A Review of Performance Comparison on Chaos Based Image Encryption Technique

Nishant Kumar
Department of Information Technology,
Indian Institute of Information Technology Sonepat,
Sonipat, India

Dr. Sourabh Jain
Department of Computer Science & Information Technology,
Indian Institute of Information Technology Sonepat,
Sonipat, India

Abstract:- In a day today life digital images , audios and text is the most common medium of communication and they are widely transmitted over the insecure network channel including internet . Among all multimedia, Images may contain susceptible information like Satellite and UAV navigation Images , Military Communication and Medical Imagninig. In order to protect data privacy, encryption of images before transmission in internet is most crucial part to maintain confidentiality , integrity , nonrepudiation and authentication . In this paper we review and analyse various type of image encryption technique based on chaotic maps and several performance metrics to verify efficiency of security algorithms .

Keywords:- *Image Encryption, Chaotic map, Henon map , Image Security Analysis.*

I. INTRODUCTION

With the advancement of technology in communication using internet, smartphones and numerous multimedia devices. Transmission and exchange of information over a long distance on a wide network are common. Therefore, Establishing Secure transmission of digital images and videos maintains privacy and confidentiality. Image may contain susceptible information which must be protected from an attacker [1]. Cryptography is the foundation of a modern security system which investigate, encrypts and transforms images into non-recognizable for an attacker without some extra information. A Digital image is a piece of visual information in a form of a 2D matrix in a rectangular domain. A function f(x,y) mapped to the pixel value at x,y co-ordinate. In Order to attain confidentiality, Cryptographic algorithm along with some key and controlled parameters are can encrypt each pixel of an image and obtain a cipher image that is secured and only accessible to authorized personnel [2] . Modern cryptographic algorithms heavily rely on mathematical equations and computaion.

To encrypt an image we mainly use chaos or non-linear dynamic systems because it exhibit deterministic properties and sensitive dependence on initial conditions so these controlled parameters are used as a symmetric key to encrypt an image. After encryption with chaos, it looks like a noisy image to an unauthorized user. Encryption techniques like AES, IDEA, DES, etc are conventional for text encryption not for images because image contain lots of data along with interconnected pixels value [3].Many encryption techniques established by researchers like a low dimensional chaotic map which is weak to handle statistical attacks and brute force to high dimensional chaotic map is used.

A chaotic system is defined by its random behavior and sensitive dependence on the initial condition which create a random phenomenon without any random variable, this messy system highly fluctuates only small change in its parameters which behave like an initial seed or secret key and make them hard to predict, these behaviors of chaos system is ideal for cryptographic purpose. Chaos based technique is easy to implement and has faster encryption and decryption time [4]. Chaos system can be applied using two methods: a) Plain text, Secret key and controlled parameters are provided to generate cipher text, or b) Generate pseudo- random number for each pixel used as a secret key.

A. Chaotic Map in Image Encryption

Image encryption techniques based on chaos depends on some phases like diffusion, permutation, or a combination of both. In the permutation phase, pixels or bits of the plain image are shuffled without changing the pixel value in it, whereas diffusion is a phase in which every pixel value of a plain image is substitute using a chaotic function through which small change in parameter led to completely change the output [5]. In real life scenario, we use both diffusion and permutation to generate sequences.

II. DIMENSIONAL CHAOTIC MAPS

The chaos-based encryption technique relies on its nonlinear and unpredictable behavior. 1-D chaotic map has a simple design , highly sensitive to its controlled parameter and it helps in reducing inter-pixel correlation to cipher image. Some 1-Dimensional chaotic maps are Logistic, sine, tent and skew map ,etc [6] [7]. Main disadvantage of 1-D chaos-based encryption is that it is vulnerable to plain text attack and sometimes if small data is obtained then chaotic map becomes weak and their initial value is identified due to less complex mapping. Therefore various image encryption algorithm is insecure if 1-d chaotic map are used.

A. Logistic Map (LM)

Logistic map is a one- dimensional mapping with a recurrence relation of degree 2. Mathematically it is characterized as follows.

$$y_{i+1} = \lambda y_i(1 - y_i) \qquad (1)$$

Logistic map dynamic behavior depends on the two parameters y_0 and λ , where y_0 ∈ [0, 1] and λ ∈ (0, 4) respectively. When λ ∈ (0, 3) it is stable at a fixed point, when λ increases to (3, 3.44) it oscillates between two fixed points. and for λ ∈ (3.45, 4), it starts oscillating on an infinite number of points which are random and non-periodic and sensitive to its initial value [8].The issue that occurs in a Logistic map is that its key space is small, delicate security, and restricted tumultuous range. to (3.576, 4).

B. *Sine and Tent Map*

Sine map is a straightforward yet compelling chaotic model to upgrade the encryption procedure. Sine map is a non-linear transformation system that applies it to a result to be a 1-D Chaotic map. Sine capability has a limited circle which makes them complex and non-linear. [9]. Logistic Sine map can be expressed as follow:

$$y_{i+1} = L(r, x_i) = ry_i(1 - y_i) \qquad (2)$$

Here the controlled map is in the scope range of r ∈ [0, 4] to aquire chaotic behaviour.

$$y_{i+1} = S(r, y_i) = r\,sin(\pi y_m) \qquad (3)$$

Here the scope of parameters is within the range r ∈ [0, 1] to obtain chaotic behavior in sine map [10]. The tent map behave as a discrete-time polynomial mapping system with degree one. It either creases or expanse an input value based on its range in input parameter . Tent map can be addressed as follow:

$$y_{i+1} = T(y_i, r) = \begin{cases} ry_i & \text{for } y < 0.5 \\ r(1 - y_i) & \text{for } y \geq 0.5 \end{cases} \qquad (4)$$

Where r is a controlled parameter which take positive real number r ϵ [0,2] Sine and tent map has same problem of ranges.Both tent and sine map are joined to obtain a different chaotic system that overcomes the problem of weakness in the statistical attack.

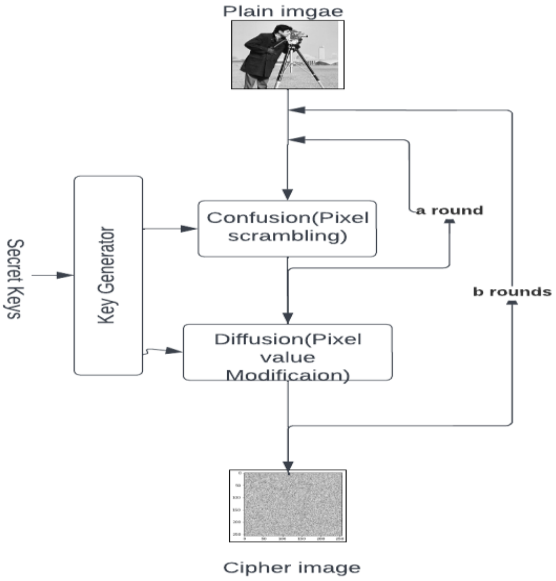

Fig 1: Image encryption flow chart

C. *Skew Map*

Skew map is an elementary nonlinear dynamic equation with complicated behavior. It is mainly used to encrypt data in real-time with high efficiency and good security but it has several security issues like smaller key space and short periodicity and numerical degradation. Skew map can be represented as follow:

$$y_{i+1} = \begin{cases} \frac{y_i}{q} & \text{for } 0 < x_i \leq q \\ \frac{1-x_i}{1-q} & \text{for } q < x_i < 1 \end{cases} \qquad (5)$$

Where r is a controlled parameter which take positive real number r ϵ [0,2]. Sine and tent map has same problem of ranges.Both tent and sine map are joined to obtain a different chaotic system that overcomes the problem of weakness in the statistical attack.

III. MULTIDIMENSIONAL CHAOTIC MAP

A. *2d Logistic map*

2-D logistic map(LM) has more complicated structure of chaotic map like basin structure and attractors than normal logistic maps which help to generate more complicated pseudo random numbers . It has more complex behavior than 1-D logistic map. Mathematically, 2-D logistic map can be represented as (Eq 6).

$$\begin{cases} p_{i+1} = \mu(3q_i + 1)p_i(1 - pi) \\ q_{i+1} = \mu(3p_{i+1} + 1)q_i(1 - p_i) \end{cases} \qquad (6)$$

where (p_i, q_i) is the point obtained on ith iteration and µ is the controlled parameter to obtain chaotic sequence.

Under the different conditions on r as a system parameter, it shows different dynamic behavior, When µ in (-1,1) it has 2 saddle point and 1 attractive node, and p and q are unstable . when µ=1, the attractive focus becomes Neimark-Hopf bifurcation . when µ in (1,1.11), oscillation appears and the attractive focus becomes repulsive in nature . when µ in [1.11,1.19] it shows cyclic chaotic behavior, invariant close curve with oscillation, and obtain unit chaotic attractor behavior. when µ >1.19 chaotic mapping become highly unstable. At some point in space 2-D logistic map exhibit a dense set of periodic window which is not adequate for chaotic cryptography.

B. *2-D Sine Logistic Modulation Map (SLMM)*

2-D Sine Logistic Modulation map (SLMM) is a Higher dimensional chaotic mapping technique that has excellent chaotic performance, complex structure, low-cost implementation and is harder to predict. It is derived with the combination of 1-D chaotic map, the sine and the logistic map. It has a wider chaotic range, better ergodicity and hyperchaotic properties. It shuffles image pixel row and column simultaneously which makes it quick. Mathematically it can be represented as (Eq 7).

$$\begin{cases} p_{i+1} = \lambda(\sin(\pi q_i) + \sigma)p_i(1 - p_i) \\ q_{i+1} = \lambda(\sin(\pi p_{i+1}) + \sigma)q_i(1 - q_i) \end{cases} \qquad (7)$$

Here λ and σ are the controlled parameter where λ ε [0,1] and λ ε[0,3] . 2-D SLMM scatter in a much larger region in the phase plane, and able to generate more arbitrary result with better ergodicity property which help to generate strong cryptosystem in wider range.

C. Henon Map

Henon map is the simplest two-dimensional mapping technique based on stretching and folding dynamics of chaotic behavior . Henon map exhibit some property like stability, periodic orbits ,fixed point . 2D-Henon map changes the value of pixel instead of position along these lines make challenging to anticipate the picture, Henon map is represented as (Eq 8).

$$\begin{cases} x_{i+1} = 1 - a x_i^2 + y_i \\ y_{i+1} = b x_n \end{cases} \tag{8}$$

Here parameter α control how much streching and parameter b controls the thinkness of folding.Henon map works essentially on three stages ,collapsing, contracting along x and flipping about x=y . Since collapsing of preserves region ,the flipping preserves the region yet inverts the sign ,and the compression gets the region by constant factor b . Henon map behave like a convergent for constant value and for canonical value it behave like chaotic in range [1.07,1.4]. Henon map is structurally stable for only specific ranges of parameter which make henon map practically meaningful.

D. Lorenz Map

Lorenz chaotic map has some advantages such as unpredictability, confusion and being highly sensitive to the initial condition .Lorenz attractor can be used directly for generating confusion matrix which has all property of random walk and ergodicity which ensure unpredictability and keep secure to all known attacks .Lorenz map is represented as (Eq 9).

$$\begin{cases} \frac{dx}{dt} = \sigma \times (p - q) \\ \frac{dy}{dt} = rp - pz - q \\ \frac{dz}{dt} = py - bz \end{cases} \tag{9}$$

Here σ , b , r are controlled parameters whose values are positive real constant, σ is called a Prandtl number and b is called a Rayleigh Number, and p,q,z, are variables which take real values. In order to obtain chaotic behavior in Lorenz system σ = 10 and r>24.74 and b=8/3.Lorenz encryption scheme is both strong and compelling due to its 3-d model ,but it slow regarding generation of confusion matrix because coordinate wise operation.

E. Arnold Cat Map

Arnold cat map algorithm is one of the cryptographic algorithms based on confusion and changing the position of pixels without removing any information. ACM is based on the concept of continuously rotating the image so that it becomes random and unrecognisable and converted it into a cipher image for secure transmission in the channel . An encrypted image is a permutation of the original image which generated due to shuffling on pixels to reduce the correlation of adjacent pixels. This map is a respectable scrambling device that has been utilized in different cryptographic and stenographic applications . 2-D Arnold cat map is a transpose chaotic map used to encode image but with its intermittent nature and a few epochs, the position of the pixel is compromised which lessen the security. ACM is represented as

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(j) \tag{10}$$

Here (x_{i+1}, y_{i+1}) implies the new position of the actual image , (x_i, y_i) represent the initial co-ordinate of image where i=0,1,2,3,4.... and a,b is positive integer and j refers the size of plain image. ACM has two shortcomings, one is the periodicity; the other is the necessity that the picture is a square matrix. The periodicity makes it unstable, while the requirement restricts its applications.

F. Baker Map

Baker map is a chaotic mapping system for N*N matrix which is generally used in shuffling of pixels position of an image without changing the pixels value, it creates a permutation of an image by shuffling the pixels of image to decrease the correlation coefficient of adjacent pixels. Bakers map best fit above all properties like sensitivity to the initial condition, mixing and bijectiveness [11]. Transformation in baker map is done by two processes 1. flatting and stretching 2. cut and stack. The processing speed of the baker map is faster which makes it an efficient shuffling model. Baker map can be represented as (Eq 11).

$$(x_{i+1}, y_{i+1}) = \begin{cases} (x_i/q, q y_i) & \text{for } 0 < x \le q \\ ((\frac{x_i - q}{1-q}, (1-q)(1+y_i) & \text{for } q < x \le 1 \end{cases} \tag{11}$$

Parameter of the given equation is q .For the equation to become a baker map when q=0.5 , (x_i, y_i) is the output with good ergodicity in the convergence region. When we simulate it on a computer this map will rapidly fall into a short circle with limited-length introductory qualities. To accomplish high-level security and faster encryption of image and strong resistance to statistical and numerical attack, the 2-Dimensional baker map converted into a 3-Dimensional chaotic map due to its speed . The handling the speed of a 3D chaotic map is approximately 2-3 times quicker than 2-Dimensional map . Higher dimensional map such as 3D chaotic maps,3D Arnold cat maps etc .3 Dimensional mapping techniques increase performance and strong resist to brute force attacks.

G. 3D Chaotic Map

Arnold cat map upgrades the security by utilizing a 3-Dimensional discrete chaotic map by adding a few additional parameters. A 3-Dimensional chaotic map is suitable for this purpose by shuffling, mixing, and scrambling the pixel value of the plain image which creates strong confusion by scrambling pixels at random places in the pain image and gradually defeats statistical, cryptanalytic , and differential attacks. 3D Chaotic map can be written as (Eq 12).

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{pmatrix} = A \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} mod1 \tag{12}$$

Where the matrix A which provides chaotic behavior. The matrix A is represented as follows.

Herep_x , p_y , $p_z$are positive integer and p_x , p_y , p_z=1and , p_x , p_y , p_z $= 2$. |A|=1 always for such type of chaotic matrix . 3D chaotic map is efficient simple and provide high end security [12].

H. 8d Chaotic map

8d chaotic cat map improves security and speed of encryption which uses the lookup table method and is more immune against statistical and differential attacks. Image encryption depends upon either shuffling of pixels of an image, encrypting every pixel of an image using an image encryption algorithm or using both on the same image to enhance the security of image [13].Encrypting speed of a chaotic map is limited because they are based on a real number domain. But using lookup table method we can increase the speed. 8d chaotic map has more parameters than 3d chaotic maps. 8d chaotic map is described as(Eq 14).

In 8d cat map uses 8 initial conditions where as in a 3d chaotic map 6 parameters are used [14].Therefore controlled parameters and key space are also increased. Therefore this algorithm improves the security system and uniform distribution of pixels.

$$\begin{bmatrix} A_{i+1} \\ B_{i+1} \\ C_{i+1} \\ D_{i+1} \\ E_{i+1} \\ F_{i+1} \\ G_{i+1} \\ H_{i+1} \end{bmatrix} = A \begin{bmatrix} A_i \\ B_i \\ C_i \\ D_i \\ E_i \\ F_i \\ G_i \\ H_i \end{bmatrix} mod1 \tag{13}$$

IV. PARAMETER FOR EVALUATION IMAGE ENCRYPTION SCHEME

Once an image is encrypted with a specific algorithm, its ability resists different attacks is evaluated. To examine the weakness of encryption algorithms, various test help to find the vulnerably so that they can be used as adversary [15]. Here are some parameters that can be used to inspect the reliability of an encrypted image.

A. Correlation Coefficient

Correlation coefficient decides the measurable connection between two factors. It estimates the level of likenesses between two factors. The relationship coefficient is a useful procedure to evaluate the idea of encryption. A plain text picture has a high relationship between's its neighboring pixels in diagonals, flat and vertical [16]. If the correlation coefficient is one it implies that two images are indistinguishable and perfect correlation. To attain a better-cipher image we try to decrease the correlation coefficient to exceptionally low or close to zero. when the correlation coefficient reaches -1 then the encrypted image is negative of the original image. Consider a grayscale image of plain text and encrypted text. Let p and q be the two-pixel at the same point in plain and cipher image, then the correlation coefficient can be represented as

$$C.C = \frac{Cov(p,q)}{\sigma_p * \sigma_q}$$

$$\sigma_p = \sqrt{VAR(X)}$$

$$VAR(p) = \frac{1}{N}\sum_{i=1}^{N}(p_i - E(p))^2$$

$$Cov(p,q) = \frac{1}{N}\sum_{i=1}^{N}(p_i - E(p))(q_i - E(q)) \tag{14}$$

Here, C.C is represented as the correlation coefficient and Cov is the covariance between pixels x and y for gray scale images of plain text and cipher text [17]. VAR(x) is variance at pixel value x in plain text, σ is known as standard deviation, E is the expected value and N and total number of pixels are N*N in the matrix.

B. Image Entropy Evaluation

Image entropy characterizes the level of randomness and state of intensity to which individual pixels can adjust, it is a significance Image entropy characterizes the level of randomness and state of intensity to which individual pixels can adjust part of the quantitative analysis of an encryption process. Image entropy provides the degree of uncertainty depicting the strength of encrypted images [18] . Entropy is measured as a disorder which means as disorder rises in images , the entropy rises which makes image less predictable and more secure. The entropy S(m) of an image is calculated as .

$$S(x) = \sum_{p=0}^{2^N-1} q(x_p) \times \log_2 \frac{1}{q(x_p)} \tag{15}$$

Here $q(x_p)$ is probability of occurrence of the symbol x_p . Consider a random source that generates 28 value with equivalent probability ie,x=(x1,x2,x3.....,x28), where each symbol is of 8 bits, which are the uniform arbitrary source. Overall the entropy value is smaller than the ideal value, Encrypted message with a source that generates 28 symbols with comparable probability, then its entropy is 8 bits . In the instance of entropy being under 8 bit then there exists a level of consistency, In request to oppose different attack, the entropy should be close to the ideal value.

C. Histogram Analysis

Histogram investigation is a graphical portrayal of the number of pixels of an image as a component of its intensity. An extraordinary encryption calculation produces cipher text that doesn't reveal any applicable information associated with the original picture. The irregular distribution of pixels values of cipher image decides by utilizing histogram investigation. Encrypted image pixels should be coherent and equally disseminated so it is hard to penetrate stastical attacks.

D. Peak Signal-to-Noise Ratio

Peak signal-to-noise ratio (PSNR) can be utilized to quantify an encryption plot that mirrors the nature of encryption. It reflects the change in pixel value between plain text and encrypted text. Higher the PSNR value better the nature of encryption. In order to accomplish better encryption mean square error (MSE) will be really less as addressed. PSNR can be represented as [19]

$$PSNR = 10 \times log_{10}\left[\frac{M \times N \times 255^2}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(P(i,j)-C(i,j))^2}\right] \quad (16)$$

Here, M is the width and N is the height of digital image ,where p(i, j) is the pixel value of plain image and C(i, j) is the pixel value of cipher image of coordinate (i,j).Lower the PSNR better is the encryption.

E. Differential Attack Investigation

Differential attack investigation relates the difference between related plain text and encrypted text. It relies upon the diffusion technique which suggests that the single piece change in the plain text prompts a total change in the ciphertext that will change absolutely in an unessential manner. In diffusion of an encrypted image algorithm, means the resulting pixel of the cipher image ought to rely upon the plain image [20].

The number pixel change rate (NPCR) and unified average change intensity (UACI) are pair of techniques that can be executed to inspect the capacity of cipher image to endure differential attacks. Number pixel rate change (NPCR) is the property that with a little change in the pixel of a plain image ought to cause huge change in an encrypted image. Let X and Y be a pair of enc cipher images whose differ by only one bit at pixel (p,q) is X(p,q) and Y(p,q) ,Now Y(p,q) is determined by X(p,q)==Y(p,q) then Z(p,q)=0 otherwise $ Z(p,q) = 1

Therefore NPCR is represented as.

$$NPCR = \frac{\sum_{1,q} Z(p,q)}{w \times h} \times 100\% \quad (17)$$

H ,w and h are denoted as width and height of cipher image and X and Y are cipher texts. NPCR refers percentage of various pixels between the plain image and encrypted image which is calculated. NPCR can likewise be known as finding the rate of pixels and variation in an encrypted image due to a substitute a unit pixel of an original image [21].

Unified Average change rate (UACI) is defined as the difference between the average intensities of two images which helps to test the differential attack of cipher images. UACI is represented as.

$$UACI = \frac{1}{w \times h}\left[\sum_{p,q}\left(\frac{X_1(p,q)-X_2(p,q)}{255}\right)\right] \times 100\% \quad (18)$$

NPCR and UACI tests score are easy to calculate and interprets with a good sense of encryption technique. Higher the NPCR and UACI better the encryption algorithm.

F. Key Space Evaluation

Key Space refers to the total number of all conceivable keys which attempted to encrypt and decrypt the image. An encrypted image is transmitted in a public channel while a security key is transmitted through a private channel. Key space should be huge to brute force assault. As the size of key space expands the number of calculations increases because of the complexity of an algorithm. Key sensitivity is also an significant factor in which encryption and decryption of an image should be majorly dependent on its key sensitivity, bit change in keys generate different cipher images. It tests how much cipher image is sensitive toward keys. Confusion and diffusion in a cipher image are important to prevent plain text attacks [22]. Absolute image encryption should be highly sensitive and a change in one pixel ought to deliver something inconsistent image.

G. Effect of Noise

Various encryption algorithms are sensitive to noise attacks. Noise opposition ability shows to withstand noise for a cipher image. Different SNR noise is added in cipher images to examine noise immunity [8]. If a decrypted image is exceptionally near to a real image then the cryptosystem is invulnerable to noise. A decent and optimised image encryption procedure should work in a noisy space ,it means it will unaffected with noise .

V. CONCLUSION

With the rapid development in communication and computer networks, the security of images is a significant issue to keep up with privacy. Encryption of images before transmission is viable means to guarantee the protection of data. Image is highly sensitive in terms of correlation coefficient and adjacent pixels. In this review paper, we studied and conclude various chaos-based encryption schemes that every encryption scheme is unique and valuable in its way, and all techniques are useful for real-time digital encryption. Image encryption varies in some factors like keyspace, and some sensitive parameters. Every day new encryption techniques evolve for the quick and more secure transmission of information.

Chaotic Map	**Properties**		**Advantage**	**Disadvantage**
	Corelation Coefficent	**Key space**	Low Computaion Easy Implement	Less Parameter, discontinuous, Small Range
1-Dimensional	-	-	Simple and Easy to Implement, High Sensitive	Limited Range, small key space
1D LM(logistic map)	High	10^{45}	Simple Structure , and better Key space	Weak accuracy, limited chaotic range
Sine and Tent Map	-	-	Expanded Key Space, line ergocity	Less perodic space,
2-D Logistic map	-	-	Large chaotic Value	Less secure due to obtain ,simple structure
2-D SLMM	-	-	Large Complex value	less secure due to simple structure
2-D Henon Map	High	2^{148}	More secure based on diffusion, genrate PSNR fast	Less Key space and sensitivity
2-D Baker Map	High	2^{128}	Permutaion and shuffling of pixel	Perodic in nature, limited iteration.
3-D Chaotic	-	-	Efficent , more secure and simple	Perodic
8-D Chaotic	-	-	Lookup table method, key space large and secure	Electronic code book is not use that make less secure

REFERENCES

[1]. N. F. Elabady, H. M. Abdalkader, M. I. Moussa, and S. F. Sabbeh, “Image encryption based on new one-dimensional chaotic map,” in *2014 international conference on engineering and technology (ICET)*, 2014, pp. 1–6.

[2]. M. Kumar, R. A. M. Lahcen, R. N. Mohapatra, C. Alwala, and S. V. K. Kurella, “Review of image encryption techniques,” *J. Comput. Eng.*, vol. 14, no. 1, pp. 31–37, 2020.

[3]. B. Zhu, A. Jiang, X. Bai, and D. Bai, “A method research of image encryption based on chaotic and secret sharing,” in *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 2015, pp. 1823–1828.

[4]. A. H. Abdullah, R. Enayatifar, and M. Lee, “A hybrid genetic algorithm and chaotic function model for image encryption,” *AEU-International J. Electron. Commun.*, vol. 66, no. 10, pp. 806–816, 2012.

[5]. X. Gao, “A color image encryption algorithm based on an improved Hénon map,” *Phys. Scr.*, vol. 96, no. 6, p. 65203, 2021.

[6]. C. Wei-Bin and Z. Xin, “Image encryption algorithm based on Henon chaotic system,” in *2009 International Conference on Image Analysis and Signal Processing*, 2009, pp. 94–97.

[7]. R. Zahmoul, R. Ejbali, and M. Zaied, “Image encryption based on new Beta chaotic maps,” *Opt. Lasers Eng.*, vol. 96, pp. 39–49, 2017.

[8]. R. Parvaz and M. Zarebnia, “A combination chaotic system and application in color image encryption,” *Opt. \& Laser Technol.*, vol. 101, pp. 30–41, 2018.

[9]. Z. Hua, B. Zhou, and Y. Zhou, “Sine chaotification model for enhancing chaos and its hardware implementation,” *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1273–1284, 2018.

[10]. Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, “2D Sine Logistic modulation map for image encryption,” *Inf. Sci. (Ny).*, vol. 297, pp. 80–94, 2015.

[11]. G. M. Kumar and V. Chandrasekaran, “A novel image encryption scheme using Lorenz attractor,” in *2009 4th IEEE Conference on Industrial Electronics and Applications*, 2009, pp. 3662–3666.

[12]. C. Guanrong, M. Yaobin, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos, Solitons and Fractals*, vol. 21, 2004.

[13]. Y. Liu, J. Zhang, D. Han, P. Wu, Y. Sun, and Y. S. Moon, “A multidimensional chaotic image encryption algorithm based on the region of interest,” *Multimed. Tools Appl.*, vol. 79, no. 25, pp. 17669–17705, 2020.

[14]. D. Valli and K. Ganesan, “Chaos based video encryption using maps and Ikeda time delay system,” *Eur. Phys. J. Plus*, vol. 132, no. 12, pp. 1–18, 2017.

[15]. S. Chapaneri, R. Chapaneri, and T. Sarode, “Evaluation of chaotic map lattice systems for image encryption,” in *2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA)*, 2014, pp. 59–64.

[16]. A. M. Babu and K. J. Singh, “Performance evaluation of chaotic encryption technique,” *Am. J. Appl. Sci.*, vol. 10, no. 1, p. 35, 2013.

[17]. H. Liu and Y. Liu, “Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve,” *Opt. \& Laser Technol.*, vol. 56, pp. 15–19, 2014.

[18]. C. Candan, M. A. Kutay, and H. M. Ozaktas, “The discrete fractional Fourier transform,” *IEEE Trans. signal Process.*, vol. 48, no. 5, pp. 1329–1337, 2000.

[19]. A. S. Menon and K. S. Sarila, “Image encryption based on chaotic algorithms: An overview,” *Int. J. Sci. Eng. Technol. Res.*, vol. 2, no. 6, pp. 1328–1332, 2013.

[20]. Y. Wu, J. P. Noonan, S. Agaian, and others, "NPCR and UACI randomness tests for image encryption," *Cyber journals Multidiscip. journals Sci. Technol. J. Sel. Areas Telecommun.*, vol. 1, no. 2, pp. 31–38, 2011.

[21]. Y. Wu, J. P. Noonan, G. Yang, and H. Jin, "Image encryption using the two-dimensional logistic chaotic map," *J. Electron. Imaging*, vol. 21, no. 1, p. 13014, 2012.

[22]. A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, "Symmetric encryption algorithms using chaotic and non-chaotic generators: A review," *J. Adv. Res.*, vol. 7, no. 2, pp. 193–208, 2016.