Selective Image Encryption Using Chaotic and ARNOLD CAT'S MAP System

[1]Manoj N, [2]Kiran, [3]Vaishnavi R, [4]Kruthi M M

[1,2,3,4]Vidyavardhaka college of engineering, Mysore, Karnataka, India.

[1]manojnagendra6@gmail.com, [2]kiranhsn@vvce.ac.in, [3]vaishnavirangaswamy@gmail.com,

[4]kruthigsx8417@gmail.com

Abstract In recent days the usage of social network and the multimedia Sharing is rapidly increased. Due to loopholes in the network security, hackers are easily hacking the social networks. Many encryption and decryption algorithms are developed by the developers. But these algorithms are being outdated and being easy for hackers to breach the network. Therefore, these outdated methods fail to provide security against new attacks. This paper gives an overview on some of the encryption and decryption methods used in recent times such as selective image encryption using chaotic system. Protection of data or information plays a very big role in every field (Medical fields, Navy, Army & Air force). Therefore, this encryption technique can be used to safeguard the important data.

Keywords ---Chaotic algorithm, Decryption, Digital image encryption, Encryption, Information security, MATLAB.

I. INTRODUCTION

Encryption is a process of converting a plaintext into alternative form known as cipher-text. Everybody cannot decipher a cipher-text back to plaintext. It can only be deciphered by authorized person. Encryption scheme commonly uses a pseudo-random encryption key generated by an encryption algorithm. In olden days various forms of encryption have been used in cryptography. Olden techniques of encryption were often used in military messaging. Modern encryption techniques ensure security because modern computers are inefficient at cracking the encryption.

One of the earliest forms of encryption is symbol replacement. Symbol replacement encryption is non-standard. These techniques were used throughout Ancient Greece and Rome for military purposes. In recent days encryption is used in communication over interest for security and commerce.

Encoding an image with the help of different encryption algorithms and Making it inaccessible to unauthorized users is known as image encryption. Therefore, no hacker has access to original message or any other type of transmitted information through public networks such as internet.

Encryption of only a selective or partial section of an image or plan text is known as Selective image encryption. This reduces the time taken and be more efficient. This helps in reducing the complexity save cost and time. This method is also known as partial image encryption because only some parts of an image or some pixels of an image is encrypted with respect to make it more difficult to decrypt and easy to encrypt.

Information which is encrypted or encoded is known as cipher-text. It contains a form of original image which is unreadable. This can't be decrypted without proper cipher. The transformation of an information into secure format to improve the protection is known as Cryptography. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing." It is a technique of secure communication where no hacker can access to the original information.

In cryptography confidentiality is ensured by encrypting the data. Since data may be visible on internet, confidential and sensitive information such as password may be exposed. To overcome this, encryption is performed where plaintext is converted into cipher-text and make the data non-readable

II. LITERATURE SURVEY

In recent days information can be transferred through many ways from one place to another place, Encryption is one of the ways to protect the information, it provides high security to the information. Military and medical applications need only partial encryption, there is no need to encrypt complete image. We can use some encryption approaches like selective image encryption and partial image encryption. The percentage of pixels throughput of the input image is randomly encrypted in partial image encryption (PIE) where only specific portion of interest in the original image is encrypted in selective image encryption (SIE). Some of the articles

 DOI : 10.35291/2454-9150.2020.0527

Zhijuan Dengand Shaojun Zhong In this article, the authors have introduced chaotic mapping based digital image encryption algorithm. the authors have analysed the algorithm theoretically, the number of iterations is reduced and the cryptographic space is highly expanded by this algorithm. algorithm is sensitive to secret key because it consists of many characteristics, key space of this algorithm is big. This algorithm is weak in resisting chosen-plaintext attacks. Therefore, chaos-based image replacement method is used. After encryption pixels are well distributed. This algorithm is very much sensitive even if there is small change [1].

Akram belazi muhammad Talha et.al In this paper, the authors have proposed a new encryption method based on chaos for medical images, it is the combination of both DNA and chaos, it consists of two encryption rounds, followed by a key generation layer, It follows the permutation - substitution - diffusion structure, The secret key of chaotic systems is generated by SHA – 256

hash function with initial secret keys. six steps are involved in each round of the algorithm, for image encryption the bitlevel substitution and the pixel-based substitution are used in cascade. By repeating previous steps with new secret keys, the final encrypted image is obtained. It is good enough against all kinds of attacks, it is very much suitable for real-time applications [2].

Hossein movafegh ghadirli Image encryption is classified into bit-level and pixel-level. Histogram of the image can be changed by bit-level permutation, because it is bit-level computing it is time consuming, In this paper, authors have proposed a new method known as digit-level permutation, the image is divided and converted into a matrix form, this pixel matrix is decomposed into three digital matrices, Using Henon map this pixels will be shuffled, pixel-level permutation is combined with bit-level permutation by digit-level permutation, high-speed diffusion operation will been designed [3].

Aqeel ur rehman et.al In this paper the authors have presented tow major technologies. They have tested and estimated the scheme of encryption of image using different parameters. This method will more efficient than the previous methods [4].

Lisungu oteko tresor et.al The author has presented a new technique of encryption. This method is suitable only for grey scale images. The speed will be more but the method is restricted only to grey scale images [5].

Ping ping et.al Image encryption is classified into bit-level and pixel-level. Histogram of the image can be changed by bit-level permutation, because it is bit-level computing it is time consuming, in this paper, authors have proposed a new method known as digit-level permutation, the image is divided and converted into a matrix form, this pixel matrix is decomposed into three digital matrices. Using Henon map this pixel will be shuffled, pixel-level permutation is combined with bit-level permutation by digit-level permutation. High-speed diffusion operation will be designed [6].

Tresor Oteko Lisungu, Mbuyu Sumbwanyambe In the paper the development of new encryption scheme, where in this method the characteristics of image is changed and compressed. This increases the complexity and makes this method more efficient [7].

Dong xie In this method only one multiplication of matrix is required, this makes it simple. Crypto system provides great security to the information where it will be hard to crack this image. Hence, this makes it more efficient [8].

III. PROPOSED WORK

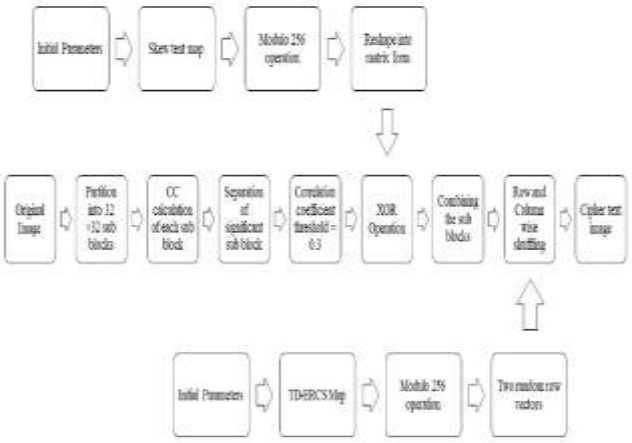

Figure 1. Basic block diagram of image encryption and decryption

The above fig. 1 shows Block diagram of this project. As we can see in the fig the plain text image is taken as the input and it is converted into cipher text image. The conversion of a plain text image into cipher text image involves many processes. This conversion is done using the chaos-based encryption technique, this also involves partial or selective encryption techniques which are time saving.

Let us divide the above flow chart into five major steps,

A. Image Division

The process of dividing a plain image into multiple sub blocks. The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyse. Image segmentation is typically used to locate objects and boundaries (lines, curves, etc.) in images. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share certain characteristics.

 DOI : 10.35291/2454-9150.2020.0527

i. In step 1 the original image or Plaintext image is divided into 32×32 blocks.

$$B = [B1, B2, B3, \ldots B1024] \quad (1)$$

B. Correlation coefficient of each sub-block

A correlation coefficient is a numerical measure of some type of correlation, meaning a statistical relationship between two variables. The variables may be two columns of a given data set of observations, often called a sample, or two components of a multivariate random variable with a known distribution. Several types of correlation coefficient exist, each with their own definition and own range of usability and characteristics. They all assume values in the range from −1 to +1, where ±1 indicates the strongest possible agreement and 0 the strongest possible disagreement.

ii. Correlation coefficient of each blocks is calculated for each block is calculated keeping a threshold value as.

$$T = 0.3 \quad (2)$$

C. Skew-Tent Map

iii. Initial conditions are set to Skew Tent map i.e.,

$$r = 0.1000 \text{ and } V0 = 0.5000. \quad (3)$$

iv. Iterate Eq. 3 1,048,576 times to generate a random vector

v. Update the random vector V by multiplying it with 10^{14}.

$$r = V \times 10^{14} \quad (4)$$

vi. Modulo 1,024 operation is performed to get updated random numbers in range of 0 to 1,024.

$$\zeta = \text{Modulo } (\Upsilon, 256) \quad (5)$$

vii. The plaintext image blocks having correlation coefficient greater than T are bitwise XORed with the random matrix ψ.

$$\text{Diffblockn} = \text{bitxor (bn, } \psi) \quad (6)$$

viii. All blocks are combined to get diffused image

D. TD-ERCS map

Tangent-Delay Ellipse Reflecting Cavity Map System is a discrete chaotic system and has many properties such as the maximum Lyapunov exponent which is over zero, unchangeable equiprobability distribution, and zero correlation in total field. TD-ERCS is described by

(7)

$$\begin{cases} X_n = -\dfrac{2k_{n-1}Y_{n-1} + X_{n-1}(u^2 - k_{n-1}^2)}{u^2 + k_{n-1}^2} \\ Y_n = Y_{n-1} + k_{n-1}(X_n - X_{n-1}), \quad n = 1, 2, 3 \ldots \end{cases}$$

$$x_n = \frac{-\left[2k_{n-1}y_{n-1} + x_{n-1}\left(u^2 - k_{n-1}^2\right)\right]}{u^2 + k_{n-1}^2},$$

$$k_n = \frac{2k'_{n-m} - k_{n-1} + k_{n-1}\left(k'_{n-m}\right)^2}{1 + 2k_{n-1}k'_{n-m} - \left(k'_{n-m}\right)^2},$$

$$k'_{n-m} = \begin{cases} -\dfrac{x_{n-1}}{y_{n-1}}\mu^2 & n < m \\ -\dfrac{x_{n-m}}{y_{n-m}}\mu^2 & n \geq m, \end{cases}$$

$$y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1},$$

$$k'_0 = -\frac{x_0}{y_0}\mu^2,$$

$$k_0 = -\frac{\tan\alpha + k'_0}{1 - k'_0\tan\alpha},$$

Eq 7 is the mathematical representation of the Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS). *α*, *X*0, *m* and *μ* represents initial secret values of the TD-ERCS map. These initial values (*α*, *X*0, *m* and *μ*) of TD-ERCS map act as keys for the proposed

Scheme.

ix. Set X0 = 0.5000, α = π/4, m = 2 and μ = 0.3000 for the TD-ERCS map.

x. Iterate Eq. 7 1,024 times to generate two random vectors

$$Xn = X1, X2, \ldots X256 \quad (8)$$

$$Yn = Y1, Y2, \ldots Y256 \quad (9)$$

xi. Update the random vectors *X* and *Y* by multiplying them with 10^{14}.

$$X' = X \times 10^{14} \quad (10)$$

$$Y' = Y \times 10^{14} \quad (11)$$

xii. Modulo 1,024 operation is performed to get updated random numbers in range of 0 to 1,024.

$$X'' = \text{Modulo } (X \times '256)$$

$$Y'' = \text{Modulo } (Y \times '256) \quad (12)$$

E. Arnold's cat map

Arnold's cat map is one of the famous discrete-time dynamical system, from both dynamics and a topological standpoint. It can be defined in the following way

$$\Gamma\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 \quad (13)$$

xiii. The diffused image DiffImage is permuted row-wise via the random row vector X''. For example, if the DiffImage and random row vector X ''are given as:

xiv. Then the row-wise permuted *Row* − ShuffledImage will be such as:

 DOI : 10.35291/2454-9150.2020.0527

X ''= [1024 1 · · · 2] (14)

These are the five major steps carried out in this project

2. PERFORMANCE ANALYSIS OF THE ALGORITHM

Parameter analysis between source and cipher image is required to judge the efficient encryption technique.

1.1 Analysis if entropy

In encryption system Entropy is a measure degree of randomness. The information entropy is calculated using formula:

$$H(S) = \sum P(S_i) log \frac{1}{P(S_i)} \quad (1)$$

where P(Si) is the probability of symbol Si.

1.2 Mean square error (MSE)

It can be calculated between input image and encrypted image by taking mean squared difference between them. If the value of MSE is more then, the amount of noise introduced is more and the strength of the signal is reduced. Let I1 and E1 denote the source image and cipher image respectively, then the equation for MSE is given by

$$MSE = \frac{1}{h * w} \sum_{p=1}^{h} \sum_{q=1}^{w} [I1\,(i,j) - E1\,(i,j)]^2 \quad (2)$$

Where h and w are row and column of picture.

1.3 Peak signal to noise ratio (PSNR)

PSNR is inversely proportional to MSE. Ciphering quality will be reflected by PSNR. If MSE is more PSNR will be less and vice versa. Values of PSNR indicates the signal strength. Mathematically PSNR is as shown below

$$PNSR = 20 * log_{10}\left[\frac{255}{MSE}\right] \quad (3)$$

2.4 NPCR and UACI

There are two testes to check the sensitivity of proposed ciphering technique to source and keys: Number of pixel change rate (NPCR) and Unified average changing intensity (UACI). The equation to calculate Unified average changing intensity (UACI) is Eq. 4.

$$UACI = \frac{1}{m*n} \sum_0 \frac{|I\,(p,q) - E\,(p,q)|}{255} \times 100\% \quad (4)$$

Where, m and n are rows and columns respectively, I (p, q) and E (p, q) are original and cipher image respectively.
The equation to calculate Number of pixel change rate (NPCR) is Eq. 5.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (5)$$

Where, m and n are rows and columns respectively and D (i, j) is defined below

$$D(i,j) = \begin{cases} 1 & if\ I(i,j) \neq E(i,j); \\ 0 & if\ I(i,j) = E(i,j); \end{cases} \quad (6)$$

Where I (I, j) and E (I, j) are the first and cipher image respectively.

IV. RESULT ANALYSIS

The proposed scheme is successfully implemented using MATLAB R2019b and the obtained results are shown in the below figures. In the output figures we can see the input image, its cipher image and their histogram in each resultant output figure. This show the efficiency and security of the scheme where it ensures the security of the data.

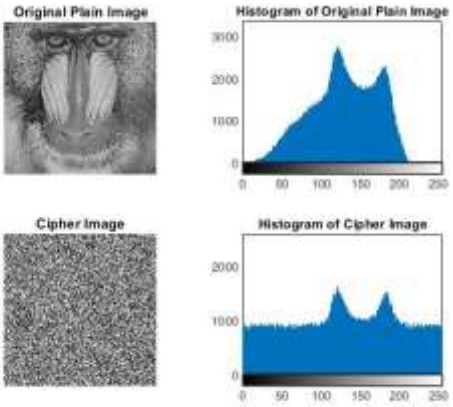

Figure 2. Input image and Encrypted Image and their histogram analysis

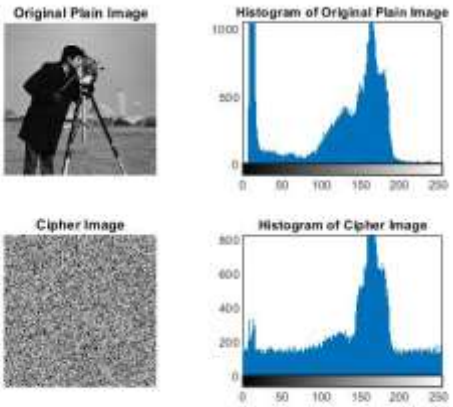

Figure 3. Input image and Encrypted Image and their histogram analysis

 DOI : 10.35291/2454-9150.2020.0527

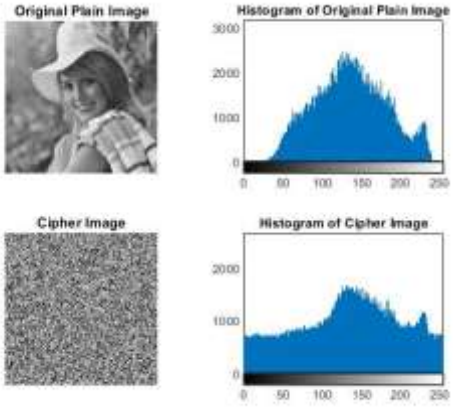

Figure 4. Input image and Encrypted Image and their histogram analysis

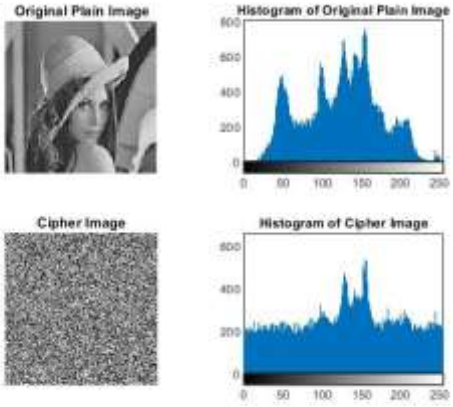

Figure 5. Input image and Encrypted Image and their histogram analysis

Table 1 shows the Performance Analysis of the encrypted images in terms of MSE (mean square error), PSNR (peak signal noise ratio) when tested with different test images of size mxn. As shown in the table there are four examples and their MSE and PSNR. It can be seen that each image has its own MSE and PSNR values. It is decided with respect to its gray level in the respective image.

IMAGE	**MSE**	**PSNR**
BABOON	**117.79**	**9.81**
CAMERAMAN	**132.54**	**9.04**
ELAINE	**115.36**	**9.96**
LENA	**123.46**	**9.54**

TABLE 1. PERFORMANCE ANALYSIS

V. CONCLUSION

In recent days there is a drastic increase in data theft and hence protection of data is very much important. By using the combination of chaotic and selective image encryption technique we can encrypt data in less time and with more efficiency and this can be more secure. In this paper we have implemented and executed this technique. In result analysis we have shown the input and output and its histogram respectively and the performance analysis show the mean square error and peak signal to noise ratio of the given examples. we conclude the each and every encryption technique has its own advantages and disadvantages but this encryption technique is more efficient and less time consuming.

REFERENCES

[1] Deng, z., & zhong, s. (2019). A digital image encryption algorithm based on chaotic mapping. *Journal of algorithms & computational technology*, *13*, 1748302619853470.

[2] Belazi, a., talha, m., kharbech, s. And xiang, w., 2019. Novel medical image encryption scheme based on chaos and dna encoding. *Ieee access*, *7*, pp.36667-36681.

[3] Ghadirli, hossein movafegh, ali nodehi, and rasul enayatifar. "an overview of encryption algorithms in color images." *signal processing* (2019).

[4] Rehman, a.u., wang, h., shahid, m.m.a., iqbal, s., abbas, z. And firdous, a., 2019. A selective cross-substitution technique for encrypting color images using chaos, dna rules and sha-512. *Ieee access*, *7*, pp.162786-162802.

[5] Tresor, l.o. and sumbwanyambe, m., 2019. A selective image encryption scheme based on 2d dwt, henon map and 4d qi hyper-chaos. *Ieee access*, *7*, pp.103463-103472.

[6] Ping, Ping, et al. "A chaos-based image encryption scheme using digit-level permutation and block diffusion." IEEE Access 6 (2018): 67581-67593.

[7] Tresor, lisungu oteko, and mbuyu sumbwanyambe. "a selective image encryption scheme based on 2d dwt, henon map and 4d qi hyper-chaos." *ieee access* 7 (2019): 103463-103472.

[8] Xie, dong. "public key image encryption based on compressed sensing." *ieee access* 7 (2019): 131672-131680.

 DOI : 10.35291/2454-9150.2020.0527