

Design of Lightweight Chaos based Cryptographic Primitives:A Comparative Analysis

Devisha Arunadevi Tiwari*^{1,2} | Bhaskar Mondal¹

¹Department of Computer Science and Engineering, National Institute of Technology, Patna, Bihar, 800005, India

²Department of Computer Science Engineering(Data Science), Ace Engineering College (Autonomous), Hyderabad, Affiliated to Jawaharlal Nehru Technological University Hyderabad, Telangana, 501301, India

Correspondence

*Devisha Arunadevi Tiwari. Email: devishaarunadevitiwari@gmail.com

Present Address

Department of Computer Science and Engineering, National Institute of Technology, Patna, Bihar, 800005, India.

Abstract

Context:

Due to enormous efforts in the development of phenomenal chaos and its desirable properties, various researchers have expressed an interest in developing secure and reliable cryptography primitives by incorporating its benedictory properties. But incorrect implementations of chaos and dependence on dubious finite precision technologies could lead to contradicting results.

Objective:

The aims of this research is to delineate the degree of chaoticity and its attribute utilization in the construction of cryptography primitives as a research arena for their security and dependability.

Method:

This work uses a comparative analysis to present the method of design of chaos-based cryptographic primitives. The study makes use of a panoramic collection of distinguished publications that have appeared in distinguished conferences and journals over the past three decades. An in-depth comparative analysis on lightweight implementations of chaos based cryptographic primitives is presented using standard metrics.

Results:

Research leveraging chaotic nonlinear systems to design cryptography primitives is classified into several domains. Chaos implementations in both analog and digital mode that were integrated in the design of cryptography primitives research are presented. Reports the evaluation metrics used to verify the algorithms. Results of several chaos-fixated implementations that have been compared across differing experiments are reported.

Conclusion:

The research is useful in determining the progress of chaos-based implementations in several scientific disciplines pertaining to the design of cryptographic primitives.

KEYWORDS:

chaos-based image encryption, permutation, substitution, chaos-based cryptography, pseudo random number generation.

1 | INTRODUCTION

This paper presents a detailed literature review of chaos based image encryption algorithms and chaos based primitive operations used in the design of image encryption algorithm. Existing encryption algorithms when applied over images do not give performance Secure image transmission requires robust encryption algorithms in order to protect the information with reliability. Image encryption is the process of providing information security and content protection by masking the image. Chaotic cryptography provides strong primitives to obscure the information within an image. The properties of chaos are exploited to acquire cryptographic needs, hence based on their applicability, these techniques are broadly categorized as analog chaos-based cryptosystems and digital chaos-based cryptosystems. When the chaos dynamics are employed to synchronize the system parameters of the cryptosystem in order to develop cryptographic primitives, then the method is called an analog chaos-based cryptosystem. Similarly, when the chaos dynamics are utilized over digital computers' precision system to apply cryptographic primitives then, the method is called a digital chaos-based cryptosystem. The spatial and temporal components of a particular image contain information description that serves as a control parameter for creating chaos-aligned encryption methods. Every quantity present in dynamic systems can be defined in a discrete-time domain. Real-life platforms like multimedia transmission, medical image security, the internet of things, and cyber-physical systems are well-known examples of dynamic systems that can be measured in the discrete-time domain. Hence, every real-world system can be modeled into different equations which are the dynamical systems themselves and so commonly termed as *maps*. The terms and the set of the universe used to quantify these equations possess numeric values, which are modeled with real-world systems' characteristics. Such features that mingle in the setting of cryptographic primitives are called *control parameters*. Research in the past three decades discusses the ways to achieve robust chaos in order to develop robust chaotic cryptosystems. Patra and Banerjee in 2018^[1], demonstrated that "*robust chaos will occur if the parameter space for the system is set to have the same parameter range as the range of parameters selected to construct the system*". Since a robust chaotic map always obeys the invertibility principle and has a unique inverse, guaranteed encryption with a benign key will result in guaranteed decryption using the same key. In case of non-invertibility, the encrypted image gets locked and we cannot retrieve the original image even with the benign key, the decryption process becomes impossible. A trustworthy cryptosystem is classified as *robust* if all of its parameters are taken up by a mutually conjunctive association between the system's dynamics and the chaotic features of the applied cryptographic primitive. Alvarez G. et al. in 2003^[2], did a thoughtful analysis of the precise derivation of control parameters to define secret key and the strength of dependence of encryption procedure dependent only on key. Hence, to understand the principle of a robust chaotic cryptosystem, it is mandatory to do three things, namely, i) first recognize the representation of an image in a visual perception system, ii) secondly, determine the characteristics of the image, iii) third, perform a gap analysis between theoretical and practical encryption procedure and its derivation with respect to chaos dynamics in the finite precision domain. A trade-off in these steps can always give an approximated *robustness* and can never give a perfectly robust chaotic encryption.

A visual impression of an object expressed as a function $f(x,y)$ in which the quantity reflecting at the point of x,y intersection is the light intensity at that location is called an image. In theory and practice, images can be categorized as analog images and digital images. An analog image is formed by capturing a continuous variation in the image tone present in the two-dimensional analog signal which is used to capture the image. Electrical signals are used as a medium to capture the analog signals in a 2D continuous space. The function used to capture the electrical variations is known as a point spread function or a 2D impulse response and is responsible for the formation of the image. Abruptly, the perception of the image is bestowed on the human notion of visual perception, which is a theory not yet well understood. Similarly, no standard formalism exists to assess the measure of the quality of the image, and also, no human observer exists as an archetypal to symbolize an ideal perception of an image.

2 | MOTIVATION

The image processing operation uses mathematical tools like convolution, Fourier transforms operations, run codes, and chain codes in order to obtain digital images from analog images. Popularly, digital images are stored in commonly used image formats like jpg, png, tiff, eps, pdf, gif, and svg. The science of design behind these file formats to store digital images is that they use raster graphics and vector graphics. The color models that have been used traditionally are RGB for limited colors and CMYK for image displays and prints. One of the most exciting facts about raster graphics is that an image is a representation of a

pixel grid or a point of color intensity at the x,y intersection. Hence, the only quantity which is static and fixed while capturing images through raster graphics is its intensity. Owing to this fact about the image during its generation process, the intensity of the image is the basis of any mathematical operation or any digital operation performed over this image in order to compute various image analysis tasks like average, standard deviation, minimum, maximum, median, mode, signal-to-noise ratio, etc. In contrast to this, the vector graphics representation used to generate the digital images focuses on the graphical features of the image. Every information postulated in the image is in fact a magnitude and a piece-let of gradient information of the contents of that image. The factual contents of the image are actually read in the form of visual effects like the color, contour, lines, fill, thickness, and stokes which enhance the visibility of the image and contribute to the human perception model about it. In totality, since, vector graphics takes into account the visual content as well as the gradient information of the image and also capture the metadata about the image like the date, time, camera settings, color composition, image size, and exposure into the image generation process, therefore, various image transformation tasks are well supported on vector graphics originated images. The vector graphics thus does not affect the loss of resolution anyhow and therefore are scalable without incurring much information loss. But vector graphics provides only svg, eps, and pdf file formats and is generally used for display and print tasks. Contrasting to this, vector graphics capture images into svg, eps, and pdf formats, in which only tiff, eps, and pdf formats use CMYK model. In order to understand the skeptical process of image cryptography, with the basis that the theoretical formalism to describe the image encryption process and its proof of correctness is available but is inexact, we contribute our survey to uncover the fine granular task of image encryption and present certain principles of image cryptography and discuss the paradigm shift in plaintext ciphering algorithms and the effect of their usage on image encryption. We also advocate that the simple techniques to encrypt images are unlikely to be strongly secure and robust and therefore discuss the visualization about strong image encryption and robust image encryption, thus concluding the design imperatives for robust image cryptographic primitives. Hence, subjectively, we present a basis of criticism about the skeptical process of image encryption, their inherent weaknesses, and the causes behind them. Henceforth, we present image algebra as a scientific representation of the image and its metadata and make headway to our discussion about the cryptographic operations performed to encrypt images for decades and thus derive the proof of inexactness in the image encryption task. We identify some of the research questions that revolve around several schools of thought in various scientific literature on chaos-based cryptography and define them to explore, examine, and analyze the application of the principles of chaos in robust image encryption. The objective of the proposed comprehensive and systematic review is to comprehend the state of the research at present, in addition to any disparities and impending concerns, but to report these in order to outline future research paths.

3 | CONTRIBUTION IN RESEARCH

1. This article presents an in-depth survey of methods used in past three decades to design chaos-based cryptographic primitives.
2. A comprehensive review on technical implementations of stochastic nonlinear systems a.k.a. chaotic maps, their benefits and defects on analog versus digital platforms have been compared and contrasted.
3. Identification of research gap, technology gap, implementation gap and tools standardization gap into chaos based cryptography.
4. Defining terms and techniques with respect to chaos implementation in the context of image encryption.
5. Empirical properties of chaos and its production by setting unique parameters and its consequence on finite precision platforms.
6. Taxonomy based on analog versus digital implementation of phenomenal chaos its comparison, analysis on several image encryption algorithms in the past thirty years.
7. Compare and contrast of permutation-only, substitution-only, permutation-substitution paradigms of chaos fixated image encryption schemes.
8. Critical observations in classical implementations of chaos based image encryption over analog versus digital platforms and probable solution domain in avante-garde techniques for these issues.

4 | PRELIMINARIES OF CHAOS THEORY

The “Design of Secure Chaos-based Image Encryption Algorithms” represents a critical endeavor in the realm of information security, aiming to fortify the protection of sensitive image data against evolving cyber threats. As our reliance on digital imagery continues to surge, ensuring the confidentiality and integrity of such data becomes paramount. This research embarks on the creation of novel algorithms grounded in chaos theory, leveraging the intricate dynamics of chaotic systems to develop robust encryption and decryption mechanisms. In this era of escalating cyber threats, the introduction sets the stage by elucidating the imperative of enhancing security measures for image data. It delineates the limitations of existing encryption approaches, particularly in the context of image-specific challenges. The motivation behind the research stems from the need to address these limitations, offering solutions that not only bolster security but also account for the unique characteristics of the image data. The scope of the study is outlined in this introduction, along with the particular issues that must be resolved and the goals that must be met. The novel application of chaos theory is highlighted, offering a divergence from traditional encryption techniques. As the narrative unfolds, readers will gain insights into the anticipated contributions of the research, the methodology employed, and the overall structure of the subsequent chapters. The journey begins with a call to fortify the security of image data through cutting-edge chaos-based encryption and decryption algorithms.

4.1 | Overview of Chaos based Cryptography

The evolution of Chaos-based secure image encryption algorithms traces a captivating journey through the annals of cryptography. This narrative explores the historical underpinnings, pivotal breakthroughs, and the collective efforts of researchers who have propelled this field from its nascent stages to its current state of intricate design and implementation. The utilization of chaos in cryptography emerged as an avant-garde concept in the late 20th century. Early pioneers recognized the potential of chaotic systems for generating pseudo-random sequences, a cornerstone in encryption. The groundbreaking work of researchers like Lorenz and Mandelbrot laid the theoretical foundation for applying chaos to cryptographic algorithms. As chaos-based cryptography gained momentum, researchers began exploring its application in image encryption. Initial algorithms faced challenges related to computational efficiency, key management, and susceptibility to attacks. Despite these hurdles, the novel approach captivated the cryptographic community, sparking a wave of research aimed at refining and enhancing chaos-based encryption schemes. The timeline of chaos-based secure image encryption is punctuated by significant milestones. Researchers have contributed innovative algorithms, addressing shortcomings and advancing the field. Notable contributions include algorithmic improvements, novel key generation methods, and adaptive strategies to counter evolving cryptanalytic techniques. These milestones collectively shaped the landscape of chaos-based image encryption. The development of chaos-based encryption algorithms is a testament to collaborative efforts within the global research community. International conferences, research publications, and collaborative projects fostered an environment of knowledge exchange. Researchers from diverse backgrounds brought expertise in chaos theory, cryptography, and image processing, enriching the collective understanding of this interdisciplinary field. Advancements in computational power and technological capabilities played a pivotal role in refining chaos-based encryption algorithms. The integration of chaos-based cryptography into various technological domains, including secure communication and image storage, marked a significant stride forward. Researchers leveraged technological progress to enhance both the efficiency and practical applicability of chaos-based encryption. Despite remarkable progress, chaos-based secure image encryption faces contemporary challenges. Researchers grapple with issues such as quantum computing threats, scalability concerns, and the need for standardized evaluation metrics. The ongoing pursuit of solutions to these challenges outlines the trajectory for future research in this dynamic field. The impact of chaos-based secure image encryption on information security is profound. From bolstering data confidentiality in image transmission to securing sensitive information in various applications, these algorithms have carved a niche in the cybersecurity landscape. The collective contributions of researchers have positioned chaos-based encryption as a viable and innovative approach to safeguarding digital assets. In its entirety, the evolution of chaos-based secure image encryption algorithms reflects the story of ongoing research, teamwork, and technological innovation. The progression from the conceptualization of chaos in cryptography to the complex architecture of modern algorithms is evidence of the tenacity and inventiveness of researchers across.

4.2 | Taxonomy of Chaotic Systems

The study presented in this research, aims to find the differentiation between weak sensitive dependence and sensitive dependence helps to deduce the chaotic states in a dynamical system. The saddle points and the empirical values of chaotic parameters play major role in handling specific level of perturbations in single, high and fractional dimensional chaotic systems. The magnitude of the $p(t)$, $q(t)$, and $r(t)$ methods which constitute a stochastic technique as its magnitude. One can subdivide stochastic systems into two primary categories: uni-modal and multi-modal. Researchers have developed a wide range of blended strategies to get around the drawbacks of chaotic maps, such as fixing the matrix tensor product theory, boolean connectivity, hybrid chaos using multiple maps and vector support devices, crossbreeding chaos and improving look-up table formation^[34], cascading or coupling of indispensable chaotic maps^[5678], and combining different transformations. Compressive sensing^[910], pixel adaptive diffusion, dynamical state variable selection^[111211910] are a few instances of finite state automata. Depending on the severity of the chaos and the number of system elements used during the chaos generating process, chaotic systems are divided into three types. We analyze and describe each of them based on how it is applied and how the chaos was established.

1. Low Dimension Chaotic System

When a dynamical system only has one positive Lyapunov exponent, it is referred to as a minimal-depth chaotic system^[13]. A minimal-depth chaotic system is constructed by extracting a smaller portion of the overall system components. It has a simple mathematical model and has low implementation cost. One dimensional chaotic maps are simpler in implementation but pose limitations such as existence of periodic windows and non-uniformity^[13]. A dynamical system with minimal dimensions is a discrete iterative nonlinear environment. Chaotic behaviour is the result of establishing an implicitly predictable process in an erratic manner^[13]. Chaos generated in such a way is theoretically manageable.

2. High Dimension Chaotic System

When a chaotic system has more than one positive Lyapunov exponent, it is referred to as a high-dimensional chaotic system^[14]. As a regime variables change, a component, for example, through a sequence of time span solitons, becomes chaotic, and the alternative component becomes chaotic, actually resulting in an extra positive Lyapunov exponent for the overall network^[14]. According to numerical data, one distinguishing feature of a high dimensional chaotic system is that the second largest Lyapunov exponent in the experimental setup goes through zero consistently iteration after iteration^[14]. A fractional map, an incessant flow, and a population scheme for species distribution are the most prevalently demonstrated instances of a high-dimensional chaotic system.

Authors^[1516] presented three unique continuous chaotic systems with advantageous chaotic dynamic features. Hyperchaotic perturbations occur frequently in irregular unsupervised dynamical systems with more than four dimensions and quasi-stochastic processes with more than three components. This crucial characteristic designates complex nonlinear systems since they typically have at least two positive Lyapunov function indices, or^[15] complex nonlinear systems. A set of equations of displacement can depict the far more extensive ephemeral aspects that a hyperchaotic system may produce^[14]. Two seminal specimens of multi-dimensional stochastic processes are the Lorenz and Rossler systems.

3. Fractional Order Chaotic System

Fractional-order chaotic systems exhibit extremely high chaotic behavior, but their realization involves much uncertainty and complexity. The fractional-order chaotic system can be implemented with circuits having fractional-order elements such as practice capacitors and switch capacitors.^[17] the limitation that the fractional-order chaotic systems suffer from complexity issues arise from fractional order units present in the electronic circuits used in its design. The uncertainty is a consequence of errors between the real and nominal values revealed in the electronic circuits. It is also a consequence of chaotic circuits' high unpredictability and non-linearity. Another approach to realizing a fractional-order chaotic circuit is cascaded series using RC ladders, two-port networks, chains, and tree networks. A posterior distribution of single-pole high-pass filter segments is employed to implement the impulse response Laplace variable required by such devices, and the experimental setup is then partitioned. Fractional calculus uses a variety of fractional operators, such as the Riemann-Liouville component^[1819]. Kilbas theory et al. 2006^[20], Podlubny's fractional derivative from 1999^[21], the derivative from Caputo and Fabrizio in 2015^[22], the derivative from Atangana and Baleanu in 2016^[18], the complex geometry derivative from Atangana and Baleanu (2016), the Hilfer derivative, and numerous other variations of the preceding operators are just a few examples. Due to its physical significance and the fact that it exhibits a higher capacity, the Caputo derivative is preferred when simulating chaotic systems. The Riemann-Liouville integral^[23], its corresponding fractional operator,

and the derivative of the Caputo fraction are discussed in this subsection. Let us look at a chaotic system from Lu, et al. 2004^[24], which is theoretically represented using the fractional derivative of Caputo by the following equations,

$$D_c^\alpha x = ax - by - yz, D_c^\alpha y = cx, D_c^\alpha z = -dz + y^2 \quad (1)$$

The initial condition parameters decided by the authors in this model for the above equations are as follows,

$x(0) = x_0 = 0.2, y(0) = y_0 = 0.2, z(0) = z_0 = 0.2$ The researchers used the above values for the fraction order chosen in the range $0 < \alpha < 1$ in modeling their fractional order proposed chaotic system. The value $a = -2, b = -6.4, c = 1$ and $d=1$ where selected. The fractional-order chaotic system exhibits hyperchaotic behavior at $\alpha = 0.94$ has hyperchaotic behavior. Hence, the chaotic and hyperchaotic behavior generation depends only on the experiment's choice of specific fractional order.

4.3 | Noteworthy Definitions

Definition 1. Chaos During his 1873 exposition, famed British researcher James Clerk Maxwell purportedly asserted that a system's state is deemed unstable "if a modification in the initial stage that is vanishingly little can lead to a linear interpolation in the state of the system in a limited amount of time."

Furthermore, Hunt and Yorke noted that it would be difficult to predict recurrence "if the viewpoint of the present situation was simply hazy during the arguments in 1993."

By setting the initial values and utilising chaotic sequences to arrive at the n, h outcome, chaotic sequences can be created using the principles of chaos-based encryption.

$$a_n + 1 = f(a_n; S) \quad (2)$$

in which a_n is the value after n, h iteration and $f(a_n; S)$ is the carefully selected chaotic map with the given specifications in set 'S'. The recurrence will occur if the stochastic model has more than one degree,

$$(a_n^1 + 1, a_n^2 + 1, \dots, a_n^M + 1) = f(a_n^1, a_n^2, \dots, a_n^M; S) \quad (3)$$

where M is the chaotic map's dimension. After the N iterations, M chaotic sequences will have occurred. As a result, every time $A_m = [a_1^m, a_2^m, \dots, a_N^m]$, $m = 1, 2, \dots, M$, that sequence will be used to mention the introduction from Devaney 2018^[25].

Definition 2. Chaos by Jacques Hadamard, 1898 French mathematician Jacques Hadamard said in a symposium in 1898, "The protracted functioning of a chaotic automata could be affected by an error or disagreement in the beginning conditions." Ruelle continued by stating that French physicist Pierre Duhem amended Hadamard's perspective in 1906, who characterized long-term estimates as "absolutely worthless"^{[26][27]}.

Definition 3. Chaos by Henri Poincare, 1908 Henri Poincaré, a French mathematician, physicist, and philosopher, contributed to a similar thread in 1908. He highlighted that, for all practical purposes, prediction was impossible since, "small deviations in initial conditions might eventually lead to huge differences"^[26].

Definition 4. Chaos by Stephen H. Kellert, 1994 Stephen H. Kellert, a psychologist at the University of Chicago, claims that chaotic components are present when the two essential traits of instability and aperiodicity occur simultaneously, and an unpredictable regimen is present when attuned dominance on the primitive state exists. As a result, quasi conduct is defined as the lack of a regular repetition of the amounts of the parameter estimate. Chaos appears to have unpredictable quasi behaviour and is extremely nonlinear, as shown by Kellert in 1994^[28].

Definition 5. Glendinning's Definition of Chaos, 2017 The most famous ubiquitous chaotic dynamical systems are the stock market, population growth in ecology, atmospheric turbulence, tornado, chemical reactions, the response of an electrical circuit, fluid dynamics, and mechanical systems^{[29][30]}. Most of these dynamical systems, found in domains like biology, medicine, information and communication technology, electrical and communication engineering, exhibit chaotic behaviour. As a result, one way to conceptualize a dynamical system is as a mathematical illustration of how the state changes over time^[31]. According to Glendinning, 2017^[31], a discrete-time dynamical system is also known as a map. The dynamics are then presented using a list of numbers.

Let's just use x_0, x_1, \dots, x_n to represent the variable x' 's status at the n th time instance. Next, a map is displayed by,

$$x_{n+1} = F(x_n) \quad (4)$$

where $F(x_n)$ is the mathematical function to modulate the evolution of the system^{[31][30]}. Chaos can be produced by both discrete and continuous equations mathematically^[25].

Definition 6. Devaney's Definition of Chaos, 2018 An eminent Professor in mathematics at Boston University Dr. R. L. Devaney^[25] states that for a continuous system "f" to be chaotic on metric space "X", it is mandatory that, "f" produces the following three behaviours,

$$f : X \rightarrow X \quad (5)$$

- "f" has a transitive relationship for every point "x" in "X",
- "X" has dense periodic points produced from "f",
- "f" has sensitive dependence on initial conditions such that change in them makes "f" non-deterministic.

Definition 7. Discrete Chaotic Maps The discrete structures, such as the Henon map, the standard map, the logistical networks, and the radial networks, are often described so, $b_{i+1} = F(b_i)$ ^[25].

Definition 8. Continuous Flow The expression for interconnected systems, also referred to as flows, is $dx(t)/dt = F(x(t))$. Chaotic flows are represented by Edward Lorenz's principle, the Rossler equation, the Duffing formula, and the Chua circuit, as cited in^[25]. There are several commonalities between smooth flows and discontinuous lookup tables.

Definition 9. Permutation A permutation is a function that transforms a set of bits or pixels in such a way that each group has a distinct inverse. A permutation is performed to incur diffusion. It shuffles the bits or pixels linearly using a predefined rule. A permutation 'p' on a set of bits or pixels in the original image *OI*, is a finite set of elements and is a bijection from elements of the original image *OI* to itself. It is denoted by,

$$p : OI \rightarrow OI$$

There can be $n!$ permutations on a set *OI* of 'n' elements.

Definition 10. Substitution Substitution is often used to incur confusion. It is used to mask the statistical properties by introducing non-linearity, which prevents pixel values from being inferred from its neighbourhood. Substitution is a method of replacing a pixel's or bit's value or position with a new one that is computationally derived with a deterministic and reversible condition. S-box, have properties such as bijection, non-linearity, rigorous cascade requirement, and bit independence constraint of input/output bits, is used to perform substitution.

Definition 11. Confusion Confusion is the process to incorporate complexities in ciphertext statistics to depend on plaintext data. It uncovers the link between the key and the ciphertext. It is impossible to identify the connection between the key and the distorted image when fixed with the key elements of the design. According to the Amigo, 2007 proposition^[32], confusion hides the dispersion of pixels in both the original and encrypted images.

Definition 12. Diffusion The cryptographic technique to nullify the statistical relationship between bits or pixels in original image *OI* and its corresponding encrypted image *EI* in order to instil avalanche effect is termed as Diffusion^[33]. A change in one pixel/bit of plain image causes changes in several pixels/bits of the encrypted image using diffusion. Reliable diffusion can be achieved using several CBP.

Definition 13. Robust Chaos Robust Chaos is incredibly susceptible to the secret key. The chaotic attractor is said to be resilient if there is not a periodic window or co-occurring electrostatic attraction in any accessible fraction of the dimensional region and it exists within that region. Such a chaotic convergence point cannot be substantially hampered by small changes in the threshold or transitional period in the nearby regions. A strong stochastic momentum cannot be damaged by low-intensity perturbations. The robustness of the cryptosystem is a necessary quality for its dependability in real-world applications. Robust chaos cannot exist in smooth systems. A set of parameters with the same size as feature field must be discernible during system design for the robust chaos to emerge^[1]. A well-known example of resilient chaos application is the three-dimensional Piecewise Linear Chaotic Map^[1].

Definition 14. Chaotic Phenomenon The border collision normal form, according to Glendinning et al.^[34], uses an unbounded group of variables for which a two-dimensional anomalous phenomenon occurs. Additionally, there are unbounded groups of the variables $(\tau k, \delta k)$, $k = L, R$ such that if $\mu < 0$ such that the boundary collision normal form has a steady state if $\mu < 0$, however if $\mu > 0$, it has a double strong stochastic magnetic dipole which results in robust chaos. The eigenvalue of BCNF is δ , and the feature vector of the attractor is τ .

As a result, one of the necessary but not sufficient conditions for the existence of robust chaos in $\mu > 0$ and a simple, stable periodic orbit in $\mu > 0$ holds if $\mu > 0$ there is a map F such that $F \in \text{BCNF}_{RC}$ has no equilibrium, and thus there can be no equivalent of the equilibria to 2D attractor result. However, stable periodic orbits in $\mu < 0$ can exist at parameter values with robust chaos. Robust chaos is visible in the attractors of Piecewise linear maps by including this additional necessary condition for the phenomenon to occur in the border collision normal form via homoclinic intersections,^[31]

Definition 15. Robust Encryption An encrypted image is vulnerable to a variety of unexpected risks when connected to an insecure channel. In the event of a metasploit, strong encryption must allow for the reconquering of the original image^[35]. A data encryption method must be highly sensitive to even a slight modification in the initial condition^[36].

Definition 16. Chaotic Keys The association between the control parameters and the initial variables, especially determine how the innate chaotic maps will evolve over time, must be described explicitly and accurately in chaos theory^[2].

4.4 | Primordial Chaotic Systems

Several researchers talk about various taxonomies of chaotic maps based on their properties, implementation or applicability etc. Muthu et. al, 2021^[37] analysed the chaotic systems and their maps from various perspectives such spatial and temporal characteristics. In this survey, we distinguish between two types of chaotic systems: *dissipative systems and conservative systems*, based on their strength and efficacy in the cryptographic task of designing a reliable image EDA, as illustrated in figure [1](#).

- **Conservative Systems**

The phase space components in the conservative systems do not change, in fact they neither show any region of attraction, any fixed point, any attracting limit cycle nor any strange attractor. But still a positive K-entropy can be seen in conservative systems where a strange attractor does exist and is mingled towards the regular regions. It does not possess attraction but are strange chaotic regions.

- **Dissipative Systems**

In contrast to this, the dissipative systems possess a fractal structure. A dissipative system possess state based on given input and move to output state based on supply rate. They have a storage function and the energy supplied to the system gives a strong connection to lyapunov stability. Due to their huge importance in quantum mechanics, an active research on discovering the properties of dissipative systems and mathematical ways to model their behaviors is still under research.

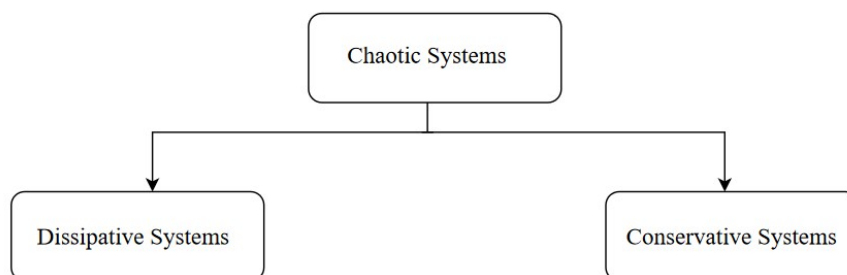


FIGURE 1 Types of Chaotic Systems.

Our goal is to assist in choosing the appropriate primordial system as the best candidate in the design of Chaos based image EDA. We do this by presenting the genesis of the primordial chaotic systems and talking about the basic properties of chaos employed in image EDA through table I. Instead of applying these features directly in their original form, we clarify appropriately applying them through chaotification as shown in table II. This will strengthen the system against image EDA-related attacks such as chosen plaintext attack (CPA), chosen ciphertext attack (CCA), and cipher only attack (COA).

4.5 | Examples: Popular Chaotic Systems and their Maps

Logistic System

Pierre Verhulst first put forward the logistic equation in 1845^[38]. A logistic system is recognized with sensitive dependence on initial conditions and is given by the equation,

$$P_{n+1} = UP_n(1 - P_n) \quad (6)$$

where n is the running variable and U is a parameter, is used to identify a logistic system with sensitive reliance on initial circumstances. The variable at the n th iteration, P_n , ranges in value from 1 to 0. A new value is generated by this recursive equation by building on the preceding one. The maximum value is 1, while the smallest value is 0. There are n generations and a growth rate of U .

Arnold's System

In 1960, Vladimir Arnold devised a dynamic system that can be shown to generate predetermined chaos^[39]. It could send itself a garbled map from the torus. Vladimir demonstrated the outcome with a cat image. As a consequence, it became known as "Arnold's Cat Map"^[39].

$$\begin{bmatrix} U_n + 1 \\ V_n + 1 \end{bmatrix} = \begin{bmatrix} 1 & A \\ B & AB + 1 \end{bmatrix} \begin{bmatrix} U \\ V \end{bmatrix} \text{mod } N \quad (7)$$

Chirikov–Taylor's System

Chirikov Taylor created a neighbourhood map for the two primary kinematic variables acceleration and vector (r, u) ^[40]. The Chirikov Taylor's map is described by the equations,

$$\hat{r} = r + K \sin u \quad (8)$$

$$\hat{u} = u + \hat{r} \quad (9)$$

the hat represents the actual values of the variables after one repetition of the map, such as when K is an abysmal variable which influences the intensity of chaos. The dynamics can be considered of as being located on a sphere by estimating $x \text{ mod } 2\pi$ as being on a torus by computing either x and $p \text{ mod } 2\pi$ owing to the periodicity of $\sin x$. The time-dependent Hamiltonian equation resulted in the map.

$$H(r, u, t) = r^2/2 + K \cos(u) \delta_1(t), \quad (10)$$

where $\delta_1(t)$ is the periodic δ function with period 1 in time. The movement is caused by a series of uncontrolled dissemination partitioned by recurrent impacts.

Lorenz's System

Edward Lorenz^[41] derived a mathematical dynamical system to model atmospheric convection in 1963. The system was represented by three ordinary differential equations and was termed as "Lorenz's equations".

$$\dot{p} = e(q - p) \quad (11)$$

$$\dot{q} = gp - pr - q \quad (12)$$

$$\dot{r} = pq - fr \quad (13)$$

These sets of equations exhibit a chaotic behavior when $e = 10$, $f = \frac{8}{3}$, and $g = 28$ where p, q, r are the state variables and e, f, g are machine components. Lorenz's system is three-dimensional, non-linear, and deterministic in nature and is demonstrated to occur on popular models like optical laser systems, electrical DC motors, and chemical reactions.

Chen's System

Chen discovered a chaotic attractor in 1999^[42] in a three-dimensional autonomous system which was far different from Lorenz's 3D system. Chen's map is represented by,

$$x = e(y_0 - x_0) \quad (14)$$

$$y = (g - e)x_0 - x_0z_0 + gy_0 \quad (15)$$

$$z = x_0y_0 - fz_0 \quad (16)$$

and is found to be chaotic when $e = 35$, $f = 3$, $g = [20, 28]$.

Sine's System

Among the most elementary nonlinear systems is the Sine chaotic map and is denominated as,

$$p_n + 1 = ex_n^2 \sin \pi p_n \quad (17)$$

The axiom takes on its simplified form and produces a chaotic sequence for the region with $p_0 = 0.7$ and $e = 2.3$ in the interval $(0,1)$.

Henon's System

In 1976^[43], Mitchel Henon arose with a condensed version of the Lorenz model's Poincare segment. A discrete-time stochastic process is the Henon map. It is one of the most explored instances of chaotic behaviour in dynamical systems. The Henon map transforms a plane vector (x_n, y_n) to a specific view determined by the expression,

$$P_n + 1 = 1 - eQ_n^2 + Q_n \quad (18)$$

$$Q_n + 1 = fP_n \quad (19)$$

The map depends on two components a and b , where $e = 1.4$ and $f = 0.3$. Henson's map is bound to be chaotic for the classical values.

4.6 | Crypto-friendly Properties of a Chaotic System

During the 1990s, several experts, scientists, and cryptography practitioners noticed an intriguing relationship between chaos and encryption. Several characteristics of chaotic systems have conventional cryptosystem equivalents. According to physics, chaotic dynamics contains a subset of cryptographic features in numerous

aspects, as shown by Gonzalo Alvarez and Shujun Li in 2006^[44]. A cognitive phenomenon that varies over time is called a transient regimen with further information. Arithmetically, a dynamical system's states are represented as a set of variables. In an equation that depicts the evolution of the system, the value of the baseline state reveals the mode of the emergence of the system. This is derived from the expression beneath,

$$\frac{dG_i(t)}{dt} = F_i(G_j(t), \lambda) \quad (20)$$

F is the element method to estimate how the system explodes to bifurcate, and $G_i(t)$ in R^N is the co-ordinate 'i' of the state of the regimen at instance 't'. 'X' is an n-dimensional vector with $i, j = 0, 1, \dots, N$ with $N \geq 1$. Only nonlinear dynamical systems with a nonlinear function F experiences chaos. Usually, discrete-time NLDS are used in chaotic digital cryptography and is represented by^[45],

$$G_{i+1} = F(G_i, \lambda)$$

where the above equation works for time "t" as discrete. So, the above system is now purely deterministic as the values of F , and λ can be calculated from the initial state G_0 . It is indeed "recurrent" when applied across finite state automata or neural networks because the subsequent entity can be simulated from the set point. Hence, both are best recognized as "deterministic and recursive". In an NLDS, the following terminologies formulate the characteristics of chaos, During the 1990s, several experts, scientists, and cryptography practitioners noticed an intriguing relationship between chaos and encryption. Several characteristics of chaotic systems have conventional cryptosystem equivalents. According to physics, chaotic dynamics contains a subset of cryptographic features in numerous aspects, as shown by Gonzalo Alvarez and Shujun Li in 2006^[44,46]. A cognitive phenomenon which varies over time is called a transient regimen^[45,27,47] with further information. Arithmetically, a dynamical system's states are represented as a set of variables^[45,27,47]. In an equation that depicts the evolution of the system, the value of

TABLE 1 Features of a Chaotic Map to Identify its Crypto-friendly Properties

Characteristic	Indicated by the presence of the conditions listed below
Dynamic instability	<ul style="list-style-type: none"> • a.k.a “butterfly effect or SDIC” • shift in initial states causes unexpected behaviour, • should have atleast one positive Lyapunov exponent, • should have a complex non-periodic orbit, • A change in λ leads to different dynamics such as “stochastic”, “cyclical”, “disparate” and causes bifurcation.
Deterministic	<ul style="list-style-type: none"> • Sensitive dependence on initial values fixes the chaotic path, • remains always the same till the initial values are not modified.
Unpredictable	<ul style="list-style-type: none"> • is non-linear, • has a high sensitivity to the initial state, • a non-linear system has “predictable short-term behaviour” but has “unpredictable long-term behaviour” and is completely “discontinuous”. • Presence of critical points and small modifications in them shows an inordinate effect.
Non-periodic	<ul style="list-style-type: none"> • Appears to be random and is disorderly, • random behaviour has a pattern and a specific order, • it is non-periodic and non-convergent.
Topological Mixing	<ul style="list-style-type: none"> • a sufficiently large N for two sets A and B in X such that $f^n(A) \cap B \neq \phi$ for every $0 \leq n \leq N$ is such that dynamical system for X is chorographically mixing, • Minimal chorographical transitivity conditions causes this to develop.
Dense periodic orbit	<ul style="list-style-type: none"> • Every position in the phase region becomes an amplified periodic juncture of topological transitivity.
Ergodicity	<ul style="list-style-type: none"> • Presence of regular and quasi periodic motions, • KAM theorem (Kolmo-gorov-Arnold-Moser) delineates a progressive transition towards chaotic trajectories.
Self Similarity	<ul style="list-style-type: none"> • The presence of a chaotic attractor makes the system produce invariant cycles resulting in self-similarity.

the baseline state reveals the mode of emergence of the system⁴⁵²⁷⁴⁷. This is derived in the expression beneath⁴⁵²⁷⁴⁷,

$$\frac{dG_i(t)}{dt} = F_i(G_j(t), \lambda) \quad (21)$$

F is the element method to estimate how the regimen evokes, and $G_i(t)$ in R^N is the co-ordinate ‘i’ of the state of the regimen at

instance 't'. 'X' is an n-dimensional vector with $i, j = 0, 1, \dots, N$ with $N \geq 1$. Only non-linear dynamical systems with a non-linear function F experience chaos^{45 27 47}. Usually, discrete-time NLDS are used in digital chaotic cryptography and is represented by^{45 27 47},

$$G_{i+1} = F(G_i, \lambda)$$

where the above equation works for time t as discrete. So, the above system is now purely 'deterministic' as the values of F, and λ can be calculated from the initial state G_0 . It is indeed 'recurrent' when applied across finite state automata or neural networks because the subsequent entity can be simulated from the set point. Hence, both are best recognized as "deterministic and recursive". In an NLDS, the following terminologies formulate the characteristics of chaos,

1. Phase Space

Every system state is constrained to $U \subset R^N$ and $F : U \rightarrow U$ in this subspace of R^N , where N is the degree of freedom and is the size of the phase space. The formation of a circle results from the evolution of the original conditions of the regimen in harmonic oscillator over moment. The discrete-time function $(j_0, p_0), (j_1, H(S_0)), \dots, (j_i, H_i(S_0))$ iterations are a set of plausible integer combinations^{45 27 47}.

2. Attractors

The protracted response of the orbits is referred to as "attractors". It recognizes the province of dimensional space where the machine's orbit meets the momentary. The system is constrained in the maneuverable region known as the attractor $A = F(A)$, within which all transformations concur^{45 27 47}.

3. Strange Attractor

A strange attractor is a specific type of attractor that can take the form of a juncture, a curve, a legion, or a dense set with a recursive pattern "strange attractor"^{45 27 47}. Ergodicity seeks to eliminate statistical relationships between the actual and encrypted images, which is analogous to the concept of confusion in encryption.

In a broader sense, the aspect of discord is achieved by ergodicity in such a way that the encrypted image has a homogeneous density. The frequency distribution of an encrypted image reveals a smooth and consistent spread. This behavior can be addressed in the prevailing encryption technology by employing the verse, "if 100 laypersons flip a coin once or a single layperson flips a coin 100 times, the output remains the same."^{48 49 30 50 51 52 53 52}

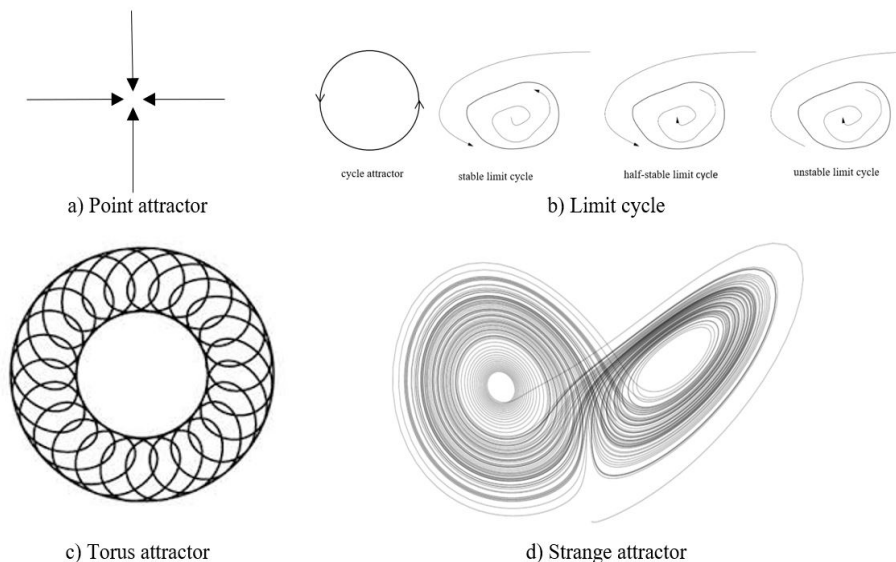


FIGURE 2 Types of Attractors.

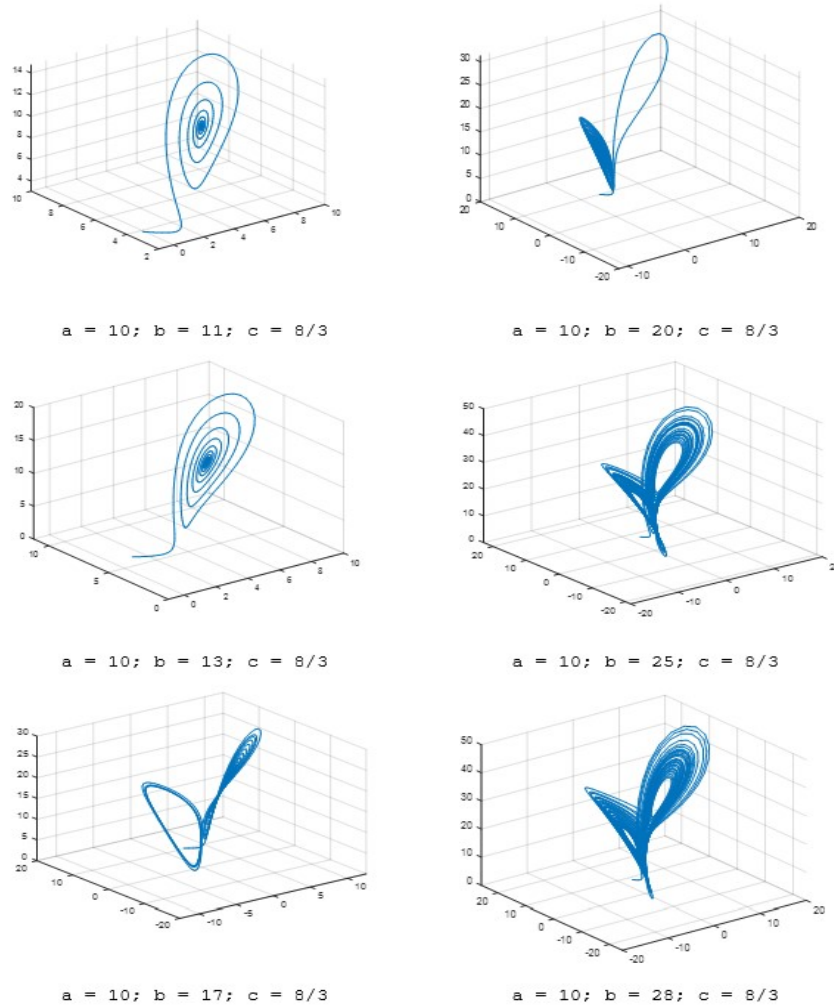


FIGURE 3 This figure illustrates the detection of chaotic attractor in Lorenz Map at various values of a,b,c. A limit cycle is detected at $a = 10, b = 11, c = \frac{8}{3}$, a torus attractor is detected at $a = 10, b = 17, c = \frac{8}{3}$ and a strange attractor is detected at $a = 10, b = 28, c = \frac{8}{3}$ in Lorenz map.

One of the essential properties in chaos dynamics is sensitivity to initial conditions wherein the concept of diffusion coincides with it one to one, in that a little deviation in the original image reflects a large deviation in the encrypted image. Chaos dynamics are deterministic in nature and exhibit pseudo-randomness behavior, usually in digitally developed chaos through a well-defined deterministic process. They also incur algorithmic complexity, one of the most desirable properties of cryptography through mathematical dynamics defined in the experimental process, thus inducing structural complexity. According to Shannon's theory, the only means to achieve a well-defined chaos⁵⁴ is the selection and incorporation of an appropriate chaotic non-linear map. Hence, a chaotic system generated in this way is called a discrete-time chaotic system. We discuss each essential property of chaos in detail below, as shown in figure ???. The chaotic maps possess some of these properties each. So, the choice and selection of a chaotic map in the design of cryptographic primitive should be bestowed on the chaotic features they possess.

4. Chaos possess dynamic instability.

The butterfly effect is a property of susceptible dominance on baseline states where a slight shift in one of the states of a deterministic nonlinear system can cause substantial variations in a subsequent state. It is one of the essential characteristics for chaos to exist. This implies that a slight change to initial conditions creates an unexpected behavior. It is also

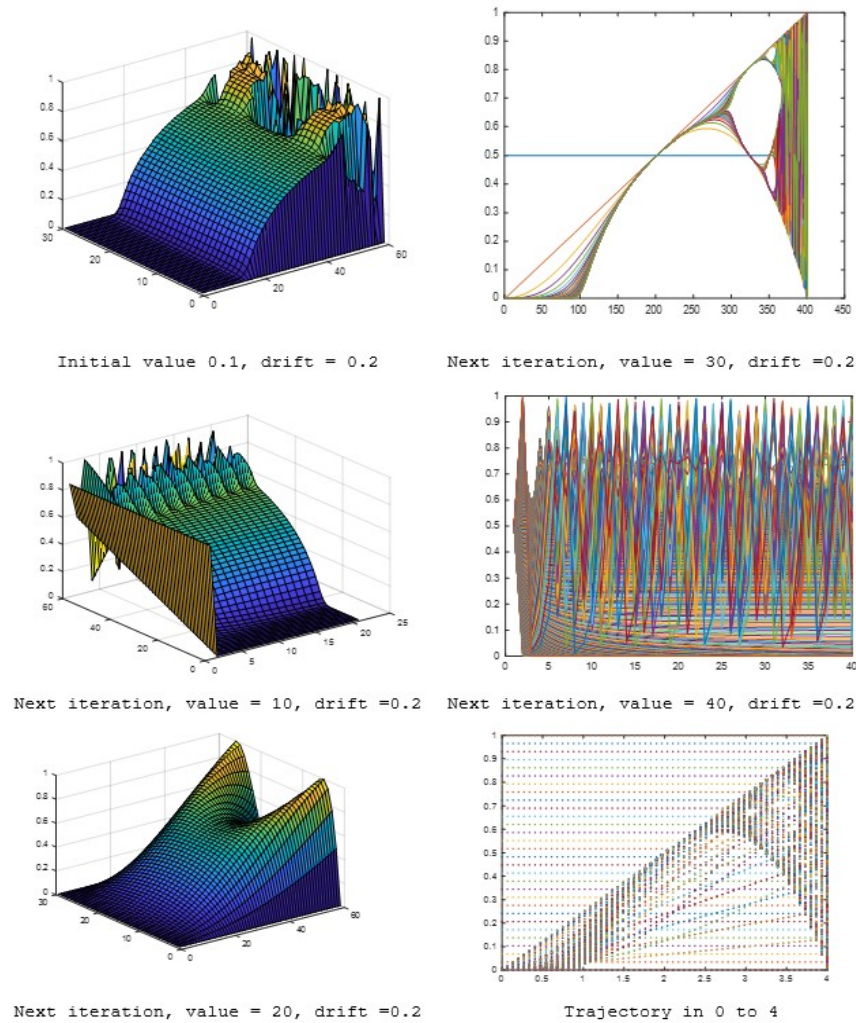


FIGURE 4 This figure illustrates the detection of the chaotic region in a Logistic map trajectory with $N = 30$. An initial seed value of 0.1 with a holding drift of 0.2 in the first 10 iterations produces a periodic cycle at $x = 20$. A bifurcation is detected in the next iteration at $x = 30$ with a holding drift of 0.2. The map shows a chaotic region at $x = 40$ with a holding drift of 0.2. The trajectory between $\lambda = 0$ to $\lambda = 4$ is illustrated in the 6th graph.

referred to as the butterfly effect. This characteristic of chaos is also known as “*dynamic instability*.” In NLDS, the orbital divergence is quantified using Lyapunov exponents. An N -dimensional system can be computed with N exponents. These exponents can be employed to estimate susceptibility towards its initial conditions of a nonlinear scheme. If a process has at least one significantly positive Lyapunov coefficient and a complex non-periodic orbit, it is said to be chaotic. In order to identify the zones of the system’s non-chaotic nature where recurring patterns can appear, it is helpful to look at the coefficients of the Lyapunov maxima as a result of the process variables, as depicted in the second equation above.

The second equation shows the impact of altering the control parameters on chaotic systems. This dependency might lead to drastically diverse dynamics for the system, such as stochastic, cyclical, disparate, etc., depending on the values of λ . A change in the quantities of the system coefficients^[27] results in a significant modification in the behavior of the system known as a bifurcation. The bifurcations charts are used to analyze the behavior of the system as a method of operation of the quantities of λ . These depictions make it possible to identify the sections of the dimensional space where the machine displays either periodic or chaotic behavior, depending on the values of the control parameters.

5. Chaos is deterministic.

The deterministic nature of chaos sincerely depends on its fundamental nature of sensitivity to initial conditions stating that determinism holds till the initial conditions remain unchanged and the chaotic path set by the initial condition values always remains the same. Chaotic maps designed using this phenomenon are deterministic by nature.

6. Chaos is unpredictable.

Chaos is a non-linear, fairly unrelated process that is highly sensitive to its initial state. The system has predictable short-term behaviour, but its long-term behaviour is unpredictable. A linear system is described by the principle of “sum of causes”, which is said to possess a cumulative sum of effects produced by the sum of causes of each previous component’s term. Popular examples of linear systems are growth in plants, flowers, a child from birth to adulthood, an object moving in a trajectory, a train moving to a destination, etc. In such systems, small changes lead to minor effect, and large change leads to big effects. Comparatively, a nonlinear system is completely discontinuous. Some popular and quantified examples are sudden breaks in atmospheric conditions, earthquakes, and tornadoes. A curve of a nonlinear system shows breaks, loops, and recursions which is a sign of the presence of some “turbulence”. A non-linear and dynamical system has critical points in which a small modification will show an inordinate effect^[29]. Hence, the physics behind the chaos is completely a postulation of a non-linear system. Thus, chaos is unpredictable^[29].

7. Chaos appears to be random.

Chaotic maps appear random and disorderly, but their random behavior resembles a pattern and a specific order. A stochastic process analogous to a non-linear dynamical system is just what chaotic phenomena resembles. It is non-periodic and non-convergent as a consequence.

8. Chaos possess topological mixing.

When there is sufficiently large N for every two open sets A and B in X such that $f_n(A) \cap B \neq \phi$ for every $n \leq N$, it is stated that a dynamical system f on X is chorographically mixing. Leading to chorographical mixtures, any given region or open set in the subspace of the scheme inevitably coincides with any other given region. Minimal chorographical transitivity conditions causes this to develop.

9. Chaos has dense periodic orbit.

Every position in the phase region becomes a periodic juncture as a result of topological transitivity and SDIC, which indicates that a chaotic system will demonstrate a substantial number of irregular phenomena^{[27][29]}. When the spots in the circuit are close enough to induce curvilinear translations, an effect known as the “strange attractor” causes every chaotic aspect in the pathway to reach adjacent regions in an exact chaos. This behavior is absolutely essential in encryption. Dr. Prof. David Ruelle, in 1972, stated the phenomenon of *strange attractor* by saying that, “the two distinct trajectories in the phase space never crossed across, but they appeared to create irregular cycles that were not completely concentric and were not completely on the same plane”^{[27][29]}. Attractors occur across many dynamical systems that are not chaotic, according to his theory of thermodynamics, however the odd attractor is a description of a chaotic system with a particular parameter space. The illustration on page [12] in figure # [2] shows the four different forms of attractors, which are a) equilibria, b) limit-cycle, c) torus, and d) strange attractor. A chaotic system amplifies the initial distances in the phase space. The changes in the system will be amplified quickly and become more chaotic if its characteristic Lyapunov time is short. The magnitude of amplification is restricted to the phase space of the universe. The amplification phenomenon is bound to come to an end eventually when the phase space ends. Therefore, the magnitude of randomness can be achieved and determined within the maximum limit of phase space^{[27][29]}.

10. Chaos possess ergodicity.

Dr. Kolmogorov A.N., an eminent professor in mathematics and physical sciences, revisited Poincare’s section and demonstrated in 1954,^{[27][29]} that every integrable system possesses a quasi-periodic regular motion even in the presence of minute perturbation which he postulated using Kolmogorov-Arnold-Moser (KAM) theorem, an indication of limits to integrability. The KAM theorem also delineates a progressive transition towards chaos that has trajectories within its integrable system with regular and quasi periodic motions. When a significant ratio of perturbation is induced, the probability of quasi periodic behaviour decreases, thereby increasing the proportion of trajectories to become completely chaotic. As

per the laws of physics presented by Dr. Prof Kolmogorov A.N., the remaining constant of motion at this instance is “*only energy*” and the motion was called “*ergodic*.” Hence, in this regard, the dynamical complex system which possess this feature are said to have “*ergodicity*”^{[27][29]}. Chaos is a dynamical and complex system and so it possess ergodicity.

11. Chaos possess Self Similarity.

The pattern of the development of the machine in time or space is the same at numerous measurement levels. This quality causes the system to look repeated at various observational scales^{[27][29]}. Eckmann J.P in 1985^[27] discovered that since an attractor is by definition invariant under a dynamical evolution, this results to a self-similarity that is often quite noticeable..

4.7 | Research Gaps

1. Quantitative Assessment: Many existing chaos-based image encryption algorithms lack comprehensive quantitative assessments of their security, making it challenging to compare their effectiveness objectively.
2. Adversarial Analysis: Limited research addresses potential vulnerabilities to adversarial attacks, such as targeted input manipulations or perturbations, leaving a gap in understanding the robustness of these algorithms.
3. Real-world Application Studies: There is a need for more studies examining the practical applicability of chaos-based image encryption in real-world scenarios, assessing its performance and security in diverse environments.

4.8 | Research Scope

1. Hybrid Approaches: Investigating the integration of chaos-based methods with other cryptographic techniques or machine learning for enhanced security and adaptability.
2. Dynamic Key Management: Exploring dynamic key management schemes to improve the adaptability of chaos-based algorithms to varying image characteristics and evolving security requirements.
3. Energy-Efficient Implementations: Exploring the feasibility of implementing chaos-based image encryption algorithms in resource-constrained devices, such as IoT devices, with a focus on energy efficiency.

5 | RESEARCH METHODOLOGY

We searched several scientific databases namely, the Google Scholar, Web of Science, Directory of Open Access Journals, PubMed, EBSCO, CNKI, MEDLINE, ProQuest, Academic Search Complete, ACM Digital Library, The arts BIOSIS Citation Index, Cabells, Clarivate Analytics, Crossref, Elsevier databases, Inspec, JSTOR, Asos index, CAS, PubScholar, Emerging Sources Citation Index, Primary index, Science Citation index, Science Citation index expanded, INSPEC, J-Gate Portal, EBSCO and retrieved quality papers based on the high quartile journal, high impact factor and minimum citations greater than 30 for each research article and performed an in-depth comparative study based on standard metrics over the methods used in the design of chaos based cryptographic primitives for lightweight implementations.

5.1 | Research Questions

The figure [5](#) illustrates the research questions in order to improve the chaos dynamics for lightweight implementations.

5.2 | Methods for Lightweight Implementations of Chaos based Primitives

5.2.1 | Mixing Transformation

Since the 1980s, academicians from a variety of fields started gaining interest in chaos-based encryption. Many similarities between chaotic systems and cryptosystems have been identified, particularly in the areas where these similarities might be used to produce cryptographic primitives. We examined many chaotic system types in the discussion above according to their power, size, complexity, and relevance. Based on the aforementioned chaotic system implementations, two categories of chaos-fixed

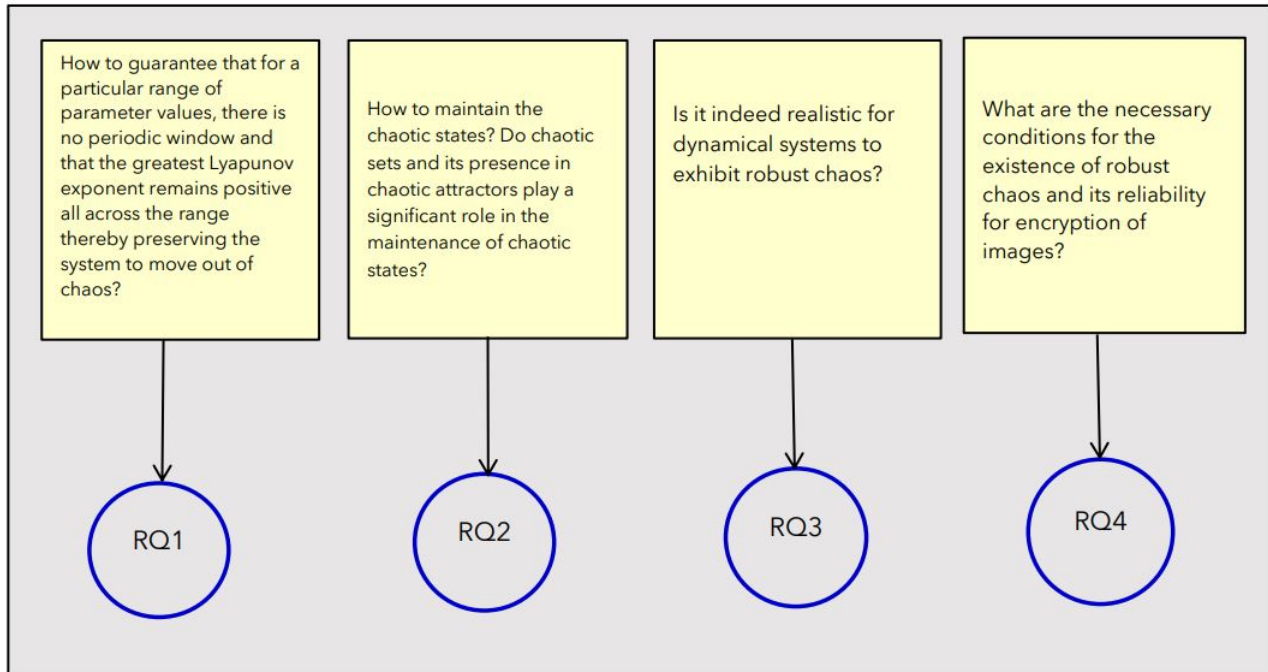


FIGURE 5 Research Questions

encryptions which operate on quite different chaotic notions may be recognized. In the first, chaotic systems are represented using analog technology, whereas in the second, chaotic systems are represented using digital technology. The following is a discussion of their use and application.

5.2.2 | Analog Chaotification

Analog chaos based systems produce strong and reliable chaotification when implemented using mixing transformations as discussed above. At the particular physical layer, an analog chaotic cryptosystem encrypts a data by camouflaging it with a chaotic noise. The analogue chaotic cryptosystems add chaos-inducing additives to the signal. One technique for adding a stochastic indication to the signal is additive chaotic masking. Chaotic shift keying is a different technique that adds to the data by shifting a digitized information signal between distinct nonlinear system. Furthermore, chaotic modulation is one of the ways where the specs or phase space of the chaotic transmitter are modified using an information signal. Chaotic control is a method of perturbing a chaotic system by intercepting an information signal in a canonical manner.

5.2.3 | Chaotic Masking

Chaotic masking, which entails supplying an input plaintext message or image as a signal described by $p(t)$ and integrating it in a carrier frequency $c(t)$ to create a paired dynamic signal $d(t) = p(t) + c(t)$, is the most basic and basic type of analog chaos-fixated encrypted transmission. Equivalent conjugative activities, such as multiplication, may substitute in place of additive depending on the needs of the system. The plaintext signal can be retrieved by estimating $p(t)$ and deducting it from $d(t)$ when stochastic synchronization has been established on the receiver section. Experiments in² showed that in order to prevent the signal of the obscured plaintext from adversely affecting chaotic synchronisation at the receiver, the energy of the plaintext message signal $p(t)$ should be significantly lower than that of the driving signal $d(t)$, that is, substantially lower than the strength of $c(t)$. The message signal cannot be precisely obtained because the message signal interferences with the driving signal, making chaotic synchronisation impossible. The unique feature of stochastic camouflage method is that the message signal has no impact on the master system's dynamics. Since an attacker can always utilise the driving signal to generate an attack, the security of chaotic masking against different attacks is dubious. Since the substantial energy of the input plaintext message or image must be considerably less than that of the output impedance, it is difficult to entirely solve the security vulnerability without replacing the encryption mechanism.

5.2.4 | Chaotic Switching

Chaotic stretching, also referred to as chaotic shift keying, is frequently used to transmit digital signals. The transmitter processes the 0- and 1-bit input plaintext message/image using two distinct chaotic systems. The plaintext message will occasionally alter the chaotic system being employed. Only one of the two chaotic systems is required at the receiver, and whether or not the plaintext bits may be retrieved depends on the replica variable capacity to establish chaos integration with the primary component. It should be noted that the two chaotic systems at the transmitter end could be homogeneous or in-homogeneous. When two homogeneous systems are employed, one dynamic system with configurable parameters operates, making chaotic switching systems easier to use. For the primary and replica units to produce coherent chaos, the bit propagation delay of each plaintext must be sufficient. As a result, the distribution velocity of a chaotic cross-coupled system is usually much slower than that of a chaotic camouflaging system. The key advantage of chaotic gating is the recovery of the actual plaintext signal, provided that the signal-to-noise proportion is not too extreme. It is well known that a number of attacks can be made against the stated simplistic chaotic switching mechanism. Testing of the currently in use chaotic shift keying approach reveals that the chaotic gating components at their core are useless and are easy targets for the attackers.

5.2.5 | Chaotic Modulation

There is a difference between chaotic multiplexing processes and catastrophic attenuation. The sender system is provided the plaintext message $p(t)$ in a stochastic regulation method, enables the plaintext message to constantly change the dynamics of the recipient component. In this situation, an optimised regulator is often added to the slave system in line with certain rule so that its output, $p'(t)$, which may also be thought of as an auxiliary random variable bidirectionally associated with the correspondent unit, asymptotically converges to $p(t)$. The slave system must receive the controller's output, $p(t)$, in the same way as the master in order to mimic the kinetics of the central controller. Chaotic modulation can be achieved using one of two methods. Direct modulation and dynamic attenuation are the first two. Direct modulation involves infusing one or more master system variables with the input plaintext message /image signal $p(t)$ without altering the regularization term. The plaintext message signal $p(t)$ modifies one or more control parameters in parameter regulation. When the driving signal and plaintext signal are mixed in certain stochastic modulation systems, input from the motor pulse signal and other required changes culminate in a refined type of stochastic attenuation. Compared to chaotic masking approaches, probabilistic attenuation algorithms can asymptotically recover the plaintext data if certain criteria are met. According to Alvarez G. et al. 2005's⁵⁵, chaotic attenuation performs better than chaotic gating and chaotic switching systems can only transport electronic information. If correctly developed, the chaotic attenuation approach might really transmit several plaintext message signals. One approach is to change the 'n' process variables of the master system using 'n' plaintext message signals. The main disadvantage of chaotic attenuation is that the controller depends on how the primary and replica schemes are designed, requiring the creation of several integrators for various master systems. In some cases, chaotic primary/replica process controllers may not even exist due to serious flaws in them.

5.2.6 | Chaos based Pseudo Random Number Generator

Digital or discrete chaotic cryptosystems are the source of Pseudo Random Number Generator (PRNGs). For multimedia security, chaos in cryptography has recently received significant interest.

5.2.7 | Bit Permutation


A grayscale image is represented by an array of pixels, each having eight bits for 256 different hues of grey. Each image pixel's bits are extracted, and then they are permuted using a key chosen from a pseudo-random generator with a chaos fixation. These permuted pixels make up the entire array of the encrypted image. The bit permutation approach transmits the encrypted image to the receiver across an unsecured channel. The recipient decodes the encrypted image using the same set of keys. Since each pixel has eight bits, it is presumed that the key length is eight. Three elements must be considered for bit-level encryption to be effective. First, each bit plane's bit distribution needs to be more uniform. First, there should be more uniformity in the bit distribution throughout each bit plane. Thirdly, the pixel values and placements should be changed, together with the second item a reduction in the correlation among nearby higher bit planes. The figure  shows the colour images of size 2000 X 1500 coffee-beans.jpg and 600 X 401 figs.jpg and their corresponding images showing permutation effect. The permutation keys are generated using hybrid 3D mixed chaotic map. The output reflects a notion of encryption but using merely permutation for encryption is astonishingly risky as it is an open door to statistical attacks.

TABLE 2 Analysis of Chaos Based Primitives for Random Number Generation

Year	Ref.	RNG-type	Chaotic-Map	Method	FPPC	Entropy	MSE
1963	56	PRNG	\times	Middle Square	\checkmark	7.9993	0.00053
2014	57	PRNG	QCM	QCM $eq^l's$	\times	7.9995	0.00010
2017	58	PRNG	Hitzl-Zele	Secret Pixel	\times	7.9999	0.00050
2019	59	PRNG	$Iked a(\mu = 0.701)$	CHAOSA	\times	7.9990	0.00060
2021	60	PRNG	Logistic map	Turbulence padded	\checkmark	7.9992	0.00054
2021	61	PRNG	Sprott Sys^m	Sprott based	\checkmark	7.9992	0.00052
2021	62	PRNG	Chaotic sequence	FPGA using VHDL	\times	\times	0.00640
2017	63	TRNG	Henon's, Logistic	Cascaded	\times	0.9998	\times
2021	64	TRNG	FPGA	$Fibo^{ci}-R^g$ Galois $Osci^r$	\times	0.9950	\times

†*Note* : This table presents an Analysis of Chaos based Primitives for Pseudo Random Number Generators and True Pseudo Random Number Generators. The research gap includes techniques to generate RNG(s) at a faster rate. The quoted entropy is in bits/bytes. A “ \checkmark ” denotes the attainment of the target value, and “ \times ” denotes test value not discovered. The test metrics used are FPPC, Entropy test and MSE.

†*Abbreviations* : Finite Precision Period Calculation(FPPC), Mean Square Error (MSE).

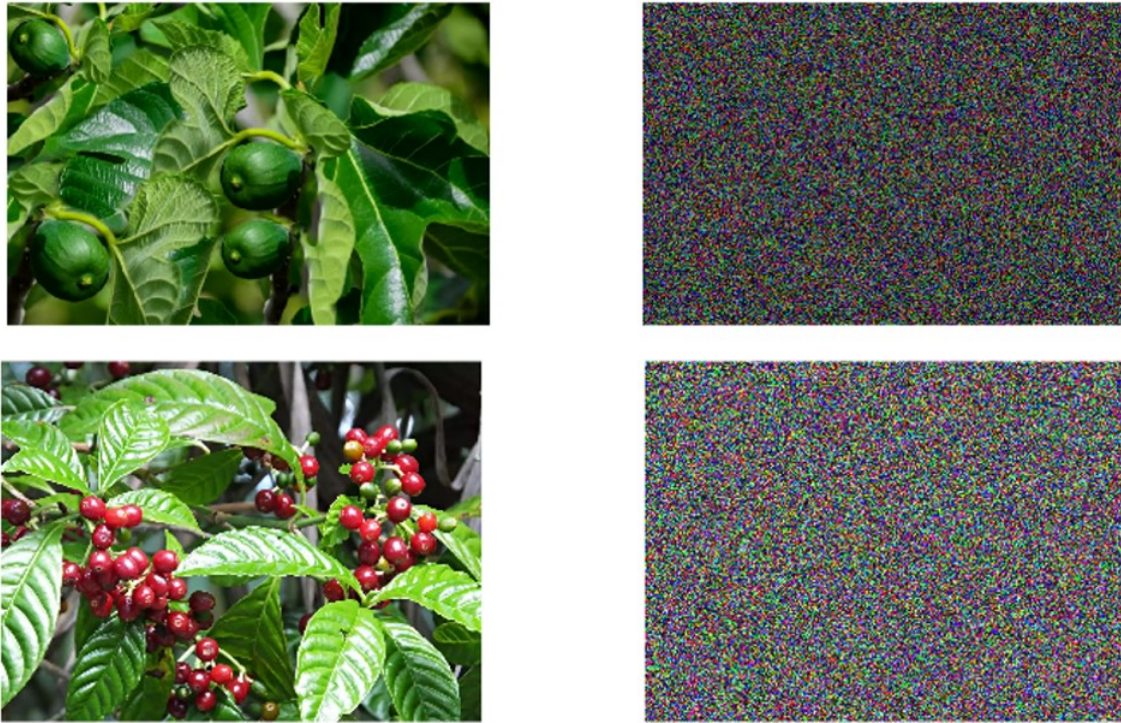


FIGURE 6 Permutation Effect on Images using Chaotic Keys

5.2.8 | Pixel Position Permutation

If the pixel position permutation meets the following three requirements, it can be used: (1) there must be no equilibrium in the permutation; (2) there must be no adjacent pair mapping in the neighborhood; and (3) the enormity of the permutation must be more than two-thirds of the shift factor in the randomization. Every set of pixels from the image is taken in this procedure. The key that is chosen from the list of keys is used to represent the pixels in the band. When utilizing the bit randomization approach, both the encryption and decryption processes are identical. The span of the keys, which are all the same extent, correlates to the dimension of the pixel group. The amount of perceptual information reduces if the span of the keys exceeds the span of the pixel clan. By periodically instantiating a chaotic map, the keys for pixel position scrambling are discovered through chaotic sequences.

5.2.9 | Pixel Value Permutation

A person, object, or work of art can all be represented by an image. Their outward appearance is defined by a group of pixels. The intensity at a given spot in the image is stored in the intensity values at that spot. The goal of pixel value transformation techniques is to eliminate the correlation between pairs of pixels. Through the use of mathematical processes like AND-ing, random shuffling, fractional-Mellin transformation, and random phase encoding through Fourier transform, the correlations between the pixels are totally eradicated.

5.2.10 | Block Permutation

A given image is divided up into blocks, and either a bit-level permutation or pixel-level permutation is then carried out. This process is known as block permutation. The block sizes should be lower for more secure encryption. However, if the size is really small, there is a big chance of information loss. One can arrange the blocks either horizontally or vertically.

Due to their lower processing complexity, permutation-only image encryption schemes have shown to be quite effective because they only change the image elements' positions, not their contents. They do not, however, provide complete security. One of the two things that lead to security flaws is statistical assaults; the data distribution of the randomized image retains an identical state as to those of the original image. Second, discretization is required for generating transposition keys from

nonlinear systems. This is a serious issue since, in the majority of instances, the chaotic map changes from aperiodic to periodic, which goes against the notion of security.

5.2.11 | Chaos based Substitution Schemes

The predictable and reversible replacement of one element from an original image with another is known as substitution. The mapping between each input and its replacement value is specified using an S-box in substitution. Chaotic S-boxes are used to defend against statistical and divergent attacks. In the process of replacing, pixel blocks are moved to a new place determined by keys generated randomly. An innovative approach proposed by Zhu et al. in 2011^[65] indicates the segmentation of image picture elements into combinations of bit streams depending on the number of image elements. Using Cat and Logistic maps, they then adjusted and updated the targeted bits in the image element values. Unfortunately, the proposed approach underwent cryptanalysis and was improved by Zhang in 2014^[66]. Nearly identical to this, the authors Fu et al.^[67] created a system using bit-level recombination with pixel-level replacements using a discontinuous cat map in 2011^[67]. This scheme was crypt-analyzed and enhanced shortly after by Zhang et al. in 2015^[68]. Unexpectedly, Chen et al. in^[69] of the effective system under revealed that it had equal permutation keys.

5.2.12 | Chaos based Permutation-Substitution Schemes

The bit pattern or pixel value can be changed using the substitution technique. The security of the image is significantly decreased by the possible combination and substitution-only image scrambling approaches. By using a replacement component that gradually modifies the pixel values, the substitution cipher form of image encryption eliminates this difficulty. Since adjustments to pixels usually rely on the consequences of all the preceding image pixels, a little modification in one data point could have an influence on almost all of the consecutive pixels. Bit replacement and pixel replacement is a method for altering the value of a bit or pixel. Simple procedures like exclusive disjunction and its complement, additive operations for pixel repositioning are employed to carry out reorganization. The security of the cryptosystem is strengthened by the existence of replacement elements. But it also puts up a distinct problem. A sizeable portion of the computation workload during the replacement process is used by the real number algebraic expression and associated downsampling needed by the key stream generation. Although the value of such computational complexity for realistic large-image encryption is substantially diminished, the mathematical accuracy cannot be too low due to security considerations.

5.2.13 | Chaos based Particle Swarm Optimization

Enthusiastic researchers in^[70] Wang et al, in 2016 introduced a novel implementation of chaotic cryptography in conjunction with the most successful notion of applied physics, 'particle swarm optimization. Their study investigates a one-dimensional Logistic map, DNA encoding sequences, and MOPSO-based image encryption technique. Particle swarm optimization (PSO) is used to determine the hash code of a plaintext image, a scramble mark bit, and the sub-key sequence, which together constitute the essence of the original study. Using a logistic map and DNA encoding, Wang et al generated random DNA mask images. They integrated it with the plaintext DNA encoding pattern, which was subject to block-shuffle, to produce an image encryption. A position in the plaintext image corresponds to the position value of the component in the recurrent PSO algorithm, which is influenced by the correlation analysis and data variance. The proffered encryption scheme was successfully able to pass the $(\chi)^2$ test and is fairly resilient to common attacks. A comparison investigation in^[71] shows that chaotic PSO outperforms various optimization algorithms, particularly the GA, DE, and ACO. Focusing on the grazing tendencies of species, Eberhart and Kennedy in^[72] established the PSO notion. A populace of ions is used in the paradigm of particle swarm optimization to signify an object that needs to be optimized. Momentum and orientation are two characteristics that each electron carries. By computing the relative merits of the actual state using a predetermined objective equation, the particulate positions can be distinguished effectively. The objective equation value is the strongest factor for determining, via successive iterations, the right place for every member, the objective value for the cluster, and the objective value of the band.

The figure ^[7] shows the pre-processed colour images of size 2000 X 1500 coffee-beans.jpg and 600 X 401 figs.jpg and their corresponding images showing substitution effect. The substitution keys are generated using hybrid 3D mixed chaotic map. The output reflects a notion of encryption but using merely substitution for encryption is again, astonishingly risky as it is an open door to statistical attacks and noise injection attacks. An adversarial machine learner can perform pattern analysis to discover substitution keys by intercepting a full-zero image.

TABLE 3 Avant Garde Radical Approaches recently used to Generate Hybrid Chaotic Maps^[73,71,72,74,75,76,77,78,79,80,81]

Year	Author&Work	Objective	Radical Approach	Improvement
2012	Akshani et.al ^[76]	Discretization	Derived map using quantum <i>represent^{ion}</i>	Period Doubling route to chaos.
2013	Ahmed A. Abd El Latif ^[77]	Encrypt Color Image	Quantum Chaotic Key	Optimized Finite <i>Prec^{ion} Repr^{ion}</i>
2014	Chauhan M Prajapati R ^[81]	Explore use of ANN in IE	ANN using Chaos	Efficient <i>Gener^{ion}</i> of Chaotic sequences
2016	Wang et.al ^[73]	Position Shuffling	Chaotic PSO	Randomization
2017	Mondal et.al ^[75]	Efficient, Secure image <i>trans^{ion}</i>	PRNG using Cellular Automata	Noise prevention
2017	Li et.al ^[80]	Color Image Encryption	ArFFT through CRPM	Quantum kernel-inverted Hilbert's Space.
2017	Maniyath SR et.al ^[82]	Expand keyspace	Encoding using Chaos Random Phase Mask	MSE of 0.01 only.
2019	Mondal et.al ^[74]	Confusion-Diffusion	2DSine-Cosine-Cross Chaotic Map	Increased Chaotic range
2019	Alawida et.al ^[83,61,2,84]	Keyspace expansion	DCFSA with-multiple chaotic maps	Improved ergodicity.
2021	Zhenlong M et.al ^[85]	Secure <i>Trans^{ion}</i>	5D Chaotic system as kernel parameters	Efficient <i>Gen^{ion}</i> of chaotic sequences.

[†] Note: This table presents avant-garde radical approach aiding improvements in chaos-based cryptographical research to develop robust hybrid chaotic maps which can counteract in the issues faced in direct implementations of chaotic maps.

[†] Abbreviations: ArFFT: Anamorphic Fractional Fourier Transform, CRPM: Chaos Random Phase Mask.

TABLE 4 Performance Comparison of Chaos based Permutation-Diffusion Primitives (CB-PD) used in Image EDA

Year	Ref.	Chaotic Map	Key Space	Performance Metric					
				NPCR(%)	UACI(%)	CC(H)	CC(V)	CC(D)	IE
2011	86	PWLCM	1.0368×10^{114}	99.62	33.49	-0.0574	-0.0035	+0.0578	7.9777
2011	65	Arnold's & Logistic	10^{42}	99.62	33.48	+0.0005	+0.0016	-0.0045	7.9999
2012	87	Chaotic Iteration	$\pi \times 2^{106}$	95.81	33.36	+0.0009	+0.0029	+0.0007	7.9972
2013	88	Tent	10^{88}	99.61	30.59	+0.0006	+0.0002	+0.0043	7.9992
2015	89	Quantum Logistic	2^{128}	99.64	33.53	+0.0011	+0.0007	+0.0008	7.9995
2017	90	Logistic	2^{492}	99.62	33.45	-0.0153	-0.0082	-0.0181	7.9993
2018	33	2D Baker's	228 bit key	91.04	37.75	+0.0090	+0.0010	+0.0013	7.9993
2018	91	Skew tent	2^{128}	99.64	33.39	+0.02238	+0.0076	+0.0295	7.9943
2019	92	Logistic-Sine	1.2219×2^{626}	99.60	33.46	+0.0031	+0.0005	-0.0041	7.9998
2020	93	Henon's	2^{256}	99.60	33.46	-0.0016	+0.0003	-0.0022	7.9987
2022	94	Logistic	2^{572}	99.62	33.32	-0.0068	-0.0091	-0.0233	7.9975

^a† Note: This table presents a comparison of chaos based permutation-diffusion primitives using classical (*non-hybrid*) chaotic maps and the key space achieved in the works during the decade. The standard Lena image 256X256 available at <https://sipi.usc.edu/database/> is used for encryption and the empirical values discussed in the table are tested on the metrics listed below in abbreviations.

^a† Table: Chaos based Permutation-Diffusion Primitives.

^a† Abbreviations: Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Correlation Coefficient Analysis Horizontal Proximity (CCH), Vertical Proximity (CCV), Diagonal Proximity (CCD), Information Entropy(IE)

TABLE 5 Performance Comparison of Chaos based Permutation-Substitution-Simultaneous-Operation Primitives(CB-PSSO) used in Image EDA

Year	Ref.	Chaotic Map	Key Space	Performance Metric					
				NPCR(%)	UACI(%)	CC(H)	CC(V)	CC(D)	IE
2011	95	Arnold's Cat	$\geq 10^{156}$	99.80	45.66	-0.0008	+0.0016	+0.0115	7.9970
2011	96	Standard	10^{45}	99.60	33.46	-0.0034	-0.0025	-0.0070	7.9957
2014	97	Logistic	$\geq 2^{256}$	99.68	33.40	+0.0008	+0.0023	+0.0045	7.9993
2018	75	2D Baker's	228 bit	99.75	39.12	+0.0214	+0.0011	+0.0178	7.9992
2020	98	Henon's	10^{27}	99.64	33.45	+0.0001	+0.0003	+0.0002	7.9997
2021	99	Standard	$\approx 2^{149}$	99.62	33.58	+0.0139	-0.0008	-0.0006	7.9986

^aNote: This table presents a comparison of chaos based permutation-substitution-simultaneous-operation(CB-PSSO) primitives using classical (*non-hybrid*) chaotic maps and the key space achieved in the works during the decade. The standard Lena image 256X256 available at <https://sipi.usc.edu/database/> is used for encryption and the empirical values discussed in the table are tested on the metrics listed below in abbreviations.

^aTable: Chaos based Permutation-Substitution-Simultaneous-Operation(CB-PSSO) Primitives.

^a†Abbreviations: Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Correlation Coefficient Analysis Horizontal Proximity (CCH), Vertical Proximity (CCV), Diagonal Proximity (CCD), Information Entropy(IE)

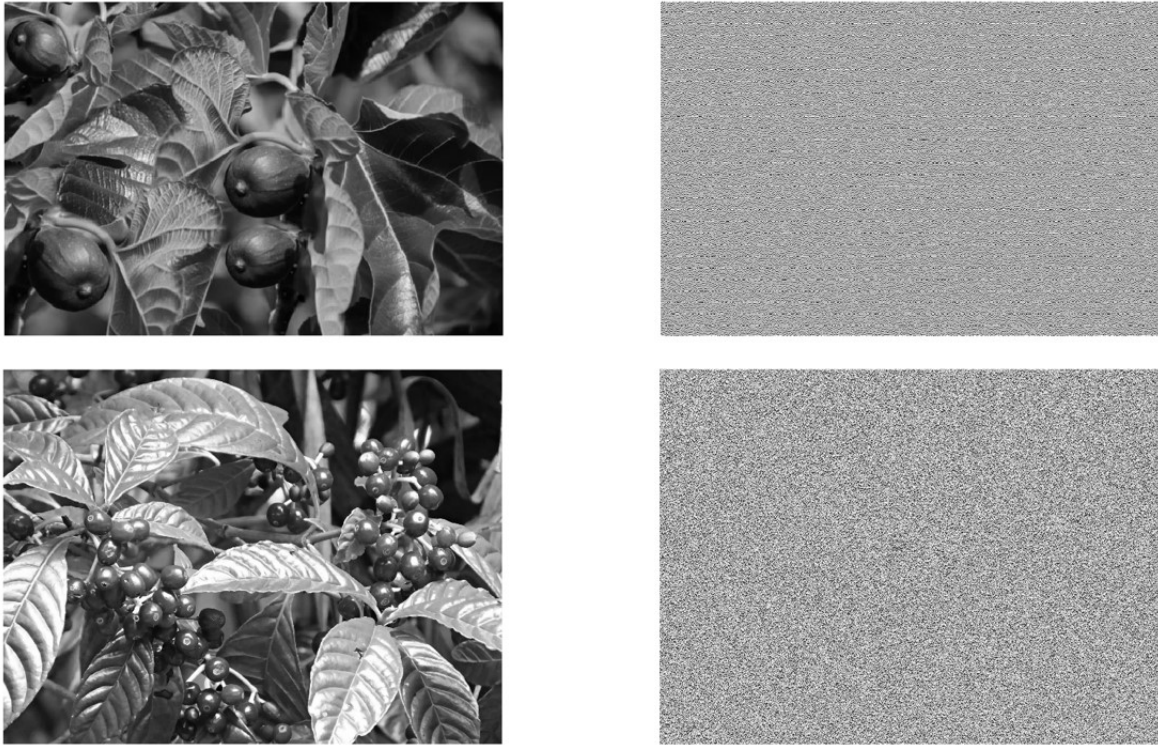


FIGURE 7 Substitution Effect on Images using Chaotic Keys

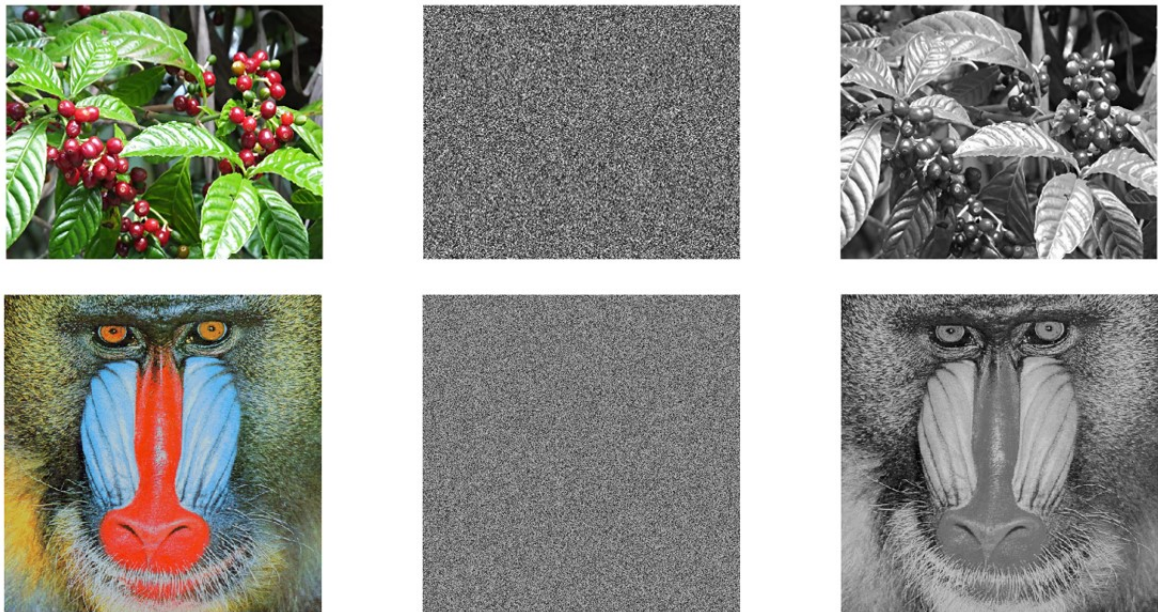


FIGURE 8 Confusion Diffusion Effect on Images using Chaotic Keys

The figure [8](#) shows the pre-processed colour images of size 2000 X 1500 coffee-beans.jpg and 512 X 512 mandril-color.tif, their corresponding images showing confusion diffusion effect and the corresponding restored images. The confusion diffusion keys are generated using hybrid 3D mixed chaotic map. The output reflects a notion of encryption but using merely confusion

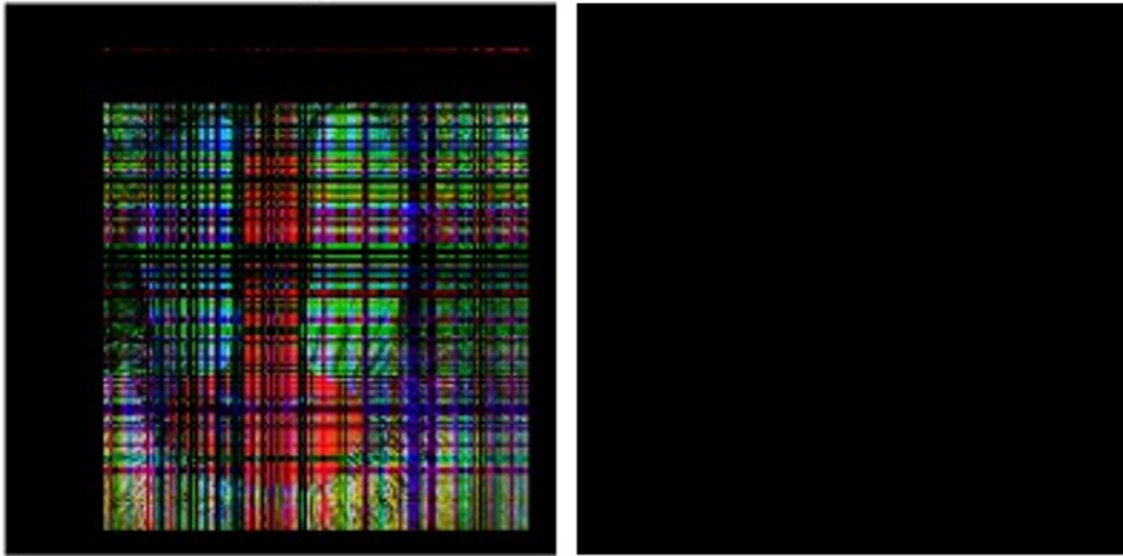


FIGURE 9 Effect of Interception by Inserting a Full-Zero Image Equal to Size of Original Image on Confusion Diffusion Scheme

diffusion is still not enough for robust encryption as discussed. Again, astonishingly taking risk of sole dependence on confusion-diffusion scheme for CB image EDA design, is again an open door to statistical attacks, noise injection attacks, frequency analysis and algebraic attacks. Through the process of reverse engineering, an adversarial machine learner can intercept a full-zero image and use pattern analysis to find confusion diffusion keys.

The figure 9 shows the pre-processed colour images of size 512 X 512 mandril-color.tif and its corresponding full-zero image showing interception effect on confusion-diffusion scheme. The confusion diffusion keys are generated using hybrid 3D mixed chaotic map. During cryptanalysis of the confusion-diffusion scheme, a full-zero image as shown in 9 was intercepted into the scheme to statistically detect and trace its pattern of confusion diffusion. The figure of mandril-color image shows success in traceability. Thus the output when reflects a notion of encryption but using merely confusion diffusion is never enough for robust encryption.

6 | CRYPTANALYSIS OF CHAOS BASED PRIMITIVES

Cryptanalyzing and breaking a chaos based image encryption algorithm using a chaotic cryptology primitive used is a challenging task due to the inherent unpredictability of well defined chaotic systems used in their designs. In contrast to this, due to the fact that chaos fixated designs were not constructed with consideration for either crypt-analytic or proof-based security design, chaos-fixated image EDAs have weaker designs. Multimedia encryption decryption systems with a chaos fixation are the ones that had not been created using a crypt-analytic design methodology. The chaotic cryptology primitives are time-tested and obey either of the two design approaches. The chaotic cryptology primitives follow modern cryptography design considerations. As a result, their security features do not align with the two concepts of security—provable security and practical security. Chaotic AES and chaos based DES encryption algorithms are considered as the standard cryptographic design for encryption and have been prominently used as benchmark methods to test the weakness of newly designed chaos based image encryption algorithms.

7 | PERFORMANCE ANALYSIS AND TRADE-OFF

Table 6 outlines the limitations of chaos-focused image encryption and weakness using the primary metrics used in testing. The concept of total security and robustness still has potential for research and advancement.

TABLE 6 Standard Evaluation Metrics used to test image encryption decryption algorithms

Evaluation metric	Why (Vulnerabilities)	Formula	Accepted range of test value
NPCR	Finite precision mismatches in $E(p, q)$ of encrypted image and $C'(a, b)$ of modified original image under test	$NPCR = \frac{\sum_{p,q} D_{a,b}}{R*S} * 100,$ <p>where $D(a,b) = \begin{cases} 0, & \text{if } C(a, b) = C'(a, b); \\ 1, & \text{if } C(a, b) \neq C'(a, b); \end{cases}$ is the variation between pixels in the original encrypted image and the modified image. Image width and height are represented by R and S.</p>	NPCR must be greater than 99%.
UACI	Finite precision mismatches in $C(a, b)$ of encrypted image and $C'(a, b)$ of modified original image under test	$UACI = \frac{\sum_{a,b} C_{a,b} - C'_{a,b}}{255*R*S} * 100$	UACI value must be around 33%.
PSNR	Deviations in pixel coordinates and bit representation due to fluctuations in finite precision arithmetic.	$PSNR = 10^a X \log_{10} \frac{(2^n - 1)^2}{MSE}$ <p>at which n is the count of bits in a pixel. .</p>	PSNR value should be maximum in $\{0, \infty\}$
MSE	Use of normalized calculations in floating point arithmetic. Unmatched is treated as a noise signal.	$MSE = \frac{1}{RS} \sum_{p=1}^{a=R} \sum_{b=1}^{q=H} (O(a, b) - E(a, b))^2$ where (a,b) = pixel co-ordinates of the image, R x S = width and height of the image, (PE) = Plain and Encrypted image.	MSE should be max. between PI and EI and in $\{0, \infty\}$.

^aNote: This table presents the evaluation metrics used scientifically to measure the accuracy of image encryption decryption algorithms.

^bAbbreviations: Number of Pixel Change Rate(NPCR), Unified Average Change in Intensity (UACI), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE).

TABLE 6 b.continued

Evaluation metric	Why (Vulnerabilities)	Formula	Accepted range of test value
RMSE	Use of normalized calculations in floating point arithmetic. Unmatched is treated as a noise signal.	$RMSE = \sqrt{\frac{\sum_{b=1}^{b=S} (P(a,b)-C(a,b))^2}{R \times S}}$ where (a,b) = pixel co-ordinates of the image, R x S = width and height of the image, (PE) = Plain and Encrypted image.	RMSE should be maximum in $\{0, \infty\}$.
BCR	Operators supporting normalized precisions cause loss of invertibility of control parameters during decryption.	$BCR = (1 - \frac{\sum_{a=0, b=0}^{M \times N} O(a,b) \oplus D(a,b)}{M \times N}) \times 100\%$ where (a,b) = pixel co-ordinates of the image, W x H = width and height of the image, O,D = Original and Decrypted image.	BCR value should be zero. it is the difference between the Original image & Decrypted image.
SDR	Use of normalized calculations in floating point arithmetic. Unmatched is treated as a noise signal.	$SDR = 10 \log_{10} \frac{\sum_{a,b} O(a,b)^2}{\sum_{a,b} (O(a,b)-D(a,b))^2}$	SDR value should be a large value.
CCA	Use of normalized calculations in floating point arithmetic. Unmatched is treated as a noise signal.	$r_{a,b} = \frac{C(a,b)}{\sqrt{D(a)} \times \sqrt{D(b)}}$ where (a,b) are the adj. pixels of an image; C(a,b) is the covariance between samples a, b; K is the no. of pixel pairs (a_i, b_i) ; D(a) and D(b) is the Std. deviation of a & b; E(a) = mean of a_i pixel values.	CCA should be nearly equal to zero.

^aNote: This table presents the evaluation metrics used scientifically to measure the accuracy of image encryption decryption algorithms.

^bAbbreviations: Root Mean Square Error (RMSE), Bit Change Ratio (BCR), Signal to Distortion Ratio (SDR), Cross-Correlation Analysis (CCA).

The performance of a chaos based image EDA is evaluated based on the several criteria such as security where the algorithm should resist various attacks such as statistical attacks, differential attacks, and brute-force attacks. The ability to withstand these attacks indicates the strength of the encryption, the speed where the efficiency of the algorithm in terms of processing time should be faster but it should not compromise security. Key sensitivity where the resistance of the algorithm to changes in the encryption key is vital. Small changes in the key should significantly affect the output to enhance security. Sensitivity to initial conditions should be carefully balanced to ensure robustness and security. After decryption, the quality of the reconstructed image should be visually similar to the original. Metrics like Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSI) are used to measure image quality. Trade-offs considered in Chaos based image EDA include,

- **Complexity vs. Security**

Increasing the complexity of the algorithm may enhance security, but it could also lead to slower processing. Balancing complexity with the need for efficient encryption is a trade-off.

- **Key Size vs. Performance**

Larger key sizes generally improve security but might slow down the encryption/decryption process. Finding the right balance is crucial.

- **Randomness vs. Predictability**

Chaos based algorithms often rely on chaotic maps to generate pseudo-random sequences. Striking a balance between randomness for security and predictability for key generation is important.

- **Robustness vs. Sensitivity**

Ensuring the algorithm is robust against various attacks while maintaining sensitivity to the encryption key and initial conditions is a delicate trade-off.

- **Applicability**

Consideration of the specific use case and the desired level of security. Some applications may prioritize speed, while others may prioritize higher levels of encryption.

Evaluation and trade-offs in Chaos based image EDA require careful consideration of these factors to meet the specific requirements of the intended cryptosystem as discussed in table [6](#).

8 | DISCUSSIONS

In this comprehensive review of classical methods using chaotic concepts, it is studied that, the majority of algorithms do not use the proper ways of incorporating chaotic theories, which results in security weaknesses. Lack of proper dispersion operations, vulnerability to known and intentional unpredictable threats, a lack of key spectrum, improper key sequence development, the need for numerous iteration steps, and improperly selected chaotic maps with poor statistical features, cryptographic systems, especially those based solely on chaos, do not always provide adequate security.

Pixel value distribution and statistical correlation can be masked using two main strategies: confusion and diffusion. It becomes increasingly challenging to distinguish between the cipher text and the key and is limited in its ability to inspect the encrypted data for repeats and statistical trends. In contrast, diffusion propagates the plaintext repetition across the entire cipher text, hence decreasing duplication. Even if each of these strategies are too vulnerable to attack, when coupled, they often provide an elevated level of defence. However, classical encryption techniques like DES, IDEA, and RSA are not successful to encrypt images due to the inherent characteristics of images, such as high pixel correlation and enormous storage capacity. Chaos-fixed techniques are utilized to optimize the needs of existing image encryption algorithms. When implemented accurately, with a mindful approach to use and incorporate chaos dynamics in image encryption, these can be the best candidate to develop strong image encryption algorithms.

8.1 | Findings of Research Questions

- ★ **Findings of RQ1**

“RQ1: How to ensure that a specific spectrum of model parameters have no periodic window and that the largest Lyapunov exponent is positive throughout the whole spectrum, preventing the system from becoming entirely periodic? Is it feasible to use chaos based primitives for secure design of image EDA ?”

Over the past three decades, there has been several unique studies which report and reveal the scientific progress in chaotic cryptography. Chaos has been used extensively in image encryption algorithms due to the crypto-friendly properties they possess. These empirical works provide concrete evidence that at least one Lyapunov exponent must be positive in order for the system to exhibit long-term chaotic behaviour. It is also important to test each and every possible value of the parameter in order to find the Lyapunov exponent. The value of Lyapunov exponent should be fixed by adjusting it with the system parameters. Chaos detection tests such as bifurcation diagram (BD) which is used to study the behaviour and detects the system cycles from periodic to chaotic orbits, Lyapunov exponent (LE) to test sensitivity to initial conditions, 0-1 test and three state test to detect regular, periodic or quasi-periodic cycles, sample entropy to measure the randomness of chaotic sequences, phase portrait test to identify the attractors and note the butterfly pattern, unequal distribution in histogram test shows weak chaos, time series analysis plots the features of data distribution with respect to time as discrete component, Kaplan-Yorke or Lyapunov dimension measure occurrence of fractional dimension which shows presence of strange attractor, Poincaré's section maps shows occurrence of fixed points, periodic orbits and chaotic motion, correlation dimension detects the strangeness of a dynamical system and checks the presence of fractals.

We explored that chaos possesses crypto-friendly properties beneficial for secure design of image encryption algorithms but there are very few studies where the incorporation of chaos in cryptography is discussed. Research and analysis in preliminaries of chaos for advances in cryptography is the most crucial need of the hour. In the study, we identified that the spectrum of chaos can be controlled by setting the domain and co-domain as the control parameters. The chaos trajectories can be fixed using system parameters. The mathematical predicates of domain, codomain as upper bound and the chain of logical deductions should be the basis of chaos based image encryption algorithm. Chaos has been beneficial candidate for image encryption and can be better standardized for cryptographically secure design of image encryption algorithms.

The security of chaos based image EDAs bestows only in the design of its scheme rather than the use of chaos based primitives for several cryptographic operations involved. Chaos is a best candidate for image EDA. The weakness if exist, they mostly are due to loose design of image EDA structures. Incorporating the necessary elements as discussed above can help fortify existing CB image EDAs. Contradictory, to this discussion, weak designs, such as permutation-only schemes, or reliance merely on CBP-PDO alone for encryption decryption task, degrade the chaotic maps used causing them to become periodic thus compromising the cryptosystem.

★ Findings of RQ2

“RQ2: How to maintain the chaotic states? Do chaotic sets, and their presence in chaotic attractors play a significant role in the maintenance of chaotic states?”

The occurrence of robust chaos is governed by the maintenance of chaotic parameter values in a well defined dimension of chaos. Spano and Ding in 1998^[100], described the magneto elastic ribbon experiment on Ikeda map in which the study of saddle points and regions of chaotic attractors are the chaotic states and the values occurring at those instance of the system parameters are the chaotic sets. Similarly, when a chaotic map is chosen, its chaotic states and chaotic sets can be derived from the chaotic ribbon experiment which makes the resultant system reliable and robust such that the system does not move out of chaos within a given polynomial time asymptotically.

★ Findings of RQ3

“RQ3: Are there any methods to fortify the existing image EDA(s) against the vulnerabilities prevailing due to degradation of chaotic maps used in their design? Is it indeed realistic for dynamical systems to exhibit robust chaos?”

Hybrid implementations to produce robust chaos mandates the prior system to be a dynamical system in its original form, if not then the system has to change to hybrid form. A robust chaos does not loose its dynamics and it definitely shows stage by stage first its periodicity, then its quasi-periodicity and gradually it becomes fully chaotic which can be tested using three state test. Computer generated chaos is implemented using digital mathematics and therefore called “pseudo chaos”. Eventhough pseudo chaos is considered unreliable, the stretch of randomness and required crypto-friendly properties can

be stochastic-ally generated through hybridization and control over chaos (CoC). In section 6, we discuss the methods to fortify the CB-image EDAs against known vulnerabilities during its design.

★ Findings of RQ4

“RQ4: What are the pre-requisites for the occurrence of robust and reliable chaos and its dependability for secure image encryption?”

The retention of chaotic parameter values in a strictly delineated dimension of chaos which controls the occurrence of robust chaos. In 1998, Spano and Ding^[100] described the magneto elastic ribbon experiment on the Ikeda map, where the values occurring at those instances of the system parameters are the chaotic sets and the study of saddle points and regions of chaotic attractors are the chaotic states. The chaotic ribbon experiment can also be used to determine the chaotic states and chaotic sets of a chaotic map, which renders the resulting system stable and durable by preventing it from escaping chaos within a given polynomial time asymptotically. In short, the chaotic tip trajectories can be maintained by controlling the chaos control parameters through cascading and fixation of hybrid hardcore predicates. This assures the robustness and reliability of a chaos based system and its dependability for secure design of image EDA. The chaotic states can be controlled and maintained by identifying the chaotic sets as described above.

9 | CONCLUSION

The chaos-fixated image encryption that has been in use for over thirty years is examined and assessed in this study. The formulation and basic properties of the cryptographic primitives used in image encryption were investigated in relation to the study focus described in section I above. This rigorous analysis gives a thorough overview of chaos-fixated image encryption techniques. The survey tables presents challenges dealt with, in this field by researchers on issues related to image encryption using chaos dynamics. We deduce from the survey that the chaotic map is assumed to be resilient if it is chaotic for all possible values of the control parameter. Traditional maps, like the atomic nonlinear system, need not be satisfactory, thus resulting in a smaller key pool and less protection against a prominent assault. A chaotic system is determined by one positive Lyapunov exponent. The use of atomic nonlinear stochastic systems, a.k.a. chaotic maps in finite precision platforms, causes dynamical degradation. A thorough analysis of significant schemes from the past three decades has led to the conclusion that most classical approaches are ineffective because chaos is used without the proper testing for the features that are used in the schemes. Methods which depend solely on digital chaos are uncertain and may become periodic once they cross the upper bound as the key spectrum is not chaotified as per the control parameters of the designed algorithm. Shannon’s principle of confusion-diffusion aims to provide randomization and mask statistical similarities, which if not tested with avalanche effect can leak the initial values. Images cannot be encrypted using chaos in its natural, non-chaotified form as most of the characteristics of images are easy to bring intercepted/duplicate image. Effective implementation of chaos based crypto-primitives requires adhering to the principles of Banerjee’s robust chaos discussed in the proposed work. In this survey, we thus, proclaim the optimal selection and choice of chaos methods based on dimensions, implementation, and hardware/software precision required for chaos-fixated image encryption algorithm and also the advanced strategies to improve the efficiency of chaos-fixated image encryption. The work discussed in this survey is useful to develop strong foundations for designing chaos-fixated image encryption algorithms. Chaos is the best candidate for efficient and secure image EDA design. Loose design imperatives such as discussed in section 5.2 affect the degradation of chaos causing it to become periodic thus compromising the whole cryptosystem.

Author contributions

Devisha Tiwari: review and editing (equal); Conceptualization (in supervision); writing – original draft (lead); formal analysis (equal); writing – review and editing (equal); Methodology (lead); Conceptualization (lead). Bhaskar Mondal: formal analysis(supervision);writing – review and editing (supervision); resources-gathering and analysis(supervision).

DATA AVAILABILITY

The data used in the research is available freely and need no permission for use. The code is conceptually designed and developed in Matlab R2018a and is available with the authors, will be shared upon request.

FUNDING

No research grant was availed for pursuing the stated research. No funding is received from any research support bodies.

ACKNOWLEDGMENT

I owe a deepest gratitude to Dr. Bhaskar Mondal Sir my doctoral supervisor, for his wise counsel, unwavering encouragement, and adherence. Throughout all of the presented scientific work, his vast knowledge and wealth of experience have captivated to work over the proposed concept.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CONFLICT OF INTEREST

- **Disclosure of potential conflicts of interest**

We declare that we have no conflict of interest in relation to the proposed work and we oblige to our roles as authors of the work. We undertake to carry our duties with the highest degree of objectivity and integrity.

- **Research involving Human Participants and/or Animals**

We certify that no human subject or biological material has ever been used in any of the studies in the proposed work. We declare that no research was done for the planned task that would be considered an infraction of animal protection legislation.

- **Informed Consent**

We attest that the planned work is completed utilising the viewpoints, plans, and technique that have been previously discussed and finalized. We concurred on every point on the manner the work would be done.

ABBREVIATIONS

GA	Genetic Algorithm: A search heuristic that mimics the process of natural evolution to find optimal solutions.
DE	Differential Evolution: An optimization algorithm based on the concept of mutation, crossover, and selection.
ACO	Ant Colony Optimization: An algorithm that simulates the behavior of ants to solve optimization problems.
DNA	Differential Network Algorithm: A bio-inspired optimization algorithm based on the principles of DNA computation.
PSO	Particle Swarm Optimization: An optimization technique that simulates the behavior of swarms or flocks in nature.
CMYK	Cyan, Magenta, Yellow, Key (Black): A color model used in printing and digital imaging.
NPCR	Number of Pixel Change Rate: A metric used to evaluate the effectiveness of image encryption algorithms based on the percentage of changed pixels.
UACI	Unified Average Changing Intensity: A metric used to measure the quality of encrypted images by comparing the intensity changes.
FPPC	First Pixel Prediction Correctness: A measure of the accuracy of predicting the first pixel in an encrypted image.
MSE	Mean Square Error: A metric used to quantify the average squared difference between original and encrypted images.
PSNR	Peak Signal-to-Noise Ratio: A measure of image quality based on the ratio between signal power and noise.
CCA	Correlation Coefficient Analysis: A technique used to evaluate the correlation between original and encrypted images.
SDR	Structural Difference Ratio: A metric that quantifies the structural changes between original and encrypted images.
BCR	Bit Corruption Rate: A measure of the percentage of corrupted bits in an encrypted image compared to the original.
RMSE	Root Mean Square Error: Similar to MSE, but the square root is taken to provide a more interpretable measure of error.

References

1. Patra M, Banerjee S. Robust chaos in 3-D piecewise linear maps. *Chaos: An Interdisciplinary Journal of Nonlinear Science* 2018; 28(12): 123101.
2. Alvarez G, Hernández L, Montoya F, Muñoz J. Cryptanalysis of a novel cryptosystem based on chaotic oscillators and feedback inversion. *arXiv preprint nlin/0311042* 2003.
3. Farah M, Guesmi R, Kachouri A, Samet M. A new design of cryptosystem based on S-box and chaotic permutation. *Multimedia Tools and Applications* 2020; 79(27): 19129–19150.
4. Alzaidi AA, Ahmad M, Ahmed HS, Solami EA. Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map. *Complexity* 2018; 2018.
5. Lan R, He J, Wang S, Gu T, Luo X. Integrated chaotic systems for image encryption. *Signal Processing* 2018; 147: 133–145.
6. Alawida M, Teh JS, Samsudin A, others. An image encryption scheme based on hybridizing digital chaos and finite state machine. *Signal Processing* 2019; 164: 249–266.
7. Hua Z, Yi S, Zhou Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Processing* 2018; 144: 134–144.
8. Zhang YQ, He Y, Wang XY. Spatiotemporal chaos in mixed linear–nonlinear two-dimensional coupled logistic map lattice. *Physica A: Statistical Mechanics and its Applications* 2018; 490: 148–160.

9. Peng H, Tian Y, Kurths J, Li L, Yang Y, Wang D. Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks. *IEEE transactions on biomedical circuits and systems* 2017; 11(3): 558–573.
10. Zhang Y, Xiang Y, Zhang LY. *Secure compressive sensing in multimedia data, cloud computing and IoT*. Springer . 2018.
11. Li H, Wang Y, Zuo Z. Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms. *Optics and Lasers in Engineering* 2019; 115: 197–207.
12. Alawida M, Samsudin A, Teh JS, Alkhalwaldeh RS. A new hybrid digital chaotic system with applications in image encryption. *Signal Processing* 2019; 160: 45–58.
13. Lai YC, Bollt EM, Liu Z. Low-dimensional chaos in high-dimensional phase space: how does it occur?. *Chaos, Solitons & Fractals* 2003; 15(2): 219–232.
14. Harrison MA, Lai YC. Route to high-dimensional chaos. *Physical Review E* 1999; 59(4): R3799.
15. Pincus SM. Approximate entropy as a measure of system complexity.. *Proceedings of the National Academy of Sciences* 1991; 88(6): 2297–2301.
16. Nag Chowdhury S, Ghosh D. Hidden attractors: A new chaotic system without equilibria. *The European Physical Journal Special Topics* 2020; 229(6): 1299–1308.
17. Yao J, Wang K, Huang P, Chen L, Machado JT. Analysis and implementation of fractional-order chaotic system with standard components. *Journal of Advanced Research* 2020; 25: 97–109.
18. Atangana A, Koca I. Chaos in a simple nonlinear system with Atangana–Baleanu derivatives with fractional order. *Chaos, Solitons & Fractals* 2016; 89: 447–454.
19. Atangana A, Gómez-Aguilar J. Numerical approximation of Riemann-Liouville definition of fractional derivative: from Riemann-Liouville to Atangana-Baleanu. *Numerical Methods for Partial Differential Equations* 2018; 34(5): 1502–1523.
20. Kilbas AA, Srivastava HM, Trujillo JJ. *Theory and applications of fractional differential equations*. 204. elsevier . 2006.
21. Podlubny I. Fractional-order systems and PI/sup/spl lambda//D/sup/spl mu//-controllers. *IEEE Transactions on automatic control* 1999; 44(1): 208–214.
22. Caputo M, Fabrizio M. A new definition of fractional derivative without singular kernel. *Progress in Fractional Differentiation & Applications* 2015; 1(2): 73–85.
23. Sene N. Analysis of a fractional-order chaotic system in the context of the Caputo fractional derivative via bifurcation and Lyapunov exponents. *Journal of King Saud University-Science* 2021; 33(1): 101275.
24. Lü H, Wang S, Li X, et al. A new spatiotemporally chaotic cryptosystem and its security and performance analyses. *Chaos: An Interdisciplinary Journal of Nonlinear Science* 2004; 14(3): 617–629.
25. Devaney RL. *An introduction to chaotic dynamical systems*. CRC press . 2018.
26. Barrow-Green J. *Poincaré and the three body problem*. No. 11 American Mathematical Soc. . 1997.
27. Eckmann JP, Ruelle D. Ergodic theory of chaos and strange attractors. *The theory of chaotic attractors* 1985: 273–312.
28. Kellert SH. *In the wake of chaos*. University of Chicago press . 1994.
29. Oestreicher C. A history of chaos theory. *Dialogues in clinical neuroscience* 2022.
30. Kocarev L, Lian S. *Chaos-based cryptography: Theory, algorithms and applications*. 354. Springer Science & Business Media . 2011.
31. Glendinning P. Robust chaos revisited. *The European Physical Journal Special Topics* 2017; 226(9): 1721–1738.

32. Amigo J, Kocarev L, Szczepanski J. Theory and practice of chaotic cryptography. *Physics Letters A* 2007; 366(3): 211–216.
33. Mondal B, Kumar P, Singh S. A chaotic permutation and diffusion based image encryption algorithm for secure communications. *Multimedia Tools and Applications* 2018; 77(23): 31177–31198.
34. Glendinning PA, Simpson DJ. Robust chaos and the continuity of attractors. *Transactions of Mathematics and Its Applications* 2020; 4(1): tnaa002.
35. Hosny KM, Kamal ST, Darwish MM. A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map. *The Visual Computer* 2022: 1–18.
36. Khan JS, Ahmad J. Chaos based efficient selective image encryption. *Multidimensional Systems and Signal Processing* 2019; 30(2): 943–961.
37. Muthu JS, Murali P. Review of chaos detection techniques performed on chaotic maps and systems in image encryption. *SN Computer Science* 2021; 2: 1–24.
38. Bacaër N. Verhulst and the logistic equation (1838). In: Springer. 2011 (pp. 35–39).
39. Peterson G. Arnold's cat map. *Math Linear Algebra* 1997; 45: 1–7.
40. Venegeroles R. Calculation of superdiffusion for the Chirikov-Taylor model. *Physical Review Letters* 2008; 101(5): 054102.
41. Tucker W. The Lorenz attractor exists. *Comptes Rendus de l'Académie des Sciences-Series I-Mathematics* 1999; 328(12): 1197–1202.
42. Guan ZH, Huang F, Guan W. Chaos-based image encryption algorithm. *Physics letters A* 2005; 346(1-3): 153–157.
43. Wen H. A review of the Hénon map and its physical interpretations. *School of Physics Georgia Institute of Technology, Atlanta, GA* 2014: 30332–0430.
44. Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos* 2006; 16(08): 2129–2151.
45. Ruelle D, Isola S. *Chaotic evolution and strange attractors*. 1. Cambridge University Press . 1989.
46. Li S, Chen G, Alvarez G. Return-map cryptanalysis revisited. *International Journal of Bifurcation and Chaos* 2006; 16(05): 1557–1568.
47. Carmen PL, Ricardo LR. Notions of chaotic cryptography: sketch of a chaos based cryptosystem. In: IntechOpen. ; 2012: 267–294.
48. Kocarev L, Halle KS, Eckert K, Chua LO, Parlitz U. Experimental demonstration of secure communications via chaotic synchronization. *International Journal of Bifurcation and Chaos* 1992; 2(03): 709–713.
49. Kocarev L. Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine* 2001; 1(3): 6–21.
50. Kocarev L, Jakimoski G, Stojanovski T, Parlitz U. From chaotic maps to encryption schemes. In: . 4. IEEE. ; 1998: 514–517.
51. Kocarev L, Galias Z, Lian S. *Intelligent computing based on chaos*. 184. Springer . 2009.
52. Baptista M. Cryptography with chaos. *Physics letters A* 1998; 240(1-2): 50–54.
53. Biham E. Cryptanalysis of the chaotic-map cryptosystem. In: Springer. ; 1991: 532–534.
54. Beck C, Schögl F. *Thermodynamics of chaotic systems* . 1995.
55. Alvarez G, Montoya F, Romera M, Pastor G. Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value. *Chaos, Solitons & Fractals* 2005; 23(5): 1749–1756.


56. Von Neumann J. Various techniques used in connection with random digits. *John von Neumann, Collected Works* 1963; 5: 768–770.
57. Akhshani A, Akhavan A, Mobaraki A, Lim SC, Hassan Z. Pseudo random number generator based on quantum chaotic map. *Communications in Nonlinear Science and Numerical Simulation* 2014; 19(1): 101–111.
58. Kordov K, Stoyanov B. Least significant bit steganography using Hitzl-Zele chaotic map. *International Journal of Electronics and Telecommunications* 2017; 63(4): 417–422.
59. Stoyanov B, Ivanova T. CHAOSA: Chaotic map based random number generator on Arduino platform. In: . 2172. AIP Publishing LLC. ; 2019: 090001.
60. Krishnamoorthi S, Jayapaul P, Dhanaraj RK, Rajasekar V, Balusamy B, Islam SH. Design of pseudo-random number generator from turbulence padded chaotic map. *Nonlinear Dynamics* 2021; 104: 1627–1643.
61. Cang S, Kang Z, Wang Z. Pseudo-random number generator based on a generalized conservative Sprott-A system. *Nonlinear Dynamics* 2021; 104: 827–844.
62. Dridi F, El Assad S, Youssef WEH, Machhout M, Samhat AE. Design, FPGA-based implementation and performance of a pseudo random number generator of chaotic sequences. *Adv Electrical Comput Eng* 2021; 21(2): 41–48.
63. Suryadi M, Ramli K, others . On the design of henon and logistic map-based random number generator. In: . 893. IOP Publishing. ; 2017: 012060.
64. Nannipieri P, Di Matteo S, Baldanzi L, et al. True random number generator based on Fibonacci-Galois ring oscillators for FPGA. *Applied Sciences* 2021; 11(8): 3330.
65. Zhu Zl, Zhang W, Wong Kw, Yu H. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences* 2011; 181(6): 1171–1186.
66. Zhang X, Shao L, Zhao Z, Liang Z. An image encryption scheme based on constructing large permutation with chaotic sequence. *Computers & Electrical Engineering* 2014; 40(3): 931–941.
67. Fu C, Lin Bb, Miao Ys, Liu X, Chen Jj. A novel chaos-based bit-level permutation scheme for digital image encryption. *Optics communications* 2011; 284(23): 5415–5423.
68. Zhang Lb, Zhu Zl, Yang Bq, Liu Wy, Zhu Hf, Zou My. Cryptanalysis and improvement of an efficient and secure medical image protection scheme. *Mathematical Problems in Engineering* 2015; 2015.
69. Chen G, Chen Y, Liao X. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. *Chaos, solitons & fractals* 2007; 31(3): 571–579.
70. Wang X, Li Y. Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. *Optics and Lasers in Engineering* 2021; 137: 106393.
71. Peng Y, Sun K, He S, Peng D. Parameter identification of fractional-order discrete chaotic systems. *Entropy* 2019; 21(1): 27.
72. Kennedy J, Eberhart R. Particle swarm optimization. In: . 4. IEEE. ; 1995: 1942–1948.
73. Wang X, Lin S, Li Y. Bit-level image encryption algorithm based on BP neural network and gray code. *Multimedia Tools and Applications* 2021; 80(8): 11655–11670.
74. Mondal B, Singh S, Kumar P. A secure image encryption scheme based on cellular automata and chaotic skew tent map. *Journal of information security and applications* 2019; 45: 117–130.
75. Mondal B, Mandal T. A light weight secure image encryption scheme based on chaos & DNA computing. *Journal of King Saud University-Computer and Information Sciences* 2017; 29(4): 499–504.

76. Akhshani A, Akhavan A, Lim SC, Hassan Z. An image encryption scheme based on quantum logistic map. *Communications in Nonlinear Science and Numerical Simulation* 2012; 17(12): 4653–4661.
77. Abd El-Latif AA, Li L, Wang N, Han Q, Niu X. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal Processing* 2013; 93(11): 2986–3000.
78. Boneh D, Dagdelen Ö, Fischlin M, Lehmann A, Schaffner C, Zhandry M. Random oracles in a quantum world. In: Springer. ; 2011: 41–69.
79. Cong I, Choi S, Lukin MD. Quantum convolutional neural networks. *Nature Physics* 2019; 15(12): 1273–1278.
80. Li J, Di X, Liu X, Chen X. Image encryption based on quantum-CNN hyperchaos system and anamorphic fractional Fourier transform. In: IEEE. ; 2017: 1–6.
81. Chauhan M, Prajapati R. Image encryption using chaotic based artificial neural network. *Int. J. Sci. Eng. Res* 2014; 5(6).
82. Maniyath SR, Thanikaiselvan V. An efficient image encryption using deep neural network and chaotic map. *Microprocessors and Microsystems* 2020; 77: 103134.
83. Alawida M, Samsudin A, Teh JS, others . Digital cosine chaotic map for cryptographic applications. *IEEE Access* 2019; 7: 150609–150622.
84. Alawida M, Samsudin A, Teh JS. Enhancing unimodal digital chaotic maps through hybridisation. *Nonlinear Dynamics* 2019; 96(1): 601–613.
85. Man Z, Li J, Di X, Sheng Y, Liu Z. Double image encryption algorithm based on neural network and chaos. *Chaos, Solitons & Fractals* 2021; 152: 111318.
86. Liu H, Wang X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Optics Communications* 2011; 284(16-17): 3895–3903.
87. Li S, Zhao Y, Qu B, Wang J. Image scrambling based on chaotic sequences and Veginère cipher. *Multimedia tools and applications* 2013; 66(3): 573–588.
88. Diaconu AV, Loukhaoukha K. An improved secure image encryption algorithm based on Rubik’s cube principle and digital chaotic cipher. *Mathematical Problems in Engineering* 2013; 2013.
89. Seyedzadeh SM, Norouzi B, Mosavi MR, Mirzakuchaki S. A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. *Nonlinear Dynamics* 2015; 81(1): 511–529.
90. Hu G, Xiao D, Zhang Y, Xiang T. An efficient chaotic image cipher with dynamic lookup table driven bit-level permutation strategy. *Nonlinear Dynamics* 2017; 87(2): 1359–1375.
91. Teng L, Wang X, Meng J. A chaotic color image encryption using integrated bit-level permutation. *Multimedia Tools and Applications* 2018; 77(6): 6883–6896.
92. Patro K, Acharya B, Nath V. A secure multi-stage one-round bit-plane permutation operation based chaotic image encryption. *Microsystem Technologies* 2019; 25(6): 2331–2338.
93. Shahna K, Mohamed A. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. *Applied Soft Computing* 2020; 90: 106162.
94. Annaby M, Ayad H, Rushdi M. A Difference-Equation-Based Robust Image Encryption Scheme with Chaotic Permutations and Logic Gates. *Journal of Mathematical Imaging and Vision* 2022: 1–14.
95. Ye R. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. *Optics Communications* 2011; 284(22): 5290–5298.
96. Patidar V, Pareek N, Purohit G, Sud K. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *Optics communications* 2011; 284(19): 4331–4339.

97. Panduranga H, Naveen Kumar S, others . Image encryption based on permutation-substitution using chaotic map and Latin Square Image Cipher. *The European Physical Journal Special Topics* 2014; 223(8): 1663–1677.
98. Vidhya R, Brindha M. A novel dynamic chaotic image encryption using butterfly network topology based diffusion and decision based permutation. *Multimedia Tools and Applications* 2020; 79(41): 30281–30310.
99. Mousavi M, Sadeghiyan B. A new image encryption scheme with Feistel like structure using chaotic S-box and Rubik cube based P-box. *Multimedia Tools and Applications* 2021; 80: 13157–13177.
100. In V, Spano ML, Ding M. Maintaining chaos in high dimensions. *Physical review letters* 1998; 80(4): 700.


AUTHOR BIOGRAPHY



Devisha Arunadevi Tiwari  is currently working as an Assistant Professor in Computer Science Engineering(Data Science) department at Ace Engineering College, affiliated to Jawaharlal Nehru Technological University, Hyderabad, Telangana, India. She is pursuing PhD in Computer Science and Engineering from NIT Patna. She received her Master's Degree in Computer Science and Engineering from Rashtrasant Tukodoji Maharaj Nagpur University. She has qualified Bachelor's in Engineering in Computer Technology (Industry Collaborated).She is an Axelos Certified Project Manager and has qualified Data Scientist Masters Program from SimpliLearn Pvt Ltd in Apache Alliance partnership under the Apache Software Foundation.

She worked as a Software Engineer(offshore) for four years.She is a member of ACM, IAENG and CSTA. Her research interest includes Deep Learning Architectures, AI and Robotics, Fuzzy Neural Networks and Social Networks Mining Algorithms, Cryptography and Information Security.



Bhaskar Mondal (Ph.D)  serves as an Assistant Professor in the Department of Computer Science and Engineering at the National Institute of Technology (NIT) Patna. He has nearly 10 years of experience in academics and research during which he had worked at NIT Patna, Xavier University Bhubaneswar (XUB), Orisha, India. BIT Sindri, Dhanbad, and NIT Jamshedpur. He was conferred with PhD from the National Institute of Technology Jamshedpur, India in 2018 followed by M. Tech. (CSE) from Kalyani Government Engineering. He has published more than 40 research papers in reputed journals and international conferences. He is senior member of IEEE and ACM, Life member of Computer Society of India (CSI) and

Cryptology Research society of India (CRSI). He is a book series editor titled Cyber Security of CRC Press. He acted as Lead Guest Editor for a special issue in CAEE, Elsevier. He has served several international conferences as session chair, advisory committee member and technical committee member. He has also reviewed articles in journals include Artificial Intelligence Review, Scientific Reports, Security and Communication Networks, Innovations in Systems and Software Engineering, ICT Express, IEEE Access, etc. His research interests include lightweight cryptography and machine learning.

How to cite this article: Devisha Arunadevi Tiwari and Bhaskar Mondal, Design of Lightweight Chaos based Cryptographic Primitives:A Comparative Analysis. *QEIOS* (2024) Vol.XX:XXXX-XXXX.