Analysis of Various Chaos Based Image Encryption Methods

Amita Yadav[1], Apurav Poriya[2], Raj Kumar[3], Sachet Gulia[4]
{amita.yadav@msit.in[1], apuravporiya10@gmail.com[2], roopaksharma1029@gmail.com[3], sachetgulia@gmail.com[4]}

Maharaja Surajmal Institute of Technology, Delhi[1,2,3,4]

Abstract. In today's data transfer environment images are one of the major parts of Internet and online interaction. As a result, there is intrusive. Different type of chaotic maps which are utilized for image encryption are analyzed in the paper, along with their advantages and disadvantages. Chaotic maps are advantageous for image encryption because of their unexpected, exponential, and very sensitive initial circumstances, which results in more trustworthy image encryption. Numerous previous suggested image encryption systems rely on low dimensional chaotic maps, which provides a poor amount of security and are especially susceptible to most common cyber attacks. To tackle this issue, various chaotic maps were designed. The objective of this review article is to discuss the properties and methodology of numerous chaotic maps that have been utilized for image encryption.

Keywords: Encryption, chaos image encryption, cryptography, security.

1 Introduction

Images account up a significant amount of the data sent over the internet as a result of the fast evolution of internet technologies. As a consequence, security of these photos is a critical issue. To solve these concerns, many steganography and cryptography methods have been offered. Cryptography is the study of techniques for communicating securely in the presence of an adversary. It addresses difficulties such as encryption and verification. Native data is encoded into an obfuscated cypher image prior to being stored or transferred. Encrypting an image may be accomplished in a number of ways, including delivering it over the internet, through email, or via instant messaging services. Due to the vast amount of information, the high excess, and the interdependence of adjacent pixels, standard techniques and methods such as IDEA, are incompatible in case of encrypting the images. Due to the specific characteristics of image data, such as a low bulk limit, a high repetition rate, and a high degree of connectedness between pixels, any encryption system must meet very stringent requirements. Image encryption is done to convert a plain image to a cypher image. Each type of data has its individual features and processes for preventing unauthorized access. As a consequence, in unblocked systems where the pixel value is updated, data encryption is utilised to guarantee security. Each pixel is given a numerical value. Image size divided by the matrix size is equal to pixel size. The image size is proportional to the field of view, whereas the matrix size is proportional to the number of pixels along the image's length and width. The

ICIDSSD 2022, May 24-25, New Delhi, India

DOI 10.4108/eai.24-5-2022.2318552

original image may be turned to a plain image that cannot be viewed by unauthorised users using a cryptography method and a key. On the contrary, decrypting the image is the inverse of encrypting the image. There are two kinds of cryptography computations depending on the number of keys: secret key algorithms, which encrypt and decrypt data using just one key parameter, and private key algorithms, which encrypt and decode data using two keys. The first is the symmetric key algorithm, while the second is the asymmetric key algorithm.

1.1 Chaos Based Image Encryption

Non-chaotic technique & chaotic-based specific or nonspecific techniques are the two types of image encryption. The beginning conditions are critical in chaos-based techniques If we alter a single parameter in the initial condition, the complete outcome will differ. The advantage of using chaos-based image encryption techniques are their simplicity of use, increased encryption speed, and resilience to exploitation. The chaos-based encryption technology has a wide range of applications in a number of industries, which includes health care, social media, military, internet chatting applications, image messaging apps, government documents, telemedicine, security, and medical imaging. The two steps of a chaos-based encryption scheme are confusion and diffusion. **Figure 1.** illustrates the chaos-based image encryption algorithm in block diagram form. Confusion happens when the placement of pixels is altered without altering their values. The objective of a diffusion phase is to alter the estimate of each pixel in the image.

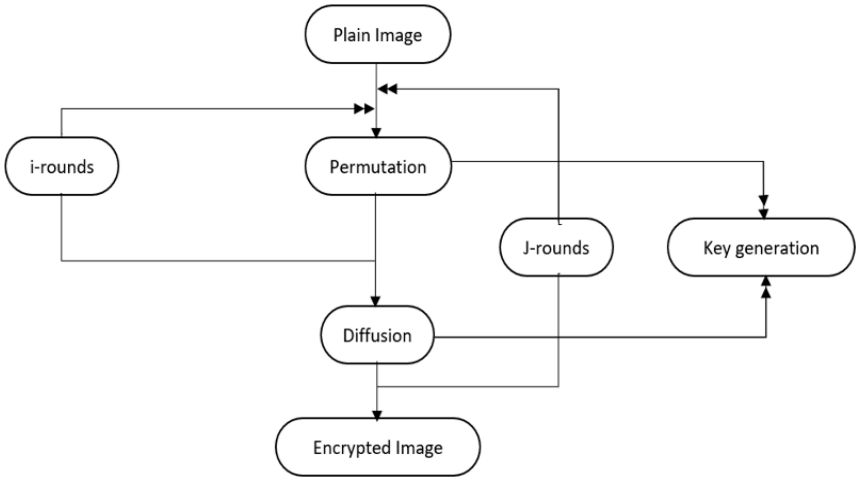

Fig. 1. Flow chart of Chaos Based Encryption

1.2 Performance Parameters

A. Key Security Analysis. The emphasis of a good encryption method should be done on encryption method keys throughout on both the encoding as well as decoding processes. The key space estimation is the total number of unique keys that can be used in the encryption. The

general channel is used to communicate the cypher text images, while the private channel is used to convey the security key. In this method, the security key should have a reasonable amount size and also be resistant to the bruteforce attacks.

B. Differential Attack Analysis. The differential attack is one of the attack that is most widely used and effective security techniques. The unified average change intensity (UACI) and, more precisely, the number of pixel change rate (NPCR) are from some of two metrics that can be used to determine if an image's encoding is capable of resisting differential attack.

$$\text{NPCR} = \frac{\sum_{ij} E(k,l) * 100\%}{q * p} \tag{1}$$

$$\text{UACI} = \frac{1}{q*p}\left[\frac{\sum_{ij}|d_1(k,l) - d_2(k,l)|}{255}\right] * 100\% \tag{2}$$

$$\text{where E (k, l)} = \left\{ \begin{matrix} 1\,, when\ D1(k,l) \neq D2(k,l) \\ 0,\ when\ D1(k,l) = D2(k,l) \end{matrix} \right\}$$

C. Correlation Coefficient Analysis. A good cypher image should generate a cypher image with a little degree of connectivity between the pixel values. The optimal way for determining the suggested image cryptosystem's efficacy is to use correlation coefficient analysis to determine the relationship between the cipher's pixel values. The pixels in an original image are always inextricably linked to their adjacent pixels, whether vertically, horizontally, or diagonally. In this manner, a strong image encryption computation should eliminate significant correlations between adjacent pixels.

$$C_{x,\,y} = E\left[\frac{(x-\mu_x)(y-\mu_y)}{\sigma_x \sigma_y}\right] \tag{3}$$

where E (.) denotes the expected value and is mean value and standard deviation.

D. Histogram Evaluation. The histogram charts is used to determine how an encrypted image's distribution is distributed. Keeping in mind the underlying purpose of withstanding cypher and statistical attacks, histogram should be as uniform. The histogram analysis may be used to determine the irregular distribution of pixel values in a cypher image. According to the results, it is logical that the pixels of the encrypted image are equally distributed, making it difficult for an unauthorised individual to use statistical assaults to get the plain image.

2. Literature Review

[1] Zhongyun Hua et al. employed a cosine-transform based chaotic system (CTBCS) to create new chaotic maps using any two chaotic maps. This method utilizes two existing chaotic maps as seed maps and then generates a large number of new chaotic maps with exceptional performance.

[2] J.S. Khan et al. suggest an approach in which plaintext image blocks with the highest correlation coefficient values are pixel-wise XORed with random numbers produced from the skew tent map using a predefined threshold value. The image is then permuted using two random sequences created from the TD-ERCS chaotic map, resulting in increased security.

[3] Yong Zhang develops a cryptosystem that generates key streams for encrypting or decrypting images using the Piecewise Linear Chaotic Map (PWLCM) and cubic S-box. The visual difference between two images is quantified using a novel analytical index called Blocked Average Changing Intensity (BACI). A 512-bit secret key is employed.

[4] Ü. Çavuşoğlu et al. propose a chaos-based hybrid encryption method that combines the complicated dynamic properties of chaotic systems with the S-AES algorithm. This technique consumes much less memory than the AES algorithm. This approach employs a mixture of the CS-AES and AES algorithms, as well as S-AES, S-AES, and chaos based encryption.

[5] Xiao Chen et al. employ a method in which the algorithm first scrambles the plain image position using logistic-sine chaos mapping and then applies hyper chaos system is to the adaptive as well as to image encryption technique of numerous selected images in order to overcome sequences in old encryption algorithms. Permutation was performed on the rows and columns of photos using the sequences obtained by the secondary key during the permutation step.

3. Various Chaotic Maps Analyzed

3.1. Chaos-transformed based Chaotic System (CTBCS)

CTBCS is intended to overcome the shortcomings of current chaotic maps in the presence of fragile chaos and weak dynamical behaviours. The CTBCS may be expressed mathematically as

$$x_{i+1} = \cos(\pi(F(a, x_i) + G(b, x_i) + \beta)) \quad (4)$$

where variable β is referred as shifting constant and F(a,xi) and G(b,xi) are called two pe-existing chaotic maps known as the seed maps where a and b are known as control-based parameters. The CTBS generates the output by first combining the outputs of $F(a,\ xi$)and $G(b,\ xi$) with a shifting constant and then performing a cosine transform. Combining the two seed maps effectively shuffles their chaotic dynamics, and the cosine transform shows very complicated nonlinearity. Thus, the CTBCS's new chaotic maps exhibit complicated characteristics. Because the seed maps $F(a,\ xi$) and $G(b,\ xi$) in the CTBCS may be any

existing chaotic maps, users have the freedom to create various new chaotic maps by adjusting the parameters of existing maps.

3.2. Tangent-Delay Ellipse Reflecting Cavity-Mapping

Li-Yuan et al. created a novel chaotic system, the Tangent Delay Ellipse Reflecting Cavity-Map System (TD-ERCS), in 2004 [6]. The TD-ERCS system is a discrete chaotic system that exhibits a number of features, including a maximum Lyapunov exponent greater than zero, an unchanging equiprobability distribution, and zero correlation in the total field. The TD-ERCS is defined by

$$x_n = \frac{-\left[2k_{n-1}y_{n-1} + x_{n-1}(u^2 - k_{n-1}^2)\right]}{u^2 + k_{n-1}^2} \tag{5}$$

$$k_n = \frac{2k'_{n-m} - k_{n-1} + k_{n-1}(k'_{n-m})^2}{1 + 2k_{n-1}k'_{n-m} - (k'_{n-m})^2} \tag{6}$$

$$k'_{n-m} = \begin{cases} -\frac{x_n - 1}{y_{n-1}}\mu^2, & n < m \\ -\frac{x_{n-m}}{y_{n-m}}\mu^2, & \text{n} \geq \text{m} \end{cases} \tag{7}$$

$$y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1} \tag{8}$$

$$k'_0 = -\frac{x_0}{y_0}\mu^2 \tag{9}$$

$$k_0 = -\frac{tan\alpha + k'_0}{1 - k'_0 tan\alpha} \tag{10}$$

where (μ, x0, α, m) are referred to as the TD-ERCS seed parameters. In TD-ERCS seed parameters, the seed parameters are μ ∈ (0,1], with initial x0 ∈ [-1,1], α ∈ [0, π], and tangent-delay parameters are m=2,3,4,5…

3.3. Piecewise Linear Chaotic Map

A Piecewise Linear Chaotic Map (PWLM) is a map composed of multiple linear segments that conform to specified constraints. PWLCM may be denoted by

where xj ∈ [0,1] and control guidelines p ∈ (0,0.5) are specified, and this is used as the secret key. If 2n unique states are used as inputs to the chaotic map, the distinct output is obtained after a 1digital chaotic epoch, which is less than 2n, since the 1d PWLCM is a multi-to-one map (m>1).

$$x_{j+1} = F_q(x_j) = \begin{cases} x_{j_{/q}}, & 0 \le x_j < p \\ \frac{x_j - p}{0.5 - p}, & p \le x_j < 0.5 \\ F_q(1 - x_j), & 0.5 \le x < 1 \end{cases} \quad (11)$$

3.4. Hybrid CS-AES

Specifically, in each loop of the CS-AES method, a chaos based RNG system produces as many bits as required for the encryption algorithm from the RNG system's x and y phases; an S-Box structure suitable for encryption is produced using the S-Box design algorithm. Decryption employs the inverse of encryption methods. The round number is 10 for the AES algorithm and 2 for the S-AES algorithm, as seen in block diagrams.

Table 1. Analysis Result. The values of various algorithms based on various parameters.

Algorithms	Correlation Coefficient	Key Space Analysis	NPCR	UACI	Adjacent Pixel Correlation	Information Entropy	Time Analysis (in sec)
Cosine-transform based Chaotic System	-0.0051	2^{256}	99.7055	33.4172	H = -0.003280 V = -0.000777 D = -0.000181	Plaintext - 7.5241 Ciphertext - 7.9512	0.91
Tangent-Delay Ellipse Reflecting Cavity-Map	0.0128	2^{299}	99.2304	33.0341	H = -0.0163 V = 0.0185 D = -0.0129	Plaintext - 7.5241 Ciphertext - 7.9925	0.65
Piecewise Linear Chaotic Map	-0.0237	2^{512}	99.6119	33.4661	H = -0.009448 V = 0.024064 D = -0.041171	Plaintext - 7.5241 Ciphertext - 7.9993	0.47
Hybrid CS-AES	-0.00475	10^{126}	99.6912	33.3786	H = -0.00498 V = -0.00362 D = -0.0091	Plaintext - 7.5241 Ciphertext - 7.9565	1.45
Logistic-sine and Hyper-chaotic systems(Multiple chaotic mapping)	-0.00925	10^{64} X 4^{256}	99.5901	33.4227	H = -0.0028 V = 0.0171 D = -0.0022	Plaintext - 7.5241 Ciphertext - 7.9844	6.2

3.5. Logistic-sine and Hyper-chaotic systems

The logistic-sine compound chaotic system's mapping equation is expressed as

$$\begin{cases} x_{k+1} = \mu x_k (1 - x_k) \\ y_{k+1} = \sin(r \, arc \sin \sqrt{y_k}) \end{cases} \quad (12)$$

where xk ∈ (0, 1) signifies the logistic mapping status and yk denotes the sine mapping status. When 3.5699456l4 is greater than one, the logistic-sine system reaches a chaotic state. By mapping the sensitivity of the starting value to a composite chaotic system, it is possible to produce matching chaotic sequences. Permutation-based encryption of digital images is accomplished by transformation processing.

The hyper-chaotic system's equation is as follows:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2 x_3 x_4 \\ \dot{x}_2 = b(x_1 + x_2) - x_1 x_3 x_4 \\ \dot{x}_3 = -cx_3 + x_1 x_2 x_4 \\ \dot{x}_4 = -dx_4 + x_1 x_2 x_3 \end{cases} \tag{13}$$

where a, b, c, and d are the system's control parameters. While the other parameters remain unaltered, x1 is set to a modest initial value generated from the key stream. Iteration produces four types of discrete chaotic sequences: X1, X2, X3, and X4.

4. Results

The above-mentioned chaotic maps were used to implement the chaos encryption in the MATLAB R2021b by using the algorithms provided by the authors of respective papers. Therefore, these algorithms compared on the bases of parameters such as key analysis, differential attack (NPCR and UACI), correlation coefficient, information entropy and time taken by them. The plaintext image is from USC-SIPI “Miscellaneous”, 4.1.01 (256*256 px) and of 192kb size. According to the data obtained as shown in Table 1, the algorithm based on multiple chaotic mapping is more secure than the others but takes more time, where as the algorithm based on the cosine-transform based chaotic maps is more efficient.

5. Conclusion

When we communicate information through an untrusted medium, information security becomes increasingly important and image plays a major role in communication nowadays. A few strategies may be used to provide a safe data transfer, one of which is chaos encryption of images. This paper discusses various chaos encryption methods and reviewed them on various factors.

References

[1] Hua, Zhou and Huang: Cosine-transform-based chaotic system for image encryption (2019)

[2] Khan, J.S., Ahmad, J.: Chaos based efficient selective image encryption. Multidim Syst Sign Process (2019)

[3] Yong Zhang.: The unified image encryption algorithm based on chaos and cubic S-Box, Information Sciences (2018)

[4] Çavuşoğlu, Ü., Kaçar, S., Zengin, A.: A novel hybrid encryption algorithm based on chaos and S-AES algorithm (2018)
[5] Xiao Chen, Chun-Jie Hu.: Adaptive medical image encryption algorithm based on multiple chaotic mapping, Saudi Journal of Biological Sciences (2017)
[6] S. Li-Yuan, S. Ke-Hui, and L. Chuan-Bing: Study of a discrete chaotic system based on tangent-delay for elliptic reflecting cavity and its properties (2004)