IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 18, Issue 4 Ser. I (Jul. – Aug. 2022), PP 32-39
www.iosrjournals.org

Image Encryption on Chaotic Maps: A Survey of Chaos Detection Algorithms.

F. E. Abd Elbary[1], A. M. Abdelwahab[2], F. E. H. Khalil [3],Z. H. Abdelwahab[4], W. Alsobky[5].

[1, 5](Department of Engineering Mathematics and Physics, Faculty of Engineering Benha, Benha University, 11629 Cairo, Egypt),
[2](Collage of Engineering and Technology, AASTMT),[4](Communications Engineering Department, Higher Technological Institute, Ramadan city, Egypt).

***Abstract**: In recent years, security concerns have grown tremendously, necessitating extremely secure picture transmission. Image encryption based on chaos is gaining popularity as a more safe and stable method of securing images than previous encryption methods.. As a result, new chaotic dynamical systems with more advanced characteristics and models are being developed for this purpose. To investigate and analyze their complexity, they are subjected to various chaos detection techniques. This study looks at the frequency and effectiveness of chaos experiments performed on 18 discrete chaotic systems. As a result, three key facts must be understood. The emerging system must first be carefully analyzed using a suitable chaos detection method. Second, a system's chaotic and quasi regions must be represented in their complete. Third, the chaos's strength must be considered. These studies are essential for developing a highly secure nonlinear key for an attack-resistant encryption scheme.*

***Keywords –**; chaotic Maps; Chaos detection Algorithms; image encryption based on chaos.*

Date of Submission: 24-06-2022 Date of Acceptance: 07-07-2022

I. INTRODUCTION

With the huge rise of communications systems, data leakage happens in an incredible stream during network storage and communication. Most network users are now aware of the effects of information leaking [1, 2]. One of the primary concerns in multimedia communication is the secure storage and transmission of digital images [3, 4]. Three methods for protecting digital data from unwanted access and criminal use include cryptography, steganography, and watermarking [5, 6, 7]. Cryptography is one of these, and it plays an important role in enabling highly secure communication over an unsafe channel. Stream cyphers and block cyphers are two types of cryptographic algorithms. Stream cyphers encrypt digital data bit by bit with a secret key generator, whereas block cyphers encrypt blocks of bits. Image security is generally handled using various cryptographic techniques that convert messages to be transmitted into an unreadable and unintelligent form by encryption process, so that only authorized persons can correctly recover the information by decryption process, and is widely recognized as the best method of information protection and image security. Conventional cryptographic techniques like (AES), (DES), International Data Encryption Algorithm (IDEA), Rivest-Shamir-Adleman (RSA) algorithm, ElGamal algorithm are primarily designed for text and have been effective solutions to the information security problems. However, they are found not suitable for encrypting images due to the following three reasons: (i) Because images are always very huge in size, encrypting them using traditional methods takes longer., (ii) A encrypted image does not have to be identical to the original image; in fact, due to human perception properties and the great redundancy of image data, a decrypted image with minor distortion is frequently acceptable to the eyes.(iii) The contents of digital images are closely connected, and previous approaches do not take advantage of this fact, reducing the encryption efficiency. Various image encryption and concealing systems have been developed to increase the efficiency and security image encryption methods. Among these schemes, the chaos based encryption schemes got the attention of many researchers because of its interesting properties, which include: determinism and ergodicity, sensitivity to the initial condition and control factors. Table I shows the differences between chaos-based systems and conventions algorithms..

The rest of this paper is organized as follows: Section II will provide a review of the literature on chaos-based image cryptographic algorithms. The classes of maps and their characteristics are explained in section III. A relatively short study of chaos identification experiments is presented in section VI. We give a thorough list of commonly used maps in image coding in section V. Furthermore, "Discussion" examines the frequency of chaos detection approaches used for reviewing the novel chaotic maps nonlinear dynamic properties. The need of adopting an appropriate chaos detection Algorithm to establish completely chaotic behaviuor in new dynamic systems is highlighted at the end of the review paper.

Table1: Difference between chaotic system & Cryptographic system

Systems in chaos	**Cryptographic algorithms**
-Phase space set of numbers -Iterations -Parameters	-Phase space finite set of integers -Rounds -key
Sensitive to parameters and initial conditions.	Diffuse.

II. LITERATURE REVIEW

This section examines a variety of survey papers on the issue of Chaos-based image encryption schemes. To draw attention to the evolution and challenges of the chaos-based cryptographic system. Several literature studies have been conducted over time, some of which are listed in the table2.

Table2: Review Of Chaos-Based Image Encryption algorithm literature

a survey	**Headline**
1. Li et al. [8]	A review of images cryptography algorithms was presented in 2018.. The issues of designing and analyzing image encryption algorithms are discussed.
2.Chapter 1: A Survey on Chaos Based Image Encryption Techniques[9]	An examination of image encryption schemes based on chaos The advantages and disadvantages of using chaotic maps in image encryption
3. Kamal et al. [9] Chapter 2: An assessment of chaotic maps for encrypted images	The reliability of chaotic map-based encryption techniques is examined. PSNR, NPCR, UACI, correlation coefficient, computing time, and entropy are among the performance measures examined.
4. Younes et al. [10]	An study of several image encrypting algorithms
5.Sharma et, al. [11]	Encryption of images in the spatial and frequency domain: a review of the literature
6.Suneja et al. [12]	Significant security evaluations Comparing and studying chaotic maps
7.Ozkaynak [13]	Chaos-based image encryption is compared and classified. Features of a chaos-based encrypted images

Because of the inherent properties of chaos, the survey found that image encryption with chaos is the most desirable method for encrypting an image (see Table 2).

To demonstrate and establish the strength of chaos-based cryptosystems (GVD), the authors used performance measures such as key space analysis, key sensitivity analysis, (PSNR), (UACI), statistical attack analysis, net pixel change ratio (NPCR), information entropy, and grey value difference[9].

As a result, the focus of this review paper is on reviewing some of the discrete chaotic maps that are often utilized in numerous publications, as well as the techniques for detecting chaos that are used to examine these maps.

III. THE CHARACTERISTICS OF CHAOS

A. Chaos's Characteristics

Many important aspects characterize chaos, making it ideal for constructing a secure cryptosystem. It has been correlated with sensible initial conditions, non - linearity, determinism, ergodicity, non-periodicity, and unpredictable behavior [11, 27, 28].

Table3: Summarizes The Chaos Characteristics

Chaotic features	**Indicating**
Deterministic	Mathematical equations can be used to represent and govern the process, and it can be handled quantitatively to some extent.
Sensitive to initial conditions	A simple modification in the starting condition has a significant impact on the output.
Non-linear	The output has no direct relationship with the input.
Non-periodicity	The technique makes random results..
Unpredictable	The cumulative impact of many contacts produces an unpredictable outcome.
Ergodicity	The model's long-term average predictions is possible.

B. Classification of Chaos

Both the discrete computation and the continuous chaos system are chaotic processes. Iterative equations are used to construct dynamical systems with discrete domain. They're called "chaotic maps". One-dimensional and multi-dimensional maps are the two types of maps available. The coupled map lattice (CML) is a new type of chaotic map that was created to address chaotic maps' restricted and discontinuous range [17, 18].Continuous-time dynamical systems are also governed by differential equations. They're called chaotic systems since they appear in three or more dimensions[19], It will be discussed in detail in another study. Figure1 shows the chaotic nonlinear dynamical system classifications.

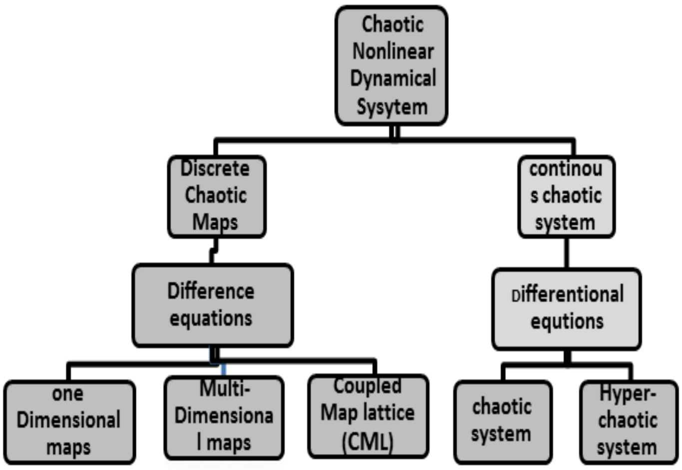

Fig1 Chaotic nonlinear dynamical system classification

IV. CHAOS DETECTION TECHNIQUES

Chaos theorists have proposed numerous chaos detection algorithms that review the dynamic system's behaviour in multiple dimensions [20]. They have a crucial role in defining the level of confusion in chaotic systems.. These chaotic experiments find use within biology, physics, economics, meteorology, social psychology and, instrumentation, among other areas. This section covers some chaos detection algorithms, as well as the approach and the necessity of using them.

A. Lyapunov Exponent(LE)

The Lyapunov exponent is a measure of how sensitive and predictable a dynamic system is to change in its initial condition[21]. It is mathematically compute the mean logarithmic rate of distance or convergence of two neighbouring pair of point time series Xt and Yt divided by an initial range $\Delta R_0 = \|X_0 - Y_0\|_2$.

The following equation is used to determine the Lyapunov exponent:

$$\lambda = lim\frac{1}{n}\sum_{i=1}^{n} ln\left|\frac{\Delta R_i}{\Delta R_0}\right|, \qquad (1)$$

Where $\boldsymbol{\lambda}$ is the Lyapunov exponent.There are n Lyapunov exponents in a chaotic system with n - dimensional space. A chaotic system is one that has a positive Lyapunov exponent. For integer-order dynamical systems with known equations, the Lyapunov exponent is often employed. This technique is ineffective for evaluating experimental results or a fractional-order dynamic system with an uncertain equation.In these kind of cases, space - time restructuring is required to estimate the Lyapunov exponent [22].

B. Bifurcation Diagram(BD)

One of the most significant tools for studying the behaviour of a dynamic system is the bifurcation diagram. It's a crucial graphical tool for detecting system cycles as a function of system control parameters, from periodic to chaotic orbits. It plots the discrete map or continuous system control parameter against the steady state solution. The bifurcation diagram is important because it shows how a qualitative behaviour emerges suddenly as a parameter is modified. Bifurcation is a behaviour result of a change when two sets divide[23Because it is relatively easy to draw and detect the chaos and quasi domains that use this diagram, it is a common study approach for investigating dynamic systems. It can also be used to illustrate how the period doubling approach leads to chaos. However, because it is dependent on human vision's perceptiveness, its use takes time [20].

C. Three-State Test (3ST)

The (3ST) was created to diagnose the dynamic system's behavior qualitatively. Because it labels behaviour with one of three states: chaotic, semi, or periodic, Because it labels behaviour with one of three states: chaotic, semi, or periodic, it has been shown to be superior than existing chaos detection techniques. Furthermore, the bifurcation diagram is automated, as is the discovery of the period double approach to chaos [20]. The (3ST) is based on a data series pattern analysis. The data set investigates the distribution of system states as a function of time. A regular signal is identified by a simple pattern that emerges at periodic intervals in the data series. After a lengthy period of observation, a quasi-periodic signal has a basic pattern that repeats repeatedly. The basic pattern cannot be identified in non-regular dynamics, and the period cannot be accurately stated. Finally, the sensitivity index λ of the 3ST describes nature's dynamism of the chaotic map. The three states of λ are classified according to their sign, with λ = 0 indicating periodical signals , λ<0 indicating the presence of quasi periodic signals, and , λ > 0 indicating chaotic signals. Another noteworthy finding established by the 3ST is the time period's evaluation L. As a result, the 3ST generates two outputs: a cycle of periodical orbits L and a regularity index represented as:

$$3ST(\varphi(x)) = \begin{cases} L \\ \lambda(n) \end{cases} \quad (2)$$

As a result, the chaotic map's dynamic character as cyclic, semi, or chaotic has been confirmed, as well as other benefitsIt operates with set of data directly and does not require previous knowledge of the chaotic map's mathematical formulation. It is independent by the vector field's nature or dimensions. Furthermore, the 3ST has a cheap computational cost and is simple to implement when compared to the Lyapunov exponent . Only discrete maps have been confirmed, and results for continuous time series data are currently being established, albeit they appear optimistic [20].

D. Sample- Entropy(SE)

The samples entropy (SE) is a useful measure for describing chaotic sequence behaviour It is employed to estimate the unpredictability of a set of time-series data without knowing anything about the dynamic system that created it [24]. For a time series, SE [25] estimation $\{x_1, x_2, \ldots, x_n\}$ of dimension N, template vector $Xm(i) = \{x_i, x_{i+1}, \ldots, x_{i+m-1}\}$ of size, m and acceptance, religious tolerance r is achieved in the following eqn.(3).

$$SE(m, r, N) = -log\frac{A}{B}, \quad (3)$$

Where A and B : are the number of vectors for $d[X_{m+1}, (i)X_{m+1}(j)] < r\ and\ d[X_m(i), X_m(j)] <$ r , respectively, and $d[X_m(i), X_m(j)]$
$X_m(i) and X_m(j)$are separated by the Chebyshev distance. A larger SE number indicates that there is more irregularity in the time series data, and thus greater complexity.

E. Histogram (Hist)

The histogram is a graphical depiction of a set of data distribution. It's a graph of a set of data vs its frequency of occurrence.. The histogram is a useful tool for detecting numerous phenomena in chaos dynamics. To illustrate the dynamical system's complexity, the histogram for phase space values created by the dynamic system is provided. The dynamical system's behaviour is periodic if only a few data are included in the histogram, and the trajectories are bound to restricted regions of the phase space [26]. Weak chaos is visible in an unequal distribution, making it subject to statistical attack. A histogram with an even distribution suggests that the likelihood of each space - time value occurring is uniform. As a result, value predictability is problematic. As a result, this denotes the presence of significant chaos [27]. As a result, the histogram is a fairly basic visual tool for understanding any system's dynamical behaviour

F. -Kolmogorov Entropy(KE)

A measure of a system's predictability is the Kolmogorov Entropy, often known as the Kolmogorov Sinai entropy(KS). Kolmogorov entropy K can be determined as long as two sites on the attractor are divided in space by within an insignificantly small length scale. For a big number of pair, this method yields K with high precision. K equals zero for a perfectly periodic, predictable system, whereas K is endlessly high for a stochastic system. In a system with deterministic chaos, K is a finite positive value.. As a result, the)KS(entropy predicts the chaotic and complex motion in the dynamical system [21, 28].

G. Correlation Dimension(CD)

The correlation -dimension is a fractal- dimension that depicts the spatial dimensions of a set of points.. It is a suitable .tool for determining the uniqueness of a dynamic system's attractor.The following equation is used to compute the correlation dimension:

$$d = \lim_{r\to\infty} \lim_{M\to\infty} \frac{logC_r(r)}{log\, r}, \quad (4)$$

Where $logC_r(r)$is defind as the correlation integral. A significant correlation dimension value indicates that the trajectories occupy more dimensional space. The correlation dimension is frequently used to demonstrate the strange nature of the complex, chaotic attractor [29, 30]

H. Phase Portrait(PP)

It is critical to describe the behaviour of a dynamical system in phase space in order to handle its complexity and dynamics. A set of rules defines this system, which maps a current condition into the future. Consider the dynamical system as a simple function f acting on a state space U. U is referred to as the phase space here. Iterates are obtained from the the given equation [26] given f: U→ U and an initial point x_0∈ U:

$$x_{n+1} = f(x_n) \ , \quad n \in N \qquad (5)$$

Plottingx_n versus x_{n+1}yields the phase portrait, which is used to analyze various discontinuous maps and continuous systems. However, in continuous systems, it is more typically used to investigate the attractor butterflies pattern.

I. Time -Series Analysis(TS)

The graphical evaluation of time- series data obtained by charting the dynamic system's data series against time is known as time- series analysis. It is a data analysis of a dynamical system that represents the characteristics of data series. The data's periodicities and complex are projected properties [21]. Time is viewed as distinct here, and the index i is used to label it. The progress of the dynamical system is tracked by combining the time and space variables, which are written as (t_0,x_0),(t_1,f (x_0)),...,(t_n,f^n (x_0)),... Time series data is a straightforward approach to detecting complexity both in discrete and continuous system dynamics.

V. SURVEY OF DISCRETE CHAOTIC MAPS USED IN IMAGE ENCRYPTION

Some of the most commonly used chaotic maps for the image encryption confusion and diffusion process are the Arnold's cat map, logistic map, sine map , Henon map and tent map. Due to their small and discontinuous chaotic range, they are altered to provide a larger chaotic range than the actual seed maps.To construct new maps, add a nonlinear term, increase the number of dimensions, control settings, or couple seed maps. This section contains a comprehensive collection of both traditional and adapted chaotic maps.

A list of chaotic maps and their major characteristics can be found in Table 4. The adjusted maps are submitted to multiple chaos tests to identify nonlinear behaviour and verify the chaotic region.. The tests conducted to investigate the modified maps indicated in Table 4. The tick (*) symbol in Table V indicates the tests on the updated new chaotic map. The other empty columns in the table indicate that no tests on the altered map were performed. Table V illustrates the tests the authors used to analyse the maps generated. The most often used tests to analyse the behaviour of the map are the bifurcation diagram and the Lyapunov exponent. The bifurcation diagram and Lyapunov exponent are the most used chaos tests for analyzing the non-linear behaviuor of chaotic maps, as shown in Fig. 2. The bifurcation graphic shows fixed points, periodic orbits, and chaotic attractors for 96 % of chaotic maps under various control parameter values. For 88 % of chaotic maps, the range of chaos is determined using the Lyapunov exponent, and it is the second most commonly employed test. Only 32% of chaotic maps with entropy of a sample are studied for their complexity. For just 28% of the chaotic maps, the geometric representation of their trajectories is shown in the phase plane with the phase portrait. Furthermore, only 16% of chaotic maps use the correlation dimension to estimate the fractal dimension, and only 12% of chaotic maps are statistically investigated using time- series analysis.Other chaos tests described are only employed in a small percentage of cases (less than 10%). For the examination of the 18 chaotic maps chosen for inquiry, none of the authors considered(3ST).

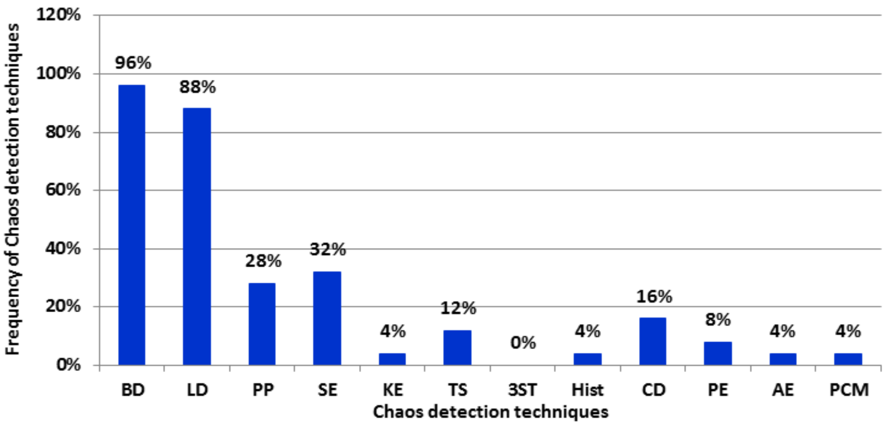

Fig.2 On new discrete chaotic maps, a survey of chaos detection algorithms was performed

VI. CONCLUSION

A examination of chaos detecting methods employed to 18 discrete chaotic maps found that this paper did not give a full characterization of several modified chaotic maps. According to the results of the survey, the Lyapunov exponent and bifurcation diagram are the most well-liked for analyzing chaotic maps.Although these tests produce some interesting results, they do not provide a complete picture of the chaotic process's behaviour.Other tests are given less importance, such as (3ST) and various entropy tests. Insufficient and undetected understanding of the chaotic approach criteria and conditions may result from an incomplete investigation of a novel dynamic system. Although performing all of the tests on the chaoticprocess is not required, it is vital to select the right chaos detection approach and offer a comprehensive analysis of the chaotic process. As a conclusion, additional in-depth experimentation and study on new chaotic maps and systems is strongly encouraged and recommended in order to develop a safe, chaotic image encryption system that is resistant to various attacks.

Table 4. listing of chaotic maps and their related number of dimensions, parameters, and chaotic range

Maps of Chaos	**Formula in mathematics**	**No of control Parameters**	**No of dimensions**	**Range of chaos**
1- Logistic map [43]	$x_{n+1} = rx_n(1 - x_n)$	1	1	r ∈ [3.54, 4]
2-Sine map [31, 25, 29]	$f_r(x) = r\,sin(\pi x)$	1	1	r ∈ [0.87,1]
3-Generalized logistic map [32, 33]	$f(x) = \frac{4\mu}{1 + 4(\mu^2 - 1)x(1 - x)}$	1	1	μ∈ [−0.6795, 0.4324]
4-Squared sine logistic map [34]	$f(x) = rx(1 - x) + \mu sin^2(2x)$	1	1	r ∈ [3.5, 6.5]
5-Enhanced -sine map [29]	$x_{n+1} = sin(\pi\tilde{\mu}sin(\pi x_n))$			$\tilde{\mu} \in (0, +\infty)$
6. Enhanced -logistic map [29]	$x_{n+1} = sin(\pi\tilde{a}x_n(1 - x_n))$	1	1	$\tilde{a} \in (0, +\infty)$
7-Enhanced tent map [29]	$x_{n+1} = \begin{cases} sin(\pi\tilde{r}x_i)\; x_i < 0.5 \\ sin(\pi\tilde{r}(1 - x_i)) \quad x_i \geq 0.5 \end{cases}$	1	1	$\tilde{r} \in (0, +\infty)$
8-Enhanced Henon map [29]	$\begin{cases} x_{i+1} = sin(\pi(1 - \tilde{a}x_i^2 + y_i) \\ y_{i+1} sin(\pi\tilde{b}x_i) \end{cases}$	2	2	$\tilde{a} = 912$ $\tilde{b} = 39$
9-Modified logistic chaotic map [35]	$x_{n+1} = 2\beta - x_i^2/\beta$	1	1	[22] cryptanalyzed an infinite key space.
10-Tent map [44]	$\boldsymbol{x_{n+1}} = \begin{cases} \boldsymbol{rx_n}\;; \quad \boldsymbol{x_n} < \frac{1}{2} \\ \boldsymbol{rx_n(1 - x_n)}\;; \boldsymbol{x_n} \geq \frac{1}{2} \end{cases}$			r ∈ [0,2]
11-(1D)- sine- powered chaotic map (1DSP) [25]	$x_{n+1} = (x_n(\alpha + 1))^{sin(\beta\pi + x_n)}$	2	1	α∈ [2.5,4]
12- Logistic-sine–cosine (LSC) map [36]	$x_{n+1} = cos(\pi(4rx_n(1 - x_n) + (1 - r)\,sin(\pi x_n) - 0.5))$	1	1	r ∈ [0,1]
13-2D Hénon-Sine Map (2D-HSM) [45]	$\begin{cases} x_{n+1} = (1 - asin^2(x_n) + y_n)mod1, \\ y_{n+1} = bx_n mod1, \end{cases}$	2	2	a ∈ (−∞, −0.71] ∪ [0.71, ∞), b = 0.7
14-Sine-tent-cosine (STC) map [36]	$x_{n+1} \begin{cases} cos(\pi(rsin(\pi x_n) + \\ 2(1 - r)x_n - 0.5)x_n < 0.5 \\ cos(\pi(rsin(\pi x_n) + \\ 2(1 - r)(1 - x_n) - 0.5)x_n \geq 0.5 \end{cases}$	1	1	r ∈ [0,1]
15-Tent-logistic-cosine (TLC)map [36]	$x_{n+1} \begin{cases} cos(\pi(2rx_n + \\ 4(1 - r)x_n(1 - x_n) - 0.5)x_n < 0.5 \\ cos(\pi(2(1 - x_n) + \\ 4(1 - r)x_n(1 - x_n) - 0.5)\,)\,x_n \geq 0.5 \end{cases}$	1	1	r ∈ [0,1]
16-Logistic-sine system [37]	$x_{n+1} = (rx_{n(1-}x_n) +$ $(4 - r)sin(\pi x_n)$/4) mod1	1	1	r ∈ [0,1]
17- 2D logistic chaotic map [38]	$x_{n+1=}x_n u_1(1 - x_n) + \lambda_1 {y_1}^2$ $y_{n+1=}y_n u_2(1 - y_n) + \lambda_2({x_n}^2 + x_n y_n)$	2	2	$2.75 < u_1 \leq 3.4$ $2.75 < u_2 \leq 3.45$ $0.15 < \lambda_1 \leq 0.21$ $0.13 < \lambda_2 \leq 0.15$
18-(4D)- chaotic map [39]	X=p(eh)g Y=hf Z=bhe W=h	6	4	P+40, b=40 h0=0:3. e0=0:3, f0=0:3,g0=0:3
19-Modified logistic map	$z_{n+1} = \mu_z z_n(1 - z_n)(1 - {z_n}^2)$	1	1	$3.9 < \mu_z \leq 6.27$

[40]				
20-Improved modified logistic map [41]	$x_{n+1} = \lvert \mu x_n(1 - x_n) \times 10^j \rvert - \mu x_n(1 - x_n) \times 10^j$	2	1	$0 \leq \mu \leq 4$ $2 \leq j \leq 8$
21-Chaotic coupled sine map (CCSM) [42]	$=x_{n+1} = \alpha \lvert sin(\beta^3 \pi x_n) \rvert + (1-\alpha)(1-\lvert sin(\gamma^3 \pi x_n)(1 - xn)))$	3	1	$\alpha \in [0,1]$ $\beta, \gamma \in [8, 10]$

Table 5. Chaos detection techniques performed on the novel discrete chaotic maps tabulated in Table 4.

Maps of Chaos	Formula in mathematics	BD	LE	PP	SE	KE	TS	3ST	Hist	CD	AE	PCM
1-Generalized -logistic -map [32, 33]	$f(x) = \frac{4\mu}{1 + 4(\mu^2 - 1)x(1-x)}$		*									
2-Squared sine logistic map [34]	$f(x) = rx(1 - x) + \mu sin^2(2x)$	*	*									
3-Enhanced sine map [29]	$x_{n+1} = sin(\pi \tilde{\mu} sin(\pi x_n))$	*	*		*					*		
4. Enhanced logistic map [29]	$x_{n+1} = sin(\pi \tilde{a} x_n(1 - x_n))$	*	*		*					*		
5-Enhanced tent map [29]	$x_{n+1} = \begin{cases} sin(\pi \tilde{r} x_i) & x_i < 0.5 \\ sin(\pi \tilde{r}(1 - x_i)) & x_i \geq 0.5 \end{cases}$	*	*		*					*		
6-Enhanced Henon map [29]	$x_{i+1} = sin(\pi(1 - \tilde{a}x_i^2 + y_i)$ $y_{i+1} sin(\pi \tilde{b} x_i)$	*	*		*					*		
7-Modified logistic chaotic map [35]	$x_{n+1} = 2\beta - x_i^2/\beta$	*	*	*								
8-(1D) sine- powered chaotic map (1DSP)[25]	$x_{n+1} = (x_n(\alpha + 1))^{sin(\beta\pi + x_n)}$	*	*	*		*	*					
9- Logistic sine cosine (LSC) map [36]	$x_{n+1} = cos(\pi(4r\ x_n(1 - x_n) + (1-r) sin(\pi x_n) - 0.5))$	*	*									
10-2D Hénon-Sine Map (2D-HSM) [45]	$\begin{cases} x_{n+1} = (1 - a sin^2(x_n) + y_n) mod 1, \\ y_{n+1} = b x_n\ mod 1, \end{cases}$	*	*	*								
11-Sine tent cosine (STC) map [36]	$x_{n+1} \begin{cases} cos(\pi(r sin(\pi x_n) + 2(1-r)x_n - 0.5) & x_n < 0.5 \\ cos(\pi(r sin(\pi x_n) + 2(1-r)(1-x_n) - 0.5) & x_n \geq 0.5 \end{cases}$	*	*		*							
12- -logistic -Tent -cosine (LTC)map [36]	$x_{n+1} \begin{cases} cos(\pi(2rx_n + 4(1-r)x_n(1-x_n) - 0.5) & x_n < 0.5 \\ cos(\pi(2(1-x_n) + 4(1-r)x_n(1-x_n) - 0.5)) & x_n \geq 0.5 \end{cases}$	*	*		*							
13-Logistic sine- system [37]	$x_{n+1} = (r x_{n(1-} x_n) + (4-r) sin(\pi x_n)/4) mod 1$	*	*									
14- 2D logistic chaotic map [38]	$x_{n+1} = x_n u_1(1 - x_n) + \lambda_1 y_1^2$ $y_{n+1} = y_n u_2(1 - y_n) + \lambda_2(x_n^2 + x_n y_n)$	*										
15-4D chaotic map [39]	$X = p(eh)g$ $Y = hf$ $Z = bhe$ $W = h$	*	*	*								*
16-Modified logistic map [40]	$z_{n+1} = \mu_z z_n(1 - z_n)(1 - z_n^2$	*	*								*	
17-Improved modified logistic map [41]	$x_{n+1} = \lvert \mu x_n(1 - x_n) \times 10^j \rvert - \mu x_n(1 - x_n) \times 10^j$	*	*									
18-Chaotic coupled sine map (CCSM) [42]	$=x_{n+1} = \alpha \lvert sin(\beta^3 \pi x_n) \rvert + (1-\alpha)(1- \lvert sin(\gamma^3 \pi x_n)(1 - x_n)) \rvert)$	*	*	*								

REFFERENCES

[1]. Dhall S, Pal SK, Sharma K (2017) Cryptanalysis of image encryption based on a new 1D chaotic Signal processing, PII S0165–1684(17)30434–6, https://doi.org/10.1016/j.sigpro.2017.12.021

[2]. Liu Y, Zhang LY, Wang J, Zhang Y, Wong K-w (2016) Chosen-plaintext attack of an image encryption scheme based on modified permutation–diffusion structure. Nonlinear Dynamics 84(4):2241–2250

[3]. Zhang Y, Xiao D, Wen W, Nan H (2014) Cryptanalysis of image scrambling based on chaotic sequences and vigen'ere cipher. Nonlinear Dynamics 78(1):235–240

[4]. Zhu Z-l, Zhang W,Wong K-w et al (2011) A chaos-based symmetric image encryption scheme using a bitlevel permutation. Inf Sci 181(6):1171–1186

[5]. Fu C, Meng W-h, Zhan Y-f et al (2013) An efficient and secure medical image protection scheme based on chaotic maps. Comput Biol Med 43(8):1000–1010

[6]. Wageda I. El Sobky, Abdelkader A. Isamail; Ashraf S. Mohra; Ayman M. Hassan" Implementation Mini (Advanced Encryption Standard) by Substitution Box in Galois Field (2^4)" 2021 International Telecommunications Conference (ITC-Egypt) DOI: 10.1109/ITC-Egypt52936.2021.9513927

[7]. Wageda Ibrahim Alsobky ,Abdelkader Esmail ,Ashraf S. Mohra, Ayman Abdelaziem "Design and Implementation of Advanced Encryption Standard by New Substitution Box in Galois Field (2^8)" International Journal of Telecommunications, IJT'2022, Vol.02, Issue 01

[8]. Li C, Zhang Y, Yong E. When an attacker meets a cipher-image in 2018: a year in review. J Inf Secur Appl. 2019;48:2361

[9]. Hosny KM. Multimedia security using chaotic maps: principles and methodologies. New York: Springer; 2020.

[10]. Younes MAB. Literature survey on different techniques of image encryption. Int J Sci Eng Res. 2016;7(1):93–8.

[11]. Sharma M, Kowar MK. Image encryption techniques using chaotic schemes: a review. Int J Eng Sci Technol. 2010;2(6):2359–63.

[12]. Suneja K, Dua S, Dua M. A review of chaos based image encryption. In: Proc. 3rd Int. Conf. Comput. Methodol. Commun. ICCMC 2019; 2019. pp. 693–8.

[13]. Ozkaynak F. Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dyn. 2018;92(2):305 13.

[14]. Niyat AY, Moattar MH, Torshiz MN. Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt Lasers Eng. 2017;90(90):225–37.

[15]. Davidovits P. Physics in biology and medicine, 5th edn. Elsevier; 2019. https:// doi. org/ 10. 1016/ B978-0- 12- 813716- 1. 00010-0.

[16]. Alligood KT, Sauer TD, Yorke JA. CHAOS : An introduction to dynamical systems. New York: Springer; 1996.

[17]. Zhang Y, He Y, Li P, Wang X. A new color image encryption scheme based on 2DNLCML system and genetic operations. Opt Lasers Eng. 2020;128:106040.

[18]. Zhang Y-Q, Wang X-Y. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf Sci (N Y). 2014;273:329–51.
[19]. Arumugham S, Rajagopalan S, Rethinam S, et al. Synthetic image and strange attractor: two folded encryption approach for secure image communication. Adv Intell Syst Comput. 2020;1082:467–78.
[20]. Eyebe Fouda JSA, Effa JY, Kom M, Ali M. The three-state test for chaos detection in discrete maps. Appl Soft Comput J. 2013;13(12):4731–7.
[21]. Rudisuli M, Schildhauer TJ, Biollaz SMA, Van Ommen JR. Fluidized bed technologies for near-zero emission combustion and gasification; 2013. https:// doi. org/ 10. 1533/ 97808 57098 801.3. 813.
[22]. Sun KH, Liu X, Zhu CX. The 0–1 test algorithm for chaos and its applications. Chin Phys B. 2010;19(11):7.
[23]. Sayed WS, Ismail SM, Said LA, Radwan AG. On the fractional order generalized discrete maps. In: Azar AT, Radwan AG, Vaidyanathan S, editors. Mathematical Techniques of Fractional Order Systems. Elsevier Inc.; 2018. https://d oi.o rg/1 0.1 016/B 978-0-1 2- 813592- 1. 00013-1.
[24]. elgado-Bonal A, Marshak A. Approximate entropy and sample entropy: A comprehensive tutorial. MDPI. 2019. https:// doi. org/ 10. 3390/ e2106 0541.
[25]. Mansouri A, Wang X. A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. Inf Sci (N Y). 2020. https:// doi. org/ 10. 1016/j. ins. 2020. 02. 008.
[26]. Tucker W. Studies in computational intelligence. Berlin, Heidelberg: Springer; 2008.
[27]. Parvaz R, Zarebnia M. A combination chaotic system and application in color image encryption. Opt Laser Technol. 2018;101:30–41.
[28]. Xiong H, Shang P, He J, Zhang Y. Complexity and information measures in planar characterization of chaos and noise. Nonlinear Dyn. 2020;100(2):1673–87.
[29]. Hua Z, Zhou B, Zhou Y. Sine chaotification model for enhancing chaos and its hardware implementation. IEEE Trans Ind Electron. 2019;66(2):1273–84. 30. Hua Z, Yi S, Zhou Y, et al. Designing hyperchaotic cat maps with any desired number of positive lyapunov exponents. IEEE Trans Cybern. 2018;48(2):463–73.
[30]. Kalpana J, Murali P. An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos. Optik. 2015;126(24):5703–9.
[31]. Krishnamoorthi R, Murali P. A selective image encryption based on square-wave shuffling with orthogonal polynomials transformation suitable for mobile devices. Multimed Tools Appl. 2017;76(1):1217–46.
[32]. Bhatnagar G, Wu QMJ. Selective image encryption based on pixels of interest and singular value decomposition. Digit Signal Process. 2012;1:1–16.
[33]. de Carvalho RE, Leonel ED. Squared sine logistic map. Phys A Stat Mech Appl. 2016;463:37–44.
[34]. Han C. An image encryption algorithm based on modified logistic chaotic map. Opt Int J Light Electron Opt. 2019;181:779–85.
[35]. ua Z, Zhou Y, Huang H. Cosine-transform-based chaotic system for image encryption. Inf Sci (NY). 2019;480:403–19.
[36]. Zhou Y, Bao L, Chen CLP. A new 1D chaotic system for image encryption. Signal Process. 2014;97:172–82.
[37]. Chai X, Chen Y, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations. Opt Lasers Eng. 2017;88:197–213.
[38]. Gupta A, Singh D, Kaur M. An efficient image encryption usingnon-dominated sorting genetic algorithm—III based 4—D chaotic maps. J Ambient Intell Humaniz Comput. 2019. https:// doi. org/ 10. 1007/ s12652- 019- 01493-x.
[39]. Hanis S, Amutha R. A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterflylike structure. Nonlinear Dyn. 2018;95:421–32.
[40]. Hanis S, Amutha R. A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterflylike structure. Nonlinear Dyn. 2018;95:421–32.
[41]. Attaullah, Shah T, Jamal SS. An improved chaotic cryptosystem for image encryption and digital watermarking. Wirel Pers Commun. 2020;110(3):1429–42.
[42]. Yosefnezhad B, Peyman I, Jabalkandi FA, et al. Digital image scrambling based on a new one-dimensional coupled Sine map Behzad. Nonlinear Dyn. 2019;97:2693–721.
[43]. Safi HW, Maghari AY (2017) Image encryption using double chaotic logistic map. In: Proceedings 2017. International Conference on Promising Electronic Technologies (ICPET), pp 66–70.
[44]. Wu J, Liao X, Yang B (2017) Color Image Encryption Based on Chaotic Systems and Elliptic Curve ElGamal Scheme, Signal processing, PII: S0165–1684(17)30134 2, https://doi.org/10.1016/j. sigpro.2017.04.006
[45]. Wu J, Liao X, Yang B (2018) Image encryption using 2D Hénon-Sine map and DNA approach. Sig Process 153:11–23

F. E. Abd Elbary. "Image Encryption on Chaotic Maps: A Survey of Chaos Detection Algorithms.." *IOSR Journal of Mathematics (IOSR-JM)*, 18(4), (2022): pp. 32-39.