Review Article

*ACCENTS Transactions on Information Security, Vol 2(5)*
*ISSN (Online): 2455-7196*
*http://dx.doi.org/10.19101/TIS.2017.25001*

# Application of chaos theory in data security-a survey

**Sheela S.[1*] and S. V. Sathyanarayana[2]**
Assistant Professor, Department of Electronics and Communication Engineering, JNNCE, Shimoga, Karnataka, India[1]
Professor, Department of Electronics and Communication Engineering, JNNCE, Shimoga, Karnataka, India[2]



## Abstract
***In cryptography key sequence generation is one of the important areas. Earlier pseudo random number generators were used as key sequence in stream cipher. After the evolution of chaotic systems, it was found that properties of chaotic systems are more superior to pseudo random number generators. In this context, we have tried to explore the basic theoretical background of chaotic systems, their types and properties in this paper. Along with chaotic systems, sequence generation using chaotic systems and the application of sequences in various image encryption methods is also discussed. Finally, a suitable key sequence generation using chaotic system is proposed.***

## Keywords
***Chaotic functions, Sequence generation, Image encryption, Chaotic systems.***

## 1.Introduction
The fascinating developments in digital image processing and network communications during the past decade have created a great demand for real-time secure image transmission over the Internet and through wireless networks. To meet this challenge, a variety of encryption schemes have been proposed. Among them, Chaos based algorithms have shown some exceptionally good properties in many concerned aspects regarding security, complexity, speed, computing power and computational overhead, etc. Due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels, traditional encryption algorithms are not suitable for practical image encryption especially under the scenario of on-line communications [1]. In this direction, chaos based Stream Cipher Systems (SCS) are generally used as an alternative technique for image encryption. As we know that the random numbers are widely used in applications like cryptosystem to generate key sequences to be used in a Stream Cipher Systems (SCS). In terms of algorithmic complexity, a sequence is said to be random if the smallest program needed to produce random sequence is approximately equal to the size of the sequence itself. Such a sequence is called “maximally complex”. But, no finite algorithm can produce a maximally complex sequence of infinite length.

*Author for correspondence

A consequence is that truly random sequences cannot be computed [2]. Hence Pseudo Random Number Generators (PRNGs) are used.

Chaos is one of the most important theories that used to create a random sequence that firstly used in the computer by Edward Lorenz in 1963. In a cryptosystem, the secrecy should be in the key not in encryption or decryption algorithm. Though there are many encryption algorithms and schemes like AES, DES, Chaos, Arnold based method and so on for digital image data, chaos is of the great interesting for researchers to construct a good cryptosystem. Because there are numerous interesting properties of chaotic systems, such as sensitive to initial conditions, system parameter, ergodicity and mixing(stretching and folding) which is analogous to the confusion and diffusion property of good cryptosystem. Also chaotic sequences are non-periodic, wide band, more difficult to predict, reconstruct and characterize than periodic carriers [3]. Though chaotic sequences are random like but they are produced by deterministic systems and hence it can be reproduced [4].

Since image is one of the major data that is transmitted over the communication channel, designing a secure image encryption algorithm is one of the important tasks. The main obstacle in designing image encryption algorithms is that it is rather difficult to swiftly shuffle and diffuse data by

traditional means of cryptology. In this respect, chaos-based algorithms have shown their superior performance [1]. It has been proved that in many aspects chaotic maps have analogous but different characteristics as compared with conventional encryption algorithms [5]. Classical encryption algorithms are sensitive to keys, while chaotic maps are sensitive to initial conditions and parameters; cryptographic algorithms shuffle and diffuse data by rounds of encryption, while chaotic maps spread the initial region over the entire phase space via iterations. The main difference between these two techniques is that encryption operations are defined on finite sets, while chaos in a strict mathematical sense is defined on real numbers [1]. The Chaotic real sequences need to be converted to binary before using them in Encryption. In this context, this paper reviews the various research works in the area of chaotic key sequence generation and presents a comparative study on chaos based PRNGs and chaos based image encryption algorithms.

The rest of the paper is organized as follows. Section 2 consists of chaos theory, types and properties of chaos. Section 3 deals with sequence generation using chaotic systems and comparison of chaotic sequence generators. Section 4 consists of the survey of chaotic cryptosystems and their application in image encryption. Section 5 deals with a comparative study of various image encryption methods discussed in section 4. Section 6 deals with concluding remarks.

## 2.CHAOS

Chaos is an aperiodic long-term behavior in a deterministic system that exhibits sensitive dependence on initial conditions. “Aperiodic long-term behavior” means that the systems trajectory in phase space does not settle down to any fixed points (steady state), periodic orbits, or quasi-periodic solutions as time tends to infinity. “Deterministic” systems can have no stochastic (meaning probabilistic) parameters. The irregular behavior of chaotic systems arises from intrinsic nonlinearities. “Sensitive dependence on initial conditions” requires that trajectories originating from very nearly identical initial conditions will diverge exponentially quickly [6].

To understand the concept of chaos first we should know some basic knowledge of dynamic systems. Time is essential in the scientific field of chaos (also called chaotic dynamics) in which one is interested in the movement, variation in the position, or orbits of points, x(t), in an n-dimensional Euclidian space $\Re^n$. Space need not have a discrete set of dimensions. If the medium under consideration is a continuum, one needs to study the dynamics of a system of partial differential equations describing the properties of variables $u_i(x, t)$, i = 1, 2, ….., as functions of $x \in \Re^n$ and time t. This extends the realm of chaos to a broader scientific field, which may be called complexity as it examines and discusses the evolution of nonlinear systems in both time and space [6].

Complexity, however, does not occur only in time but also in space. Chaotic orbits that are often attracted by spatial structures of extreme geometric complexity are called strange attractors. These structures are characterized by the property of self-similarity under scaling, as they exhibit detailed features, similar to their original form, at all scales of magnification. It becomes evident that geometry plays an important role in the study of dynamics. However, in the study of chaos there is the complementary between geometry and dynamics more evidently manifest than in the concept of fractals [6].

“Fractal” is a word used to describe static objects, or collections of points in an n-dimensional Euclidian space, which are self-similar down to their finest detail and have dimension $D \leq n$, which often takes fractional, i.e., non-integer values. It is important to point out that chaos and fractals rest on a firm theoretical foundation, encompassing several mathematical topics: analysis, differential equations, topology, differential geometry, number theory, measure theory, discrete mathematics, and the geometry of fractal sets [6].

One more concept related to chaos is the local bifurcations or qualitative change of the dynamics, connected with the destabilization of equilibria or periodic states. Let us consider discrete time dynamical models, since they are easier to analyze and contain all the important features of systems working in continuous time [6].

Having these basics discussed, some survey related to chaos theory is presented below:

**Paper 1 [2] “Random number generators are chaotic”, 1989.** Herring et al. have mentioned that in 1951, Lehmer was proposed a pseudo-random number generator algorithm and it has become the defacto standard pseudo-random number generator. Through statistical theory approach, in 1966 Martin

has proved that a random sequence must pass all of a countable infinity of statistical tests. It was observed that the chaotic system behavior is similar to the random number generator behavior. Hence the study of highly unstable nonlinear dynamical systems that is chaotic systems has emerged as an area of major interest and applicability across the mathematical, physical and social sciences, particularly in the mathematical understanding of complex systems. An important insight that has become widely recognized is that deterministic systems can give rise to chaotic behavior.

**Paper 2 [7] "In the wake of chaos: Unpredictable order in dynamical systems", 1994.** Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions, an effect which is popularly referred to as the butterfly effect. It is the qualitative study of unstable aperiodic behavior in deterministic nonlinear dynamical systems.

**Paper 3 [8] "A prime case of chaos", 1999.** Cipra et al. has mentioned that chaos got prominence in 1980's stemmed from the realization that disorderly systems tends to be disorderly in an orderly fashion, that underlying order present in the chaos phenomena is can be studied by using both mathematics analysis and computer simulations. Mathematically nonlinearities present in the dynamical systems leads to chaos, but all nonlinear dynamical systems are not chaotic.

**Paper 4 [9] "Synchronization in chaotic systems", 1990.** Pecora et al. has shown that how two chaotic systems can be synchronized using a common linking signal. To implement this concept, Lorenz and Rossler chaotic systems were used. The systems were divided into subsystems and then it is demonstrated that for these subsystems when the Lyapunov exponents are all having negative sign then the systems will synchronize. Synchronization means that trajectories of both the systems will converge to the same value and they will remain in step accordance with each other.

**Paper 5 [5] "Chaos-based cryptography: a brief overview", 2001.** Chaotic systems are characterized by sensitive dependence on initial conditions, similarity to random behavior, and continuous broad-band power spectrum. In digital communication many of the functional blocks like compression, encryption, modulation and others will use chaos. Since conventional cryptographic algorithms are weak, chaotic cryptography is preferably stronger. An important difference between chaos and cryptography is that encryption transformations are defined on finite sets, while chaos has meaning only on real numbers.

**Paper 6 [10] "Chaotic sequences to improve the performance of evolutionary algorithms", 2003.** Caponetto et al. has mentioned that chaotic systems can be characterized as signals with a broad-band spectrum that depend strongly on the initial conditions with respect to time-series prospective and analytically using Lyapunov exponents. The Lyapunov exponent is given by equation (1). If the value of h > 1 then the attractor of the dynamic system is chaotic.

$$h = \lim_{t \to \infty} \frac{1}{t} \left( \frac{\delta x(t)}{\delta x(0)} \right) \quad (1)$$

In this paper, numerous examples and their statistical tests have been conducted and showed an improvement of the Evolutionary Algorithms when chaotic sequences were used instead of random processes.

**Paper 7 [11] "Introduction to chaos in deterministic systems", 2003.** Gershenson et al. mentions that there are certain deterministic systems where their behavior turns out to be non-predictable: not because of lack of determinism, but because the complexity of the dynamics requires a precision that is unable to be computed. Those systems will produce random sequences which are chaos in nature. Chaos is extremely sensitive to initial conditions because there is an exponential divergence of the trajectories of the system which can be measured with Lyapunov exponents.

**Paper 8 [12] "Image encryption scheme with key sequences based on Chaotic functions", 2014.** Based on the definition of chaotic systems, several conclusions about the characteristics of chaos is done. First, that the system is dynamical means that it changes over time. Second, that the behavior of the system is aperiodic and unstable means that it does not repeat itself. Third, because the system is nonlinear, it is sensitive to initial conditions. Fourth, because the system is deterministic, chaotic behavior is not random even though its aperiodicity and unpredictability may make it appears to be so. The natures of chaotic signals can be very helpful in enhancing the security in Cryptographic applications.

Having dealt with the literature related to chaos theory, it will be essential to discuss the various types

of chaotic functions and is presented in the next subsection.

**A.Types of chaotic functions**

The different types chaotic functions available are as follows:

**1)Logistic map:** The most widely used one dimensional chaotic map is Logistic map and is given in three different equations are as shown

**Logistic map 1 [4], [10], [11], [13]:**

$$x_{n+1} = r x_n \left(1 - x_n\right) \tag{2}$$

where $x_n \in [0, 1]$, $r \in [0, 4]$, n = 1, 2, … and r is the bifurcation parameter or control parameter which indicates the "fertility" or "growth rate". The system will be in chaotic state under the condition that $3.99465 \le r \le 4$. The chaotic codes generated using equation (2) is found to be superior to pseudo-random codes such as Gold code in several key aspects such as security, bit error rate, code generation speed and the number of possible code sequences [13].

**Logistic map 2 [4], [13]:**

$$x_{n+1} = \left(1 - 2x_n^2\right) \tag{3}$$

Where $x_n \in [-1; 1]$. In the spread spectrum communication, the broad band, noise like nature of this improved logistic map offers several advantages. Chaotic sequences are uncorrelated when their initial values are different, so in chaotic spread spectrum systems, a user is assigned an initial value [13].

**Logistic map 3 [13]:**

$$x_{n+1} = \left(2x_n^2 - 1\right) \tag{4}$$

**2)Tent map:**

**Tent Map 1 [10], [13]:**

$$x_{n+1} = \begin{cases} x_n / 0.7 & \text{for } x_n \le 0.7 \\ \left(1 - x_n\right) / 0.3 & \text{otherwise} \end{cases} \tag{5}$$

This system is employed to generate sequences with different parameter sets to carry different binary bit streams which lead to good discrimination between each two adjacent bit streams. The signals generated from this system are noise like, extremely sensitive to initial conditions and have spread and flat spectrum in the frequency domain. Therefore it is advantageous to carry messages in communication system [13].

**Tent Map 2 [14]:**

$$x_{n+1} = 1 - \left|1 - 2x_n\right| \text{ where } x_n \in [0,1] \tag{6}$$

**Tent Map 3 [15]:**

$$x_{n+1} = \begin{cases} \dfrac{x_n}{\alpha} & \text{for } x_n = [0, \alpha) \\ \dfrac{1 - x_n}{1 - \alpha} & \text{for } x_n = (\alpha, 1] \end{cases} \tag{7}$$

where $x_n$ is the initial condition and α is the system parameter which determines position of the top of the tent in the interval [0,1].

**3)Sinusoidal Map:**

**Sinusoidal map 1 [10]:**

$$x_{n+1} = a x_n^2 \sin\left(\pi x_n\right) \text{ where } a = 2.3 \tag{8}$$

**Sinusoidal map 2 [13]:**

$$x_{n+1} = a x_n^2 \sin\left(x_n\right) \text{ where } a = 2.3 \tag{9}$$

**4)Gaussian map [10], [13]:**

$$x_{n+1} = \begin{cases} 0 & \text{for } x_n = 0 \\ \dfrac{1}{x_n} \bmod 1 & \text{for } x_n \in (0,1) \end{cases} \tag{10}$$

**5)Lozi map [10], [13]:**

$$\begin{aligned} x_{n+1} &= y_n + 1 - a\left|x_k\right| \\ y_{n+1} &= b x_k \text{ where } a = 1.7 \ \& \ b = 0.5 \end{aligned} \tag{11}$$

**6)Chuas generator [10], [13]:**

$$\begin{aligned} \dot{x} &= \alpha\left(y - m_1 x - 0.5\left(m_0 - m_1\right)\left[\left|x+1\right| - \left|x-1\right|\right]\right) \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y - \gamma z \end{aligned} \tag{12}$$

where α = 9, β = 14.286, γ = 0, $m_0$ = -1/7, $m_1$ = -2/7. The Chua generator was the first Chaos generator obtained from a real or physic system. It is an electronic circuit capable of generating Chaos [16].

**7)Lorenz map [13], [16], [17], [18], [19]:**

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - xz - y \\ \dot{z} &= xy - bz \end{aligned} \tag{13}$$

Where, σ, r and b are parameters. When σ = 10, r = 28, b = 8/3, the system is chaotic. Lorenz system is used to generate continuous signal and is converted to binary sequences [13].

**8)Lu system [13]:**

$$\begin{aligned}\dot{x} &= (25\alpha+10)(y-x)\\ \dot{y} &= (28-35\alpha)x+(29\alpha-1)y-xz\\ \dot{z} &= xy-((8+\alpha)/3)z\end{aligned} \quad (14)$$

The Lu system is a unified chaotic system and includes both Lorenz and Chen systems. If α = 0, equation (14) becomes original Lorenz system, if α = 1, it becomes original Chen system and if α = 0.8, it becomes critical system. Moreover system given in equation (14) is always chaotic in the whole interval α ∈ [0; 1] [13].

**9)Rossler generator [16]:**

$$\begin{aligned}\dot{x} &= -y - z\\ \dot{y} &= x + ay\\ \dot{z} &= b + z(x - c)\end{aligned} \quad (15)$$

where a, b, c are the control parameters. Author has proposed the values a = b = 0.3 and c = 35 to generate the chaotic behavior by varying the parameter 'c'. In the Rssler system, the variable z presents the lowest autocorrelation function, but in the case of Lorenz it is the y signal and for the Chua generator it is the x signal [16].

**10)Chebyshev map [14]:**

$$x_{n+1} = \cos\left(k\cos^{-1}x_n\right) \text{ where } k \geq 2, x_n \in [0,1] \quad (16)$$

**11)Bernoulli map:**

**Bernoulli map 1 [14]:**

$$x_{n+1} = 2x_n \bmod 1 \text{ where } x_n \in [0,1] \quad (17)$$

**Bernoulli map 2 [20]:**

$$x_{k+1} = \begin{cases} rx_k + 0.5; x_k < 0 \\ rx_k - 0.5; x_k \geq 0 \end{cases} \quad (18)$$

where -0.5 < x < 0.5 and 1.2 < r < 2

**12)Cubic Map equation [20]:**

$$x_{k+1} = 4x_k^3 - 3x_k \ \ where \ \ -1 < x < 1 \quad (19)$$

**13)Quadratic Map equation [20]:**

$$x_{k+1} = r - 4x_k^2 \quad (20)$$
$$where \ \ -0.5 < x < 0.5 \ \& \ 0.36 < r < 0.5$$

**14)Baker map [19]:** Let X = $[0, 1]^2$ = [0,1]*[0,1] be the unit square. Consider the following two dimensional map $F : X \to X$ is given by equation (21).

$$F(x,y) = \begin{cases} \left(2x, \frac{y}{2}\right) & if \ \ 0 \leq x < \frac{1}{2} \\ \left(2x-1, \frac{y+1}{2}\right) & if \ \ \frac{1}{2} \leq x < 1 \end{cases} \quad (21)$$

Geometrically, F is obtained by cutting $[0,1]^2$ into two vertical rectangles $R_0$ = [0,1/2][0,1] and $R_1$ = [1/2,1][0,1], stretching and compressing each to obtain an interval of horizontal width 1 and vertical height 1/2 and then putting them on top of each other. The name bakers map comes because these mimic the movement made by a baker to prepare the bread dough.

**15)4D Chaotic system or Hyper-Chaos system [21], [22]:**

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = -x_1x_3 + dx_1 + cx_2 - x_4 \\ \dot{x}_3 = x_1x_2 - bx_3 \\ \dot{x}_4 = x_1 + k \end{cases} \quad (22)$$

where, when a = 36, b = 3, c = 28, d = -16, and k ∈ [-0.7,0.7] the system will be in chaos.

**16)One-parameter families of rational order chaotic maps [23] :**

$$x_{n+1}(x,\alpha) = \frac{\alpha^2\left(T_N\left(\sqrt{x}\right)\right)^2}{1+\left(\alpha^2-1\right)\left(T_N\left(\sqrt{x}\right)\right)^2} \quad (23)$$

where α is the control parameter and $T_N(x)$ is the Chebyshev polynomial of first kind with degree N. N is a integer greater than 1.

Conjugate map of equation (23) is

$$\tilde{x}_{n+1}(x,\alpha) = \frac{1}{\alpha^2}\tan^2\left(N\arctan\sqrt{x_n}\right) \quad (24)$$

**17)Arnold cat map [24]:** The classical Arnold cat map is a two-dimensional invertible chaotic map defined by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \quad (25)$$

**18)Generalized cat map [24]:** In permutation process of image encryption scheme, it is more common to use the generalized cat map as following:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ 1 & 1+pq \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad (26)$$

Where N represents the number of rows or columns.

**19)3D Cat Map:** It can be obtained from generalized 2D cat map, more details can be found in [1]. A simple 3D cat map can be defined as follows

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 5 \\ 2 & 1 & 4 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1 \qquad (27)$$

The various types of chaotic functions are discussed. What follows are the properties of chaos functions. Properties of Logistic map (equation (2)) is dealt in detail in the next subsection.

**B.Properties of chaos**

Chaotic systems are very much suitable for data message encryption because they have several good properties. According to [25], (a) chaotic motion is neither periodic nor convergent, and the domain is limited. With time passing, the points of the movement trace traverse all over domain, namely the ergodicity of the chaotic orbit; (b) the flexing and collapsing are carried continually through the limited domain. Therefore the outputs of chaotic systems are very irregular, similar to the random noise; (c) Because chaotic systems are extremely sensitive to their initial conditions, the movement of any two closed points can be separated in an exponent rule. The long-term movement trace of systems cannot be forecasted. These dynamics characteristics cause chaotic sequences to be wide band, pseudo-random, and unmasked hardly.

To understand the properties of chaos, let us consider the analysis of a simple one dimensional logistic map function $x_{n+1} = rx_n(1-x_n)$. The sensitivity of this chaotic function is based on bifurcation parameter r and initial condition $x_o$. Bifurcation is a period doubling, a change from an N-point attractor to a 2N-point attractor, which occurs when the control parameter is changed. *Figure 1* shows the bifurcation diagram of logistic map [3]. In this Figure, initially it shows that the attracting set consists of single point that bifurcates into two points at r = 3. When r is between 3 and 3.44949, from almost all initial conditions the system will approach permanent oscillations between two values. These two values are dependent on r. With r between 3.44949 and 3.54409, from almost all initial conditions the system will approach permanent oscillations among four values. With r increasing beyond 3.54409, from almost all initial conditions the system will approach oscillations among 8 values, then 16, 32, etc. The lengths of the parameter intervals which yield oscillations of a given length decrease rapidly. When r is between 3.56995 and 4, from almost all initial conditions there is no oscillation of finite period. Slight variations in the initial condition yield dramatically different results over time, a prime characteristic of chaos.

Now Consider r = 0.25, 0.5 and 0.75 with initial value $x_o$ = 0.5 and for 10 iterations a plot of number of iterations versus magnitude (x) is plotted in *Figure 2(a)*. Consider r = 1.25, 2 and 2.75 with initial value $x_o$ = 0.5 and for 25 iterations, a plot of number of iterations versus magnitude (x) is plotted in *Figure 2(b)*. When r = 3.2 (r > 3), the system is called a twopoint attractor as it settles down between two points shown in *Figure 2(c)*. When r = 3.54, the system settles down between four points and hence called a four-point attractor shown in *Figure 2*(d).

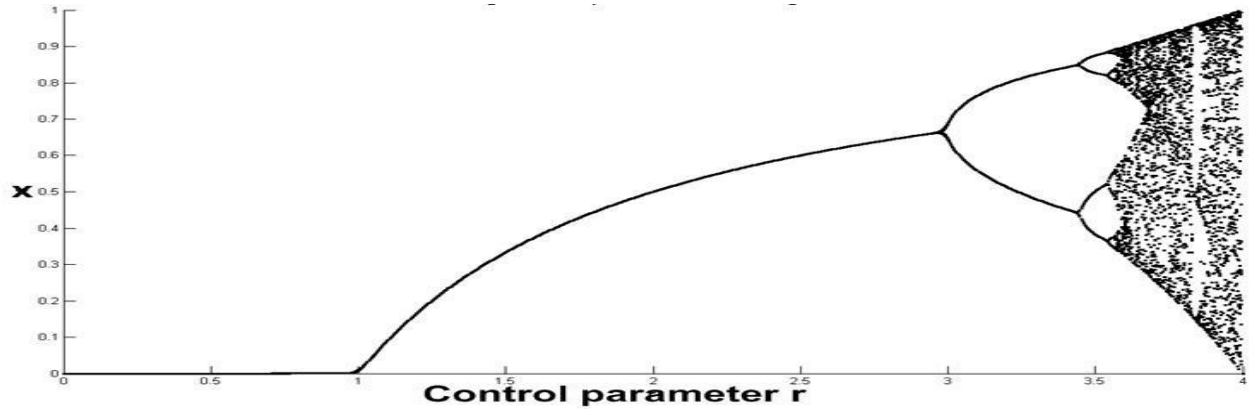


**Figure 1** First logistic map bifurcation diagram

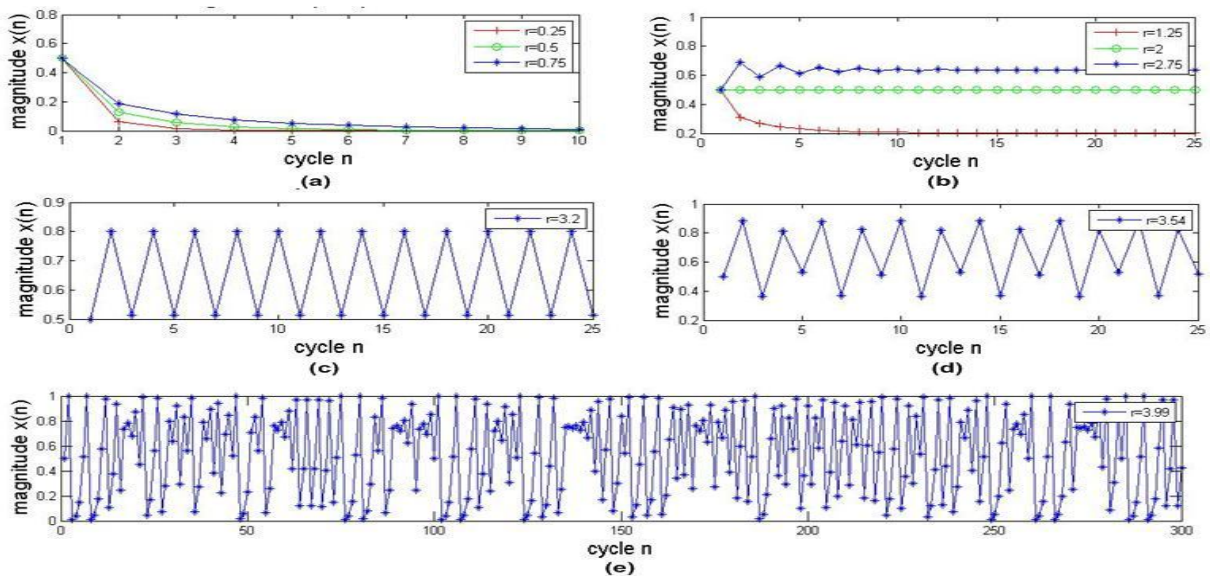


**Figure 2** Logistic map analysis for x0 = 0.5 (a) r = 0.25, 0.5 and 0.75 (b) r = 1.25, 2 and 2.75 (c) r = 3.2 (d) r = 3.54 (e) r = 3.99

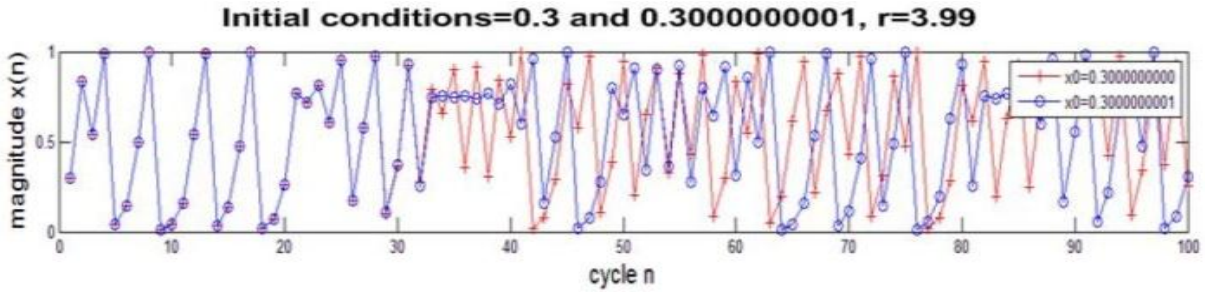


**Figure 3** Sensitivity of logistic map to initial conditions

When r = 3.99, it results in an N-point attractor and is shown in *Figure 2(e).* Sensitivity of logistic map to initial conditions is shown in the *Figure 3*, that is, a small change in initial conditions yield dramatically different results over time. As seen from the *Figure 3*, up to 33 iterations, both the initial conditions result in same values. Hence the first 100 points of the chaotic iteration curve are abnegated in order to avoid the harmful effect of transitional procedure [26].

## 3.Sequence generation using chaotic systems

A Random Number Generator (RNG) is a most crucial part in modern cryptographic systems, communication systems, statistical simulation systems and many others. Most importantly, among all the applications, RNGs are used mainly in cryptography to generate cryptographic keys. Pseudo random number generators are deterministic processes which generate a series of outputs from an initial seed state.

**Paper 9 [15] "A Random Bit Generator Using Chaotic Maps", 2010.** The proposed algorithm is named as Cross-coupled Chaotic Tent Map Based Bit Generator(CCCBG), uses two one-dimensional skew tent maps (equation (7)) which are piecewise linear chaotic maps to generate sequences. They are cross coupled by feeding output of one map as input (initial condition) for other and vice versa. The system parameter for the both chaotic maps is kept same and is in the chaotic regime. The CCCBG produces the binary sequence from the output ($x_{i+1}$; $y_{i+1}$) by comparing $x_{i+1}$ and $y_{i+1}$, if $x_{i+1} < y_{i+1}$ then the binary value is '0' else '1'. The randomness of the generated binary sequences is tested using four basic statistical tests that are monobit test, serial test, autocorrelation test and Poker test. As well as NIST statistical test suite is also used.

**Paper 10 [20] "Generation of Large Set of Binary Sequences Derived from Chaotic Functions with Large Linear Complexity and Good Cross Correlation Properties", 2010.**
Mandi et al. has considered the 6 different chaotic maps governed by equations (2), (3), (5), (19), (20) and (18) to generate binary sequences. Each chaotic map is considered separately to generate sequences using proposed algorithm. Chaotic map is used to generate infinite chaotic sequence $x_i$, i = 0, 1, 2, …. The proposed scheme is as follows: Consider the element $x_k$ from the sequence $x_i$ and then multiply by a large integer n and is either a power of decimal radix 10 or binary radix 2. In either case the fraction part is discarded. The large integer part $Q_k$ is obtained. It is then reduced to small integer $y_k$ modulo m and m < n. Generally m is chosen to be some power of 10 or 2. Then the integer $y_k$ is represented in binary value $b_k$ of v number of bits. Thus proposed model is used to derive discrete sequence $y_k$, where $0 \le y_k < m$ or binary $b_k$, from the chaotic sequence $x_k$. The scheme is governed by the equation $y_k = \left\lfloor \left\lfloor (x_k) n \right\rfloor \right\rfloor \bmod m$ where m < n and $(x_k)*n = Q_k$. The randomness of the generated binary sequence is tested based on the cross-correlation property and linear complexity.

**Paper 11 [23] "A novel dynamic model of pseudo random number generator", 2011.** In this paper, Behnia et al. has mentioned that Logistic map has a very simple structure and it was first proposed as pseudo random number generator by von Neumann in 1947. After few years it came to know that as Logistic map generates sequences with extremely short period, it is not a good pseudo random number generator. In the proposed algorithm is as follows: Generate sequences by using chaotic map given in equation (24) with x and α as secrete key. First hundred sequences have been avoided for transient effect. After that for every iteration of map, check whether K (a temporary variable) equal to 16. If 'no' compute the sequence using equation $B = \left\lfloor x \times 2^{32} \right\rfloor \bmod 2^{32}$ else compute the sequence using equation $B = \left\lfloor x \times 2^{32} \right\rfloor \bmod 2^{16}$. Then output the generated bits. Now check whether i ≤ n where n is the number of bit streams generated by the system. If 'yes' repeat the previous steps for next iteration else stop. Several tests like DIEHARD, NIST statistical test suite and ENT test suite are used to examine the randomness of the presented algorithm. ENT test is a collective term for the three tests namely Entropy, Chi-square, and Serial correlation coefficient (SCC) test.

**Paper 12 [12] "Image encryption scheme with key sequences based on Chaotic functions", 2014.** Shruthi et al. has used Logistic map equation (2) to generate the key sequence. The proposed algorithm is as follows: Generate the chaotic real sequence from the equation (2). To avoid transient effect discard first 100 chaotic real values. Convert the next chaotic sequence into k binary bits using threshold function defined by equation (28) where $x \in (0, 1)$.

$$T(x) = \begin{cases} 00....00 \ \ for \ \ 0 \le x < \frac{1}{2^k} \\ 00....00 \ \ for \ \ \frac{1}{2^k} \le x < \frac{2}{2^k} \\ \vdots \\ 11....11 \ \ for \ \ \frac{2^k - 1}{2^k} \le x < 1 \end{cases} \quad (28)$$

Next the k binary bits drive LFSR to generate binary key sequences of length 2k−1. The randomness is tested using NIST statistical test suite.

**A. Comparison of various existing PRNGS**
Based on the literature survey of PRNGs dealt so far, what follows is to discuss about the randomness of the sequences generated in the above PRNGs. The discussion is as follows:

In [15], Narendra et al. has proposed PRNG based on cross coupling of two chaotic tent maps and the following things has been observed: (a) By knowing the system parameter and initial condition of one of the map is not sufficient to identify the behavior of proposed CCCBG. (b) With the parameter α in the range [0.49, 0.5] and initial conditions in the range [0, 1], the proposed algorithm produces better random sequence compared to other values. (c) The monobit, serial and Poker tests were passed by CCCBG as the calculated value of $\chi^2$ for the given α is less compared to the critical value of $\chi^2$ at α = 0.5. (d) The CCCBG has passed autocorrelation test also because obtained value of Z is within the range ±1.96. (e) The NIST test results are tabulated in *Table 1* and CCCBG has passed all the conducted tests in the NIST suite. From the above points it can be observed that the proposed algorithm can be used for cryptographic applications.

In [20], Mandi et al. has proposed a PRNG model using chaotic systems. Here 6 different chaotic maps are considered and they are two logistic maps, tent

map, cube map, quadratic and Bernoulli map. Pseudo random sequences are generated by using these chaotic maps separately from the proposed PRNG. The randomness of the generated sequences was examined based on the cross correlation property and linear complexity and compared with the Gold sequences generated in [27]. It was found that compared to Gold sequence of length 15, from the proposed model it is possible to obtain large set of binary sequences of length 15 with good cross correlation value and large linear complexity. Hence it can be used for cryptographic applications.

In [23], Behnia et al. has proposed chaotic system using one parameter rational order chaotic map to generate pseudo random sequences. The generated sequences have been tested using DIEHARD test suite, NIST test suite and ENT test suite. In DIEHARD test suite, 21 different statistical tests were conducted and the generated sequence has passed all the tests. The NIST test results are tabulated in Table I and the sequence has passed all the conducted tests. In ENT test suite, there were 3 tests namely Entropy, Chi-square and SCC and the sequence has passed all these tests. From the key space analysis it was found that the key space size is of $10^{46} \approx 2^{152}$, which leads to resist all kinds of brute force attacks. The author has also proved that sequence generated using proposed chaotic system is better compared to sequence generated using Logistic map alone. Hence the sequence generated is highly random with large key space and can be used in many cryptographic applications.

**Table 1** Comparison of result of existing PRNGs based on NIST statistical test suite

| S. NO | Test name | P Value of papers | | |
|---|---|---|---|---|
| | | [15] | [23] | [12] |
| 1 | Approximate Entropy Test | 0.113169 | 0.616827 | 1.0000 |
| 2 | Frequency Test within Block | 0.571881 | 0.500934 | 1.0000 |
| 3 | Cumulative (forward) Sum Test | 0.355713 | 0.343168 | 1.0000 |
| 4 | Cumulative (reverse) Sum Test | 0.850139 | 0.888137 | 1.0000 |
| 5 | DFT Test | 0.524923 | 0.295498 | 0.0000 |
| 6 | Frequency Test | 0.556614 | 0.444867 | 1.0000 |
| 7 | Lempel-Ziv Compression Test | 1.000000 | 0.178278 | - |
| 8 | Linear Complexity Test | 0.274193 | 0.416273 | 1.0000 |
| 9 | Longest Runs of ones in a Block Test | 0.706404 | 0.6449420 | 1.0000 |
| 10 | Non-overlapping Template Matching Test | Success | 0.976927 | Success |
| 11 | Overlapping Template Matching Test | 0.048349 | - | 1.0000 |
| 12 | Rank Test | 0.994872 | 0.517363 | 0.0000 |
| 13 | Run Test | 0.008225 | 0.500617 | 1.0000 |
| 14 | Serial Test | 0.532974 | 0.798665 | 1.0000 |
| 15 | Universal | - | 0.802942 | 1.0000 |
| 16 | Random Excursions Test | - | Success | Success |
| 17 | Random Excursions Variant Test | - | Success | Success |

In [12], Shruthi et al. has proposed PRNG to generate chaotic binary sequence using LFSR. The logistic map has been used to generate the random sequences. The randomness of the generated sequence is tested using NIST test suite and the results are tabulated in *Table 1*. 15 tests were conducted. Out of that 13 has been passed and failed in Rank and DFT test as the obtained P-values are 0.0000. In this paper authors have made an attempt to analyze the property of sequences generated by using simple chaotic map that is logistic map, and found that the sequences generated are not highly random and provides less security. From this paper it indicates that generating key sequences using logistic chaotic maps may not provide high level of security in cryptographic applications.

From the above discussion it can be observed that security analysis of the proposed PRNGs has been done for only few PRNG algorithms and also the time complexity of algorithms is not mentioned. So, construction of new PRNG algorithms using other

chaotic maps and analyzing their security analysis as well as time complexity can be taken as further research problem.

## 4.Chaotic cryptosystems

Cryptosystem mainly consists of the following three objects: block-encryption algorithms, pseudo-random number generators and cryptographic hash functions. Block encryption algorithms transform a relatively small string of size 64 or 128 bits to a string of the same length by using a secret key. A pseudo-random number generator is a deterministic method uses a small set of "random numbers called the seed to produce a larger set of random looking numbers called pseudo-random numbers. A one-way function H known as hash function operates on an arbitrary-length message M and returns a fixed-length value, h (h = H(M)), such that given M it is easy to compute h, given h it is hard to compute M and it is very difficult to find same hash value for two different inputs [5]

Two general principles that are necessary for practical encryption algorithms are diffusion and confusion. Diffusion means spreading out of the influence of a single plain text digit over many ciphers text digits so as to hide the statistical structure of the plain text. Whereas, confusion means complicate the dependence of the cipher text statistics on the plain text statistics. This diffusion and confusion can be achieved by a robust key sequence. To generate such key sequence chaos based PRNGs are used as the dynamic properties of chaos like aperiodic, random, highly sensitive to initial condition, large bandwidth and low power spectrum density has made its use to build an excellent cryptosystem. Hence it is known as chaotic cryptosystems.

The information transferred through the communication channel is not only text but also audio, image, video and other multimedia data. Since images are widely used for data transmission, the security for image data is very important. One of the ways to secure the data is through cryptography. Hence image encryption is a field that has drawn much attention in the latest years. Due to numerous interesting properties of chaos, they are widely used in most of the image encryption systems. It is known that the image data is very large than the text data, so the conventional encryption is difficult. So chaos based image encryption is widely used.

### A. Survey of existing chaos based image encryption

The chaos-based image cryptosystem mainly consists of two stages. The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels by permutation matrix developed using chaotic map and the image becomes unrecognizable. In the diffusion stage, the pixel values are modified sequentially. So the initial conditions and control parameter values serves as secret key. The confusion and diffusion stages are repeated until satisfactory level of security is obtained. Hence the inherent property of randomness present in chaotic maps makes it more suitable for image encryption [19]. The general architecture of chaos based image encryption is as shown in the *Figure 4.*

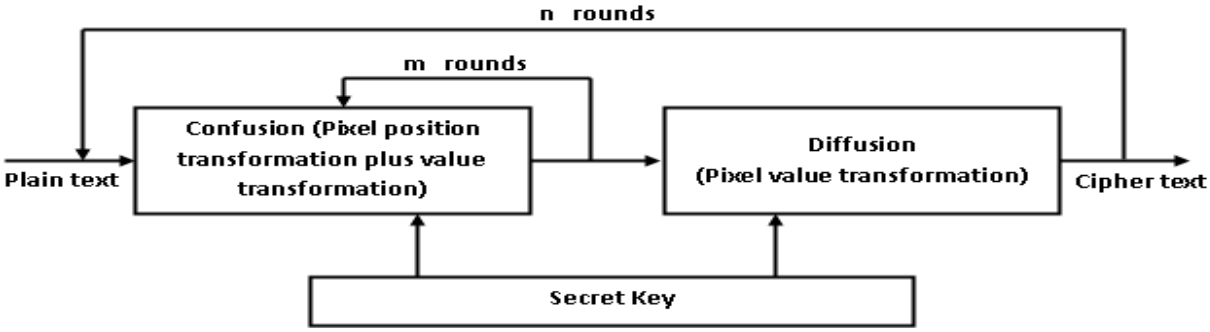


**Figure 4** Architecture of chaos based image cryptosystem

A good encryption scheme should resist all kinds of known attacks. At present, the main attacks aimed at the chaotic encryption systems include key space analysis, statistical analysis, known-plain-text attack, cipher-text only attack and so on. In this context brief survey of some of the existing chaos based image encryption methods are discussed here.

**Paper 13 [14] "An enhanced chaos based image encryption algorithm", 2006.** In this paper, before applying encryption algorithm the binary image is decomposed into eight bitplanes and encryption will be done for each bitplane Bi separately and encrypted images are combined. The proposed algorithm consists of two steps: permutation and substitution. In the proposed algorithm three chaotic systems with corresponding initial values is considered. Original image is decomposed into eight bitplanes. Eight ergodic matrix P is constructed by optimized chaotic sequences generated by one of the chaotic system, then permute bitplanes with ergodic matrices. Generate two cross-sampling binary chaotic sequences for every bitplane. Then construct substitution matrices and perform substitution. Combine the bitplanes and get the encrypted image. Author has analyzed and done simulation tests and found that the algorithm has been effective and largely secure.

**Paper 14 [25] "An image encryption scheme based on chaotic systems", 2006.** Author has used Logistic map in equation (2) for encryption process. The encryption scheme is composed of two chaotic systems. One creates a binary stream and the other creates a permutation matrix P. First, generate the chaotic sequence using subkey k1 for the first chaotic system and then transform the sequence into bit stream by a threshold function (equation (28)). Then the pixel values of the plain image are modified randomly using the binary stream by the traditional stream ciphers technology, namely bit-wise XOR operation. Second, construct a permutation matrix P using the subkey k2 for the second chaotic system. Then the modified image in first process is permuted by matrix P to get the encrypted image. The proposed algorithm provides a high security against different types of attacks like brute force attack and statistical attacks.

**Paper 15 [21] "A new image encryption algorithm based on hyper-chaos", 2008.** Gao et al. have mentioned that image encryption using one dimensional chaotic map is not secure. The author has been investigated that as the hyper-chaos is having more than one positive Lyapunov exponent, and more complex dynamical characteristics than one dimensional chaos, it is safer than chaos in security algorithm. It is defined by the equation (22). In the proposed algorithm, encryption is done in two steps. First the total shuffling of image is done by chaotic Logistic map. Second, encryption using hyper chaos system is done to change the grey values of the shuffled-image. For total shuffling permutation matrix P is generated using chaotic sequences of Logistic equation (2) with r = 4. For row shuffling, the chaotic sequences (with initial value $x_o$) are converted to integers in the range 0 to M – 1 (Number of rows) by the function $l = \mathrm{mod}\left(x_0 \times 10^{14}, M\right)$ and row shuffling of the image is done. Next for column shuffling, the chaotic sequences (with new initial value for $x_o$) are converted to integers in the range 0 to N – 1 (Number of columns) by the function $l = \mathrm{mod}\left(x_0 \times 10^{14}, N\right)$. Is shown that the system is highly sensitive to keys, has a large key space, low correlation coefficients close to ideal values hence provides a high security against brute force attack. Is shown that the system is highly sensitive to keys, has a large key space, low correlation coefficients close to ideal values hence provides a high security against brute force attack.

**Paper 16 [28] "An image encryption scheme with a pseudo random permutation based on chaotic maps", 2010.** In the proposed method logistic map is used. First small permutation matrices are constructed by the sequence of chaotic logistic map. The initial value of logistic map and size of small permutation matrices is considered as key for the algorithm. Using these small permutation matrices, a large permutation matrix is constructed. Then permute a plain text image with the constructed large permutation matrix. Finally mask the permuted image using permutation mask. Proposed algorithm provides reasonable security against statistical cryptanalysis.

**Paper 17 [3] "Image Encryption Algorithm Based on Logistic Map and Pixel Mapping Table", 2011.** Al-Najjar has proposed encryption algorithm using two approaches of pixel replacement. In the first approach, each pixel is shifted by using a random shifter generated by using the logistic map with a Key1 and modified by using the modulus operation to get integer values. In the second approach, the resulted image will be mapped by using Pixel Mapping Table (PMT) constructed using logistic map with a key2 for each column. Then modify the resulting image by using another PMT which is constructed using logistic map with a key3 for each row in the image.

**Paper 18 [29] "Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function", 2012.** The author has proposed image

encryption is based on Logistic map chaotic sequences with a nonlinear function. Encryption and decryption algorithm is built by a nonlinear function and for these functions secrete keys is generated using one dimensional logistic map. It is shown that the combination of nonlinear function and logistic chaotic map has provided good statistical characteristics of cipher image and image data can be recovered correctly and reliably at the receiving end. But proposed system is not enough resistant to noise. It is also shown that encryption and decryption algorithm are not only sensitive to initial condition x but also for the bifurcation parameter r in the logistic equation (2).

**Paper 19 [22] "A new digital image encryption algorithm based on 4D chaotic system", 2012.** Authors have mentioned that image encryption using one dimensional chaotic map is not secure. So, Huang et al. has proposed image encryption algorithm using 4D chaotic system defined by equation (22). The proposed algorithm permutation matrix P is created using input image, 4D chaotic system and three controlling parameters. To construct P, half of the image data is used and from that three control parameters are defined. Also a set of chaotic real sequences are generated from (22). Based on the two control parameters value, the chaotic real sequences are selected randomly form the set and placed in P. After that elements of P are converted to integer. But the dimension of P is half of the image matrix dimension. Then encryption is done in two stages, that is half of the image is encrypted first and using this result another half of the image is encrypted. Cipher image is obtained by concatenating both the results. In order to do first half encryption, modular addition of first half of the image with product of P and third controlling parameter is done. For half encryption, modular addition of previous result and second half of the image is used.

**Paper 20 [19] "Modified Algorithm of Encryption and Decryption of Images using Chaotic Mapping", 2013.** Steffi et al. has proposed chaotic based color image encryption which consists of two stages and two high dimension chaotic systems. The chaotic systems used are Lorenz map (equation (13)) and Baker's map (equation (21)). In the first stage, based on the secret key provided either Lorenz or Baker system is selected and pixel shuffling is done. In the second stage again based on the secret key provided either Lorenz or Baker system is selected and pixel value is changed. The initial conditions and control parameters serves as secrete key in both the stages. Separate keys are used in both the stages. The resulting image is the cipher image.

**Paper 21 [12] "Image encryption scheme with key sequences based on Chaotic functions", 2014.** In the proposed algorithm synchronous additive stream cipher is designed and secrete key sequence is generated by chaotic Logistic map. Here the plain image is represented as sequence of image pixels. The encryption algorithm is built by the equation $c_i=p_i \oplus k_i \; \forall \; i = 0, 1, \ldots, d-1$ where $c_i$ is cipher text, $p_i$ is plain image, $k_i$ is key sequence and 'd' represents number of bytes equal to message length. Here the key sequences are generated and stored off-line in advance. Due to time constraint, security analysis is not conducted by the author and it can be considered as further work of investigation.

## 5.Comparative study of various existing chaotic image encryption algorithms

Based on the literature survey of chaotic image encryption algorithms dealt so far, what follows is to discuss about the security provided by the chaotic encryption algorithms for image data. The discussion is as follows: In [14] Guosheng et al. has proposed an image encryption using three chaotic maps. It is found to have large key space of about $10^{384}$ with 16 bit precision. Also the histogram of cipher image is almost flat. Based on the security analysis done, the algorithm is secure enough. From combination of the spatial-domain encryption and the traditional stream ciphers technology, the security of the encryption algorithm is enhanced effectively [25]. As hyperchaos has larger key spaces and the image shuffling algorithm proposed in [21] is more secure than other chaos systems, hence the hyper chaos has some potential application in the application of image encryption algorithms. A new image encryption algorithm with a large pseudo random permutation which is computed from chaotic maps combination provides more secure compared to other encryption algorithms. Hence the proposed algorithm [28] provides reasonable security against statistical cryptanalysis.

After modifying the pixel values and then doing row permutation and column permutation separately will enhance and increase the uncertainty of the cipher image. This provides more high security against different attacks [3]. Along with chaos if some nonlinearity is introduced in the encryption algorithm, it makes the algorithm highly sensitive. Thus security is increased [29]. Use of 4D chaotic functions provides more security compared to 1D

chaotic functions, hence using 4D chaotic maps is more suitable for image encryption [22]. Based on the key provided, selecting either of the two chaotic maps for encryption provides advantages like very large key space, high sensitivity to secret keys etc., it can be considered as a effective and robust system for image encryption [19]. In additive stream cipher the key sequences can be generated and stored off-line in advance hence is best suitable for real time tactical applications [12].

The security analysis done in [25], [21], [3], [22], [19] are key space analysis, key sensitivity test and computed correlation coefficients and found that it has large key space, highly sensitive to initial values and correlation coefficients are close to ideal value. The values computed are tabulated in Table II. Along with the above mentioned tests, some other tests like Histogram analysis, entropy and FIPS 140 has been conducted in some of the literatures as mentioned in *Table 2*.

From the above discussion it can be concluded that security analysis of the algorithms present in the literatures for different types of attacks can be taken as further work of investigation. Also developing new encryption algorithms using higher dimension chaotic maps and their security analysis for different attacks can be taken as future work.

## 6.Conclusion

In present days public media like internet and wireless networks are the main communication channel. Sending raw data of confidential information through such channels is not secure. Sensitive information like medical and legal records, business transactions, drawings specific to military and defense applications are generally exchanged through internet. In this background, this paper focuses on the survey of application of chaos theory in cryptosystems to provide security for the confidential data. Chaotic system is essentially governed by a mathematical function. Chaos systems used to generate sequence of real numbers. It is observed from the literatures that these sequences are highly nonlinear, random and very sensitive to initial conditions.

The existence of complexity and random behavior of the chaotic maps motivates many researchers to use chaotic maps in designing pseudo random number generators which can be used to generate key sequences for cryptosystems. Since the generated pseudo random numbers are real numbers, it has to be converted to binary sequence. Therefore while designing the PRNGs, a proper binarization algorithm must be used. The PRNGs use the chaotic real sequences as input and produces binary sequence as output. The literatures related to PRNGs reveal that randomness of the sequences has to be tested by using various statistical tests before using them as key sequences in any cryptographic applications. This paper also concentrates on the survey of chaos application in image encryption. Survey of image encryption reveals that the encrypted images can be analyzed based on key space, key sensitivity, visual observation, Histogram, Correlation coefficient and Entropy. It is observed that good encryption system possess large key space, highly sensitive key, almost flat histogram, correlation coefficients and entropy close to ideal values 0 and 8 respectively. When all these conditions satisfy then the encrypted algorithm is highly secure. To use image encryption algorithms in real time, time complexity also plays an important role. Based on the survey conducted on chaos theory, PRNGs and image encryption algorithms, it can be concluded that following tasks can be taken as future research problem: (i) designing of new PRNGs using chaos systems and testing their randomness using various statistical test suite, (ii) designing of new image encryption algorithm using key sequences generated and determining their computational and time complexity.

**Table 2** Performance analysis of existing image encryption algorithms based on various parameters

| **Types of analysis** | **Papers** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **[25]** | **[21]** | **[28]** | **[3]** | **[22]** | **[19]** | **[12]** |
| Key space | at least $2^{256}$ | $10^{70}$ for precision $10^{-14}$ | - | $10^{45}$ | ~ $10^{56}$ | $2^{128}$ | - |
| Key sensitivity | Highly sensitive | Highly sensitive | Highly sensitive | Precision key1 = $2x10^{-14}$ Key2 = $8x10^{-15}$ Key3 = | Highly sensitive | Highly sensitive | - |

| Types of analysis | Papers | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | [25] | [21] | [28] | [3] | [22] | [19] | | | [12] |
| | | | | $5x10^{-13}$ | | | | | |
| Correlation coefficients | | | | | | R | G | B | |
| Horizontal (p) | 0.982627 | 0.9241 | | 0.9278 | 0.9514 | 0.9508 | 0.9707 | 0.9579 | - |
| Horizontal (c) | -0.020859 | -0.0142 | $-7\times10^{-3}$ for k = 16 | 0.0965 | -0.0092 | -0.005 | 0.0018 | 0.0002 | 0.0027 |
| Vertical (p) | 0.983332 | 0.9524 | | 0.9609 | 0.9457 | 0.9718 | 0.9754 | 0.9818 | - |
| Vertical (c) | -0.024583 | -0.0074 | $-18\times10^{-3}$ for k = 16 | 0.1086 | -0.0376 | 0.0032 | -0.0063 | 0.0018 | -0.0020 |
| Diagonal (p) | 0.976314 | 0.9017 | | 0.9060 | 0.9833 | - | - | - | - |
| Diagonal (c) | 0.009668 | -0.0183 | $15\times10^{-3}$ for k = 16 | 0.0161 | 0.0733 | - | - | - | 0.0024 |
| Entropy FIPS 140 with Seq len 20,000 bits | - | - | - | 7.9996 | - | 7.99758 | 7.99708 | 7.99749 | 7.9973 |
| Monobit | - | - | 100 for k = 16 | - | - | - | | | - |
| Poker | - | - | 100 for k = 16 | - | - | - | | | - |
| Long run | - | - | 100 for k = 16 | - | - | - | | | - |
| Histogram | - | - | Almost uniform | Almost uniform | Almost uniform | - | | | flat |

## Acknowledgment
None.

## Conflicts of interest
The authors have no conflicts of interest to declare.

## References
[1] Chen G, Mao Y, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals. 2004; 21(3):749-61.
[2] Herring C, Palmore JI. Random number generators are chaotic. ACM SIGPLAN Notices. 1989; 24(11):76-9.
[3] Al-Najjar AM, Al-Najjar HM. Image encryption algorithm based on logistic map and pixel mapping table.
[4] Mandi MV, Haribhat KN, Murali R. Generation of discrete spreading sequences using chaotic functions and their use in spread spectrum communication. In proc. sonata international conference computer, communication and controls 2006 (pp. 128-33).
[5] Kocarev L. Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine. 2001; 1(3):6-21.
[6] Stavroulakis P, editor. Chaos applications in telecommunications. CRC press; 2005.
[7] Kellert SH. In the wake of chaos: Unpredictable order in dynamical systems. University of Chicago press; 1994.
[8] Cipra B. A prime case of chaos. What's happening in the mathematical sciences. 1999; 4:2-17.
[9] Pecora LM, Carroll TL. Synchronization in chaotic systems. Physical Review Letters. 1990; 64(8):821.
[10] Caponetto R, Fortuna L, Fazzino S, Xibilia MG. Chaotic sequences to improve the performance of evolutionary algorithms. IEEE Transactions on Evolutionary Computation. 2003; 7(3):289-304.
[11] Gershenson C. Introduction to chaos in deterministic systems. arXiv preprint nlin/0308023. 2003.
[12] Shruthi KM, Sheela S, Sathyanarayana SV. Image encryption scheme with key sequences based on chaotic functions. In international conference on contemporary computing and informatics 2014 (pp. 823-7). IEEE.
[13] Mandi MV, Haribhat KN, Murali R. A survey of generation of chaotic sequences for communication. In proceedings of national conference on signal processing and communication 2006 (pp. 59-60).
[14] Gu G, Han G. An enhanced chaos based image encryption algorithm. In first international conference on innovative computing, information and control 2006 (pp. 492-5). IEEE.
[15] Pareek NK, Patidar V, Sud KK. A random bit generator using chaotic maps. International Journal of Network Security. 2010; 10(1):32-8.
[16] Maldonado JA, Hernandez JA. Chaos Theory Applied to Communications--Part I: Chaos Generators. Electronics, robotics and automotive mechanics conference 2007 (pp. 50-5). IEEE.
[17] Menon AS, Sarila KS. Image encryption based on chaotic algorithms: An overview. International Journal

of Science, Engineering and Technology Research. 2013; 2(6):1328-32.
[18] Bucolo M, Caponetto R, Fortuna L, Frasca M, Rizzo A. Does chaos work better than noise? IEEE Circuits and Systems Magazine. 2002; 2(3):4-19.
[19] Steffi AA, Sharma D. Modified algorithm of encryption and decryption of images using chaotic mapping. International Journal of Science and Research. 2013; 2(2):77-81.
[20] Mandi MV, Haribhat KN, Murali R. Generation of large set of binary sequences derived from chaotic functions with large linear complexity and good cross correlation properties. International Journal of Advanced Engineering and Applications. 2010; 3:313-22.
[21] Gao T, Chen Z. A new image encryption algorithm based on hyper-chaos. Physics Letters A. 2008; 372(4):394-400.
[22] Huang X. A new digital image encryption algorithm based on 4D chaotic system. International Journal of Pure and Applied Mathematics. 2012; 80(4):609-16.
[23] Behnia S, Akhavan A, Akhshani A, Samsudin A. A novel dynamic model of pseudo random number generator. Journal of Computational and Applied Mathematics. 2011; 235(12):3455-63.
[24] Wang X, Liu L, Zhang Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Optics and Lasers in Engineering. 2015; 66:10-8.
[25] Xiao HP, Zhang GJ. An image encryption scheme based on chaotic systems. In international conference on machine learning and cybernetics 2006 (pp. 2707-11). IEEE.
[26] Gao H, Zhang Y, Liang S, Li D. A new chaotic algorithm for image encryption. Chaos, Solitons & Fractals. 2006; 29(2):393-9.
[27] Gold R. Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.). IEEE Transactions on Information Theory. 1968; 14(1):154-6.
[28] Yoon JW, Kim H. An image encryption scheme with a pseudorandom permutation based on chaotic maps. Communications in Nonlinear Science and Numerical Simulation. 2010; 15(12):3998-4006.
[29] Ogras H, Turk M. Digital image encryption scheme using chaotic sequences with a nonlinear function. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering. 2012; 6(7):885-8.

This paper is selected from proceedings of National Workshop on Cryptology-NWC 2016 organized at JNN College of Engineering Shimoga, Karnataka, India during 11-13, August 2016.