A COMPREHENSIVE STUDY OF VARIOUS HIGH SECURITY ENCRYPTION ALGORITHMS

[1]J T Pramod, [2]N Gayathri, [3]N Jayaram, [4]T Geethanjali, [5]M Anusha

[1]Assistant Professor, [2,3,4,5]Student
[1]Department of Electronics and Communication Engineering
[1]Aditya College of Engineering, Madanapalle, Andhra Pradesh, India

Abstract: It is well known that with the rapid technological development in the areas of multimedia and data communication networks, the data stored in image format has become so common and necessary. As digital images have become a vital mode of information transfer for confidential data, security has become a vital issue. Images containing sensitive data can be encrypted to another suitable form in order to preserve the information in a secure way. Modern cryptography provides various essential methods for securing the vital information available in the multimedia form. This paper outlines various high secure encryption algorithms. Considerable amount of research has been carried out in confusion and diffusion steps of cryptography using various chaotic maps for image encryption. The chaos-based image encryption scheme employs various pixel mapping methods applied during the confusion and diffusion stages of encryption. Following the same steps of cryptography but performing pixel scrambling and substitution using Genetic Algorithm and DNA Sequence respectively is another way to securely encrypt an image. Generalized Singular Value Decomposition a matrix decomposition method a generalized version of Singular Value Decomposition suits well for encrypting images. Using the similar guidelines, by employing Quadtree Decomposition to partially encrypt an image is yet another method used to secure a portion of an image containing confidential information.

Index Terms **–Chaotic Maps, Quadtree, Genetic Algorithm, DNA sequence, GSVD.**

I. INTRODUCTION

In the modern age, images are the crucial mode of information exchange. They are used in a variety of applications like Military, Governments, Healthcare and personal messaging. Though certain applications don't need image security, to communicate highly sensitive confidential documents used by Military and Governments require various protection techniques that are not only powerful but efficient as well. Cryptography involves creating written or generated codes that allow secrecy of information. It converts data into an unreadable format so that no unauthorized entity can decode the information via the transmission. Confusion and diffusion are the steps involved to get a secure cipher. The confusion is a process of scrambling the digits of a text or image. The diffusion is a process of modifying the values of the digits and establishing a meaningful interdependency among the neighboring digits. For the information to be safe, cryptography can be applied on several levels. Once the information is transmitted, integrity must be maintained during the transit as well as during storage.

The information stored in the encrypted data cannot be read without a secret key. Once the data is delivered, it must be verified by the receiver using the same key used for encrypting it. This process is called decryption. Cryptography also allows authentication of data by the senders and receivers through the use of pair of keys. Some commonly used encryption algorithms include Secret Key Cryptography, also called Symmetric Encryption, where only one key is used for both encryption and decryption. The second one is Public Key Cryptography also called Asymmetric Encryption where two keys are used. One is a public key and the other is a private key. The information is encrypted by the sender using the public key and the receiver decrypts it using private key. As these keys can be either predicted or can be hacked using a brute-force attack, special kinds of encryption mechanisms are required for keeping secret information safe. Standard encryption algorithms like Advanced Encryption Standard, Data Encryption Standard and Triple DES though provide security in transferring information are not suitable for image encryption. The encryption using chaotic maps are computationally faster and are also efficient, hence they are widely used in image encryption. A Chaotic system is sensitive to initial conditions. Hence, the sequences produced using the chaotic system possess randomness and can be manipulated to possess a large key space that can be used to encrypt data such as speech, images, texts. The images with large sizes have a large amount of information and the encryption schemes cannot handle the problems arising such as compression in such cases. With the development of information technology and the propagation of the Internet and development of computer vision, the research on information security is becoming more and more vital.

II. METHODS OF ENCRYPTION

1. Data Encryption standard:

The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data. Its key length is short i.e., 56 bits. This short key length makes it insecure for most applications. It was developed based on an algorithm submitted to the National Bureau of Standards (NBS) to propose encryption standard for protecting sensitive and unclassified electronic Government data. However, this algorithm was weak against brute-force attacks. DES is insecure mainly due to the 56-bit key size being very small. The algorithm was believed to be practically secure in the form of Triple DES, although there are theoretical attacks.

2. Advanced Encryption Standard:

The Advanced Encryption Standard (AES) is a Rijndael block cipher. Rijndael is a family of ciphers with different key and block sizes. National Institute of Standards and Technology (NIST) established AES for encrypting electronic data usually for protecting sensitive government information. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, using three different key lengths which are 128, 192 and 256 bits. It replaces the Data Encryption Standard (DES). The algorithm used by AES is a symmetric-key algorithm, it means the same key is used for encrypting as well as for decrypting the data.

3. Encryption using Chaotic Maps:

Encryption based on a chaotic system is performed using the confusion and diffusion steps with the help of various chaotic maps. A chaotic map is an evolution function that exhibits some sort of chaotic behavior. There are several types of maps supporting one or more spatial dimensions. These maps may be used in the confusion and diffusion stage with proper choice to exhibit chaotic behavior which results in both position and value change of a particular digit in a text or image pixel. The chaos-based image encryption scheme can be implemented with half-pixel-level interchange permutation strategy. Here pixel swapping operation is performed between higher and lower bit planes in contrast to the traditional confusion operation. Some of the chaotic maps are listed below.

3.1 4-Dimensional Hyper-Lorenz map:

Hyper-Lorenz is a 4-dimensional chaotic map represented in the form of differential equations. It exhibits chaotic behavior for certain initial conditions. The System exhibits chaotic behavior when the parameters have values, $\alpha = 10, \gamma = 28$ and $\beta = 2.67$. It is mathematically expressed as,

$$\frac{dx}{dt} = \alpha(y - x) \quad (1)$$

$$\frac{dy}{dt} = \gamma x + y - xz - w \quad (2)$$

$$\frac{dz}{dt} = xy - \beta z \quad (3)$$

$$\frac{dw}{dt} = \kappa xy \quad (4)$$

3.2 3-Dimensional Lorenz map:

This model is a system of three ordinary differential equations now known as the Lorenz equations. The System exhibits chaotic behavior when the parameters have values, $\sigma = 10, \rho = 28$ and $\beta = 2.67$. It is mathematically expressed as,

$$\frac{dx}{dt} = \sigma(y - x) \quad (5)$$

$$\frac{dy}{dt} = x(\rho - z) - y \quad (6)$$

$$\frac{dz}{dt} = xy - \beta z \quad (7)$$

3.3 2-Dimensional Henon map:

Henon map is a discrete time dynamical system. It takes the point (x_n, y_n) in the image space and maps it to a new point. The initial value $x_0 \in (0,1)$ and $y_0 \in (0,1)$ can be used as the key to the point (x_0, y_0). The Henon map mainly depends on two parameters α and β. For $\alpha = 1.4$ and $\beta = 0.3$ the Henon map exhibits chaotic behavior. For other values of α and β the map may be chaotic, irregular, or join a periodic orbit. Mathematically it is expressed as,

$$x_{n+1} = 1 - \alpha x_n^2 + y_n \quad (8)$$

$$y_{n+1} = \beta x_n \quad (9)$$

3.4 2-Dimensional Gingerbreadman map:

In dynamical systems theory, the Gingerbreadman map is a chaotic two-dimensional map. It is given by the piecewise linear transformation,

$$x_{n+1} = 1 - y_n + |x_n| \quad (10)$$

$$y_{n+1} = x_n \quad (11)$$

3.5 1-Dimensional Logistic map:

The basic one-dimensional logistic map can be mathematically expressed as,

$$x_{n+1} = \alpha x_n(1 - x_k) \quad (12)$$

Where $x_k \in (0,1)$. The parameter α and the initial value x_0 can be used as a key to the point (α, x_0). The system is in chaotic condition when α ranges from 3.569 to 4.0.

3.6 1-Dimensional Circle map:

The circle map is given by iterating the map,

$$\theta_{n+1} = \theta_n + \Omega - \frac{K}{2\pi}\sin(2\pi\theta_n) \qquad (13)$$

where θ lies between 0 and 1. The system exhibits chaotic behavior when $K = 0.5$ and $\Omega = 0.2$.

Confusion step applied on an image to be encrypted:

1. Divide the image of fixed size to equal number of blocks of size 1×1 pixel.
2. Generate the chaotic sequence of length using the any chaotic map.
3. Permute the blocks according to the sequence generated in above step.

Diffusion step applied on an image to be encrypted:

1. Generate two random sequences using any suitable map of length equal to total number of rows and total number of columns respectively in the image.
2. XOR the obtained sequence with pixels in both row and column.
3. Establish interdependency among pixels in an image by performing XOR operation on previous row/column with current row/column.

4. Image Encryption using Genetic Algorithm and DNA Sequence:

A hybrid symmetric model can be created for encrypting images through combination of Genetic Algorithm and DNA sequence. DNA sequence is chosen as it offers greater storage and higher computing capabilities. The encryption method consists of two phases. They are the transposition or scrambling phase and the substitution phase. In the transposition phase, pixel locations are altered by using Genetic Algorithm to reduce the correlation among adjacent pixels. In the substitution phase, the pixels are replaced with new values by performing XOR operation between the pixel values in the form of binary strings and DNA substrings. The DNA substrings are derived from a random DNA string.

Encryption Process:

The encryption process involves the following steps:

1. The input image is converted to binary.
2. ***Pixel Scrambling:*** In this step, first the binary image is converted into a fixed size 256×256 matrix. Here, the matrix elements are the pixel values in binary. The Genetic Algorithm is then applied to permute the image pixels by changing their positions in the image. The scrambling of pixels is done based on the fitness value which is calculated as per the below shown equation.

$$f = n + \frac{(p0 + p1)}{m} \qquad (14)$$

   where, $f =$ fitness value, $n =$ total number of bits in a block, $p0 =$ percentage of pixels which are binary '0', $p1 =$ percentage of pixels which are binary '1', $m =$ maximum percentage
3. ***Pixel Substitution:*** In this final step, a random DNA string is considered and the string is divided into 8 substrings. Then the intensities of the individual pixels are substituted by applying XOR operation between the DNA substrings in binary form and the pixel intensities in binary. Here the DNA substrings act as symmetric keys for the transmission. These strings are known to the receiver too. This encrypted image is then transmitted to the receiver.

Decryption Process:

To perform decryption, steps used in the encryption process are performed in reverse order.

Reverse operation of Pixel Substitution

1. Read the image and convert it into a 256×256 matrix in which the matrix entries represent the image pixels.
2. Divide the 256×256 matrix into 32×32 matrix by taking each block of size 8×8.
3. Using the same eight DNA substrings created during the encryption process, perform XOR operation between each block and the 8 substrings.
4. Repeat the above step for the remaining matrices with the same substrings.

Reverse Pixel Scrambling

1. Divide the 256×256 matrix into 32×32 matrix by taking 8×8 blocks.
2. Read the first four blocks of the matrix, i.e., the first & second blocks of first & second row.
3. Then the random number ρ generated at the sender end will be used to perform the following operations on the blocks
   a. if $(\rho < 0.2)$, no operation
   b. else if $(0.2 < \rho < 0.8)$, perform crossover
   c. else if $(\rho > 0.8)$, perform mutation
4. Repeat steps 2 & 3 for all the blocks. At the end we will get the 256×256 matrix form of the binary image.

5. Encryption using piecewise nonlinear chaotic maps:

Piecewise linear chaotic maps have efficient dynamical properties and can be realized in software as well as hardware in an easy way and hence they are widely used in designing digital chaotic ciphers. Even though an encryption system based on 1D chaotic maps has the advantage of high efficiency and extreme simplicity, there are certain essential drawbacks in such chaotic systems.

Issues such as small key space, slow encryption speed and weak security when only one particular type of chaotic map being used to design an encryption system. Such issues can be addressed using a nonlinear type of chaotic system called the piecewise nonlinear chaotic maps. In such a system, in addition to the initial conditions and control parameters used in the equation, probability is introduced. The inclusion of more than two control parameters increases the security at confusion and diffusion stages during the encryption process which results in a more secure cryptosystem. This is due to the fact that involving more than one chaotic map to perform multiple levels of confusion and diffusion stages makes the crypto system more secure and robust. Also, to improve the security of the chaotic system, the probability parameter of nonlinear piecewise chaotic maps can be adjusted by attaching it to trigonometric chaotic maps. The availability of two parameters in the trigonometric chaotic map increases the size of key space. A 1D trigonometric map is represented mathematically as,

$$x_N(n+1) = \frac{1}{\alpha^2} tan^2 \left[N tan^{-1} \left(\sqrt{x(n)} \right) \right] \qquad (15)$$

where α is the control parameter, n represents a pixel index if the input is an image and N is an integer greater than 1.

6. Image Encryption using Generalized Singular Value Decomposition:

The Generalized Singular Value Decomposition (GSVD) is a matrix decomposition mechanism more general than the Singular Value Decomposition (SVD). GSVD can be applied for image encryption and decryption. Its strength depends on the choice of the key image used in both encryption as well as decryption.

Encryption Process:

The encryption process involves the following steps:

1. Input an image A of any size.
2. Select an initial key c to generate the following two matrices:

$$\begin{cases} A_1 = c * A \\ A_2 = -c * A \end{cases} \qquad (16)$$

3. Choose an encrypting key image B.
4. Compute the GSVD for the matrices A_1 and A_2 with the encrypting key image B as follows:

$$\begin{cases} [u_1, v_1, x_1, c_1, s_1] = gsvd(A_1, B) \\ [u_2, v_2, x_2, c_2, s_2] = gsvd(A_2, B) \end{cases} \qquad (17)$$

5. Compute the following:

$$\begin{cases} AA_1 = u_1 * c_2 * x_1^T \\ AA_2 = u_2 * c_1 * x_2^T \end{cases} \qquad (18)$$

6. Construct the encrypted image F such that,

$$F = \begin{bmatrix} AA_1 \\ AA_2 \end{bmatrix} \qquad (19)$$

Decryption Process:

The decryption process involves the following steps:

1. Split the encrypted image F into AA_1 and AA_2.
2. Obtain the decrypted key image B which is the same key image used in encryption.
3. Compute the GSVD for each matrix $AA_1$and AA_2 using the decrypting key image B as follows:

$$\begin{cases} [u_1, v_1, x_1, c_1, s_1] = gsvd(A_1, B) \\ [u_2, v_2, x_2, c_2, s_2] = gsvd(A_2, B) \end{cases} \qquad (20)$$

4. Compute the original image A as follows:

$$A_1 = u_1 * c_2 * x_1^T \qquad (21)$$

$$A = \frac{A_1}{c} \qquad (22)$$

7. Partial Encryption using Quadtree Decomposition:

Quadtree Decomposition is a feature extraction step that involves subdividing an image into four blocks and each block into four more blocks and so on based on the homogeneity of the image pixels in each block. This process is repeated iteratively until each block meets a criterion. The criterion is usually a threshold calculated using the variance measure for all pixels in a block and comparing it with all the individual pixels. The result might have blocks of several different sizes. Blocks can be as small as 1×1 unless something else is specified during the process. This technique reveals information about the structure of the image. This pre-encryption step actually allows us to select a portion of the image to encrypt instead of the complete image. Once a portion of the image is selected any of the above said methods of encryption may be used to carry out the encryption. This type of partial

encryption can be applied for Government or Military documents containing certain highly sensitive text or images which are not to be revealed to the general public.

III. SUMMARY:

Various schemes of encrypting a text or multimedia files exits. Image encryption seems to be the most demanding application in the present-day scenario. Most of the Government and Military documents containing highly classified text or images are stored digitally and being shared within the departments electronically. Securing such documents seems a vital requirement now-a-days. This paper outlines few encryption methodologies starting from the most basic ones to the highly secure ones. DES, Triple DES and AES algorithms may be suitable to encrypt texts or short messages. To secure images and documents or enormous volumes, high speed, robust, efficient and hard-to-crack even with sophisticated brute-force attacks are required. Hence using more than one algorithm, exhibiting multi-level confusion and diffusion stages would provide high security. The partial encryption seems promising for encrypting only certain sections of an image document. Using a combination of multidimensional linear or nonlinear chaotic maps, GSVD or Genetic Algorithm to partially encrypt an image document may help reduce the encryption time and also provide high security.

IV. REFERENCES

[1] Revanna C R, Keshavamurthy C. 2019. A Novel Priority-Based Document Image Encryption with Mixed Chaotic Systems Using Machine Learning Approach. Electronics and Energetics, Facta Universitatis. 147-177.

[2] Li Liu, Yucheng Chen, Ruisong Ye. 2017. A Plain-Image Dependent Image Encryption Scheme Using Half-Pixel-Level Interchange Permutation Operation. International Journal of Network Security & Its Applications. 9(4): 57-75.

[3] Saswat K Pujari, Gargi Bhattacharjee, Soumyakanta Bhoi. 2018. A Hybridized model for image encryption through genetic algorithm and DNA sequence. Procedia Computer Science, Elsevier. 165–171.

[4] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan. 2008. A Novel Algorithm for Image Encryption Based on Mixture Of Chaotic Maps. Chaos, Solitons and Fractals, Elsevier. 408–419.

[5] Mohammed Abdul Hameed Jassim Al-Kufi, Hayder Raheem Hashim, Ameer Mohammed Hussein, Hind Rustum Mohammed. 2017. An Algorithm Based on GSVD for Image Encryption. Mathematical and Computational Applications. 22-28.

[6] Xiaobo Li, Jason Knipe, Howard Cheng. 1997. Image Compression and Encryption Using Tree Structures. Pattern Recognition Letters. Elsevier. 1253–1259.