavelength transform.

This paper proposes the new image encryption algorithm based on improved logistic mapping, Arnold mapping, kent mapping and wavelength transform. The Arnold mapping and the wavelength mapping is used for shuffling image pixels. The kent mapping is used to generate control parameter in the Arnold mapping.

4. Proposed hyperchaotic system for image encryption.

This paper proposed a new technique called hyper chaos system based on henon and logistic maps. This consist of three process such as transformation process, Diffusion key generation using discrete hyperchaotic system generator and Diffusion process. In transformation process, the plain image is divided into 8*8 non overlapping blocks that are transformed using 2D. In diffusion key generation for each iteration the three key stream element can be obtain from the current state of the hyper chaos system. In diffusion process, the selective encryption approach is applied on DC and the first two AC coefficients. Those coefficient are selected from each block and then it can encrypted using one key of three generated keys using hyperchaotic system.

5. Robust image encryption based on balanced cellular automation and pixel separation.

In this paper, a new technique is proposed for digital image encryption using 2D cellular automation and pixel separation. The sender and receiver exchange the secret information. Based on the selected seed the 2D cellular automation is extended using moore neighbourhood to generate pseudo random key images. Encryption is performed by using combining the source image with the help of key image. The pseudo random key image is generated using balanced cellular automaton rules and are applied on binary levels. Rules are formed using extended moore neighbourhood which helps to extend the key space.

6. A simple and practical color image encryption with the help of QR code.

In this paper, quick response (QR) code is used for simple and practical method for color image encryption. This technique is proposed using joint transform correlated (JTC) architecture. In this during encryption, the original color image is transform using QR code and the QR code is encoded into a positive ciphertext by using the JTC encryption architecture. In decryption process the QR code can be recovered using decryption key. In encryption, there are two steps, the original color image is converted into corresponding QR code. The QR code is encrypted into a ciphertext by using encryption system.

7. Encryption decryption RGB color image using matrix multiplication.

In this paper, a new technique is been used color image encryption based on random matrix key encoding. For encrypting the color image there will be separation of three colors such as red, green and blue (RGB) channels. Each channel is encrypted using double random matrix key encoding. Then the three new coding image matrices are formed.

8. Generating visually meaningful encrypted image using image splitting technique.

In this paper, the proposed method splits the color image into three images such as red, green and blue which are encrypted separately. After that it is merged into single color image and then the wavelet transform is applied to render the encrypted image. Wavelet are used in image processing to show the images in various levels of resolution. This process can be done by dividing the images into small regions called as sub bands. This sub bands can be used for compression. For encrypting the image is divided into three bands of images based on images Of RGB. Then the (AES) algorithm is used with three times using the three different keys.

9. Quantum color image encryption based on multiple discrete chaotic systems.

In this paper, the new quantum encryption for color image is proposed with the help of multiple discrete chaotic system. This process is done with the help of Not image generated by logistic chaotic map, asymmetric tent map and logistic chebyshev map to control the XOR operation in the encryption process. It helps in the efficiency as well as security against differential and statistical attacks.

10. Enhanced blowfish algorithm for image encryption and decryption with supplementary key.

In this paper, blowfish algorithm technique is proposed. The algorithm consist of enhanced features of blowfish. It is enhanced using supplementary key where it is used to strengthen the security of image. The security of the method is measure using different data set.

2. METHODS AND TECHNOLOGIES

1. Block based transformation

This technique is used to produce two or more shares of any images. After this process, the block transformation is used for encryption of the shares and then they concatenate the shares to produce a single image. The block transfer is used for the high level of security. In this technique, the image is divided into two shares and the segments into blocks. A new key generation technique is used for symmetric key generation and then the bit shifting method used for encryption. When the two images is produce using encrypted transform then the concatenation of these image is performed to produce a single image which will be transfer through wireless media. In the receiver side the reverse process is been applied.

2. Diffie Hellman key exchange, Singular value decomposition

It is a method of key exchange cryptographic key over a pubic channel. It is used to securely communicate between two parties. They first exchange the keys by using secure channel such as paper key lists transported using a trusted courier. The Diffie-Hellman key exchange method allows the two parties which they have no prior knowledge of each other to establish a shared secret key over an insecure channel. This key can then be used to encrypt having subsequent communication using a symmetric key cipher. It is used to secure various of internet services. It is non-authenticated key agreement protocol. It is used to shared secret information between two parties.

3. Logistic map, Kent map, Arnold map

The logistic map is a mapping of polynomial of degree 2. It a chaotic behavior which can arise from a simple non linear dynamical equation. Arnold cat map is a chaotic map from the torus itself. As it is a demographic model the logistic map has pathological problem that some of the initial condition and the parameter values leads to population sizes. Arnold map is nothing but the chaotic map. It is transformation applied to an image. The pixels of the image are randomly arranged. But when the transformation is repeated various times the original image will reappear.

The transformation consist of some of the principles of chaos.

4. Henon map

It is a discrete time of dynamical system. It is a suitable example of dynamical system that exhibit chaotic behavior. The maps depends on the two parameters such as a and b. The henon consist of points (Xn,Yn) in the new plane. A initial point of the plane will either approach a set of points known as henon strange attractor or infinity of diverge.

5. Cellular automata, Pseudo random key image generation

Cellular automata contain grid of cells each one having finite state A. The CA can be represented using C, S, N, F where, C is a cellular space, S is a state space, N is 'n' cell, F is a function consist of set of rules. Cellular automata is a array of identically programmed of automata and cells. The grid of the cellular automata consist of finite number of dimensions. The each cell of cellular automata is known as neighborhood and it is defined to specified cell. The initial state is selected by using a state for each cell i.e. time t=0. Example: Stream cipher.

Pseudo random is nothing but the generation of sequence of number.whose properties is similar with sequence of random numbers. The generator sequence is not truly random random because it is determined by the initial values.

6. QR Code

QR code is nothing but the quick response code. It is a trademark of matrix barcode. It is a machine readable optical label which consist of information about the item attached with it. QR code uses four type of standardized modes of encoding such as numeric, alphanumeric, byte/binary, and kanji to store data efficiently, extensions may also be used. The QR code becomes famous because of its fast readability and greater storage capacity. The application of QR code consist of product tracking, item identification, time tracking, document management and general marketing. It is a black squares arranged in a square grid place on a white background which can be read with the help of camera and processed using reed. Then the required data is extracted from the pattern that are present in horizontal and vertical component of image.

7. Double random matrix key encoding, Matrix multiplication

The random matrix is nothing but the matrix random values. It is matrix consist of random variables. The product of the matrix is designed for the composition of linear maps which are represented using matrices. It is used in various areas such as applied mathematics, statistics, physics, economics and engineering.

8. Image splitting

Image splitting is nothing but the partitioning of digital image into multiple segments. The reason for doing this is to simplify and change the representation of image in such a way that it looks more meaningful and is easier to analyze. The process assign a label to each pixels which shares some characteristics of pixels with same labels. It a set of segments which covers all the image. Each pixels are same in the region having some characteristic such as color, intensity and texture. The regions which are in adjacent are different with same characteristic. In medical imaging the resulting contours after the partitioning can be used to create 3D reconstructions with the help of interpolation algorithm like marching cubes.

9. Asymmetric tent map

The tent map consist of the parameter of u is the real value function of fu which is defined by its tent like shape of the graph. The parameter of tent map consist of value u=2 and r=4. The tent map demonstrate a range of behaviour ranging from predictable to chaotic.

10. Blowfish

It is an image encryption algorithm which can be used as an replacement for DES. It is symmetric means secret or private block cipher which uses a variable length key. It consist of 32 bits to 448 bits and make it usable for both domestic and exportable use. It has a good encryption rate in software.

3. CONCLUSION

Based on these paper it is studied that encryption plays a vital role in everyday's life. Only the authorized users have the rights to access the data. The unauthorized user cannot access such information. We studied different image encryption techniques and their approaches for providing security. All the techniques have some advantages and disadvantages and therefore the new techniques have been evolved.

REFERENCES

[1] Kakali Chatterjee "Secure image encryption technique for wireless network", August 2015.

[2] Nidhal Khdhair El Abbadi, Samer Thaaban Abaas, Ali Abd Alaziz "New image encryption algorithm based in diffie hellman and singular value decomposition", 1 January 2016.

[3] Xiao Chen, Chun Jie Hu "Medical image encryption based on multiple chaotic mapping and wavelength transform", 2017.

[4] Dr. Karim Alia "Hyperchaotic System for Image Encryption**",** 2016.

[5] Dijana TRALIC, Sonja GRGIC "Robust image encryption based on balanced cellular automaton and pixel separation", 10 March 2016.

[6] Xiaopeng Deng, Xiang Zhu "A simple and practical color image encryption with the help of QR code**",** 2015.

[7] Mohamad M, Al Laham"Encryption decryption RGB color image using matrix multiplication", October 2015.

[8] Arunkumar S, Subramaniyaswamy V, Devika R, Logesh R "Generating visually meaningful encrypted image using image splitting technique", 8 August 2017.

[9] Li Li, Bassem Abd-El-Atty, Ahmed Ghoneim "Quantum color image encryption based on multiple discrete chaotic systems", 2017.

[10] Kanagalakshm K, Mekala M "Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key", July 2016.