Journal of Technology and System Information Vol: 3, No 2, 2026, Page: 22-47

Survey on Using Chaotic Maps in Image Encryption Techniques

Malath Sabri Kareem

Middle Technical University

DOI:
https://doi.org/10.47134/jtsi.v3i2.5744
*Correspondence: Malath Technical Kareem
Email: malath-sabri@mtu.edu.iq

Received: 30-05-2026
Accepted: 30-03-2026
Published: 30-04-2026

Abstract: In this work, a direct experiment realization is proposed to encrypt 256×256 pixels grayscale image by using five different chaotic systems (Logistic, Tent, Henon, Lorenz, and a Logistic–Tent hybrid system). The permutation and diffusion process were executed with chaotic sequences derived from the same maps in order to quantitatively analyze the influence of each chaotic system on the statistical security metrics and the computation cost in a single unified execution environment. The results indicate that the quality of randomness was increased by increasing the complexity of the chaotic map as the entropy values were 7.91 for the Logistic map and 7.94 for the Tent map, 7.96 for the Henon map, 7.98 for the Lorenz system and a maximum of 7.99 for the hybrid model. This is a 0.08 better than worst model and it is closer to ideal entropy value 8. At the same time, the correlation coefficient of two adjacent pixels sharply reduced from 0.0043 to 0.0008, about 81% of decrease, which quantitatively verifying that the spatial dependencies in plain images is almost completely eliminated in the encrypted images. Regarding differential diffusion, all schemes attained NPCR values above 99.5%; however, the Lorenz system and the hybrid model yielded the best values of 99.71% and 99.74%, accompanied by UACI of 33.42% and 33.45%. This means that on average the intensity of a plain-pixel change was magnitude 33 variation to the average among 99.7% cipher-pixels. This numerical behaviour is mirrored in key sensitivity tests where a change in the control parameter μ or the initial condition x_0 in the 6th decimal place causes total decryption breakdown which is quantitatively in line with the large values of NPCR and UACI and establishes the presence of an extremely sensitive and non-approximable effective key space. The run times were 0.38 s and 0.42 s for the Tent map and the Logistic map, respectively, and rose to 0.50 s for the Henon map, and 0.63 s for the Lorenz system, whereas the hybrid model realized a medium execution time of 0.56 s. There is thus a clear quantitative trade-off between the security and the computational cost, as the marginal entropy increase of 0.01–0.02 in the Lorenz system was reached at an extra cost of 0.07 s with respect to the hybrid scheme, for this reason the security-to-time ratio of the latter was bigger. Also, when numerically compared with traditional algorithms, the hybrid chaotic approach provided better performance than AES in entropy value (7.99 compared to 7.85), in diminishing pixel correlation by up to 95% (0.0008 compared to 0.015), and in reducing execution time by 0.16 seconds. These results clearly illustrate that hybrid chaotic encryption can be expected to provide much better statistical security along with faster computation, which suggests that it is suitable for real-time image encryption and for use in systems with limited resource.

Keywords: Chaotic Maps, Image Encryption, Logistic Map, Tent Map, Lorenz System, Cryptography, Nonlinear Dynamics, Information Security

Introduction

The In the current digital age, an enormous amount of multimedia data is produced, transmitted, and stored daily. The exponential growth of digital images, facilitated by the proliferation of surveillance systems, cloud computing, social media, and medical imaging applications, requires the development of effective security mechanisms. Among the security measures is the use of image encryption to prevent unauthorized access, misuse, and leakage of sensitive data. Unlike text messages, images contain a high level of redundancy and pixel correlation. In addition, the volume of the data is large, which makes the use of traditional security mechanisms computationally intensive. The use of special encryption techniques for images has gained significant attention in the field of information security. The use of traditional encryption techniques, such as AES and RSA, is deemed secure. Nevertheless, the techniques were originally developed to secure text messages only. The techniques are inflexible to the security of images, which limits the use of the techniques in the security of images. The techniques have a fixed block length, which is disadvantageous when applied to images. The techniques may also be computationally intensive, which limits the use of the techniques for real-time images. Pseudo-orbits can produce sequences with similar random properties to measure-preserving transformations. However, there are other characteristics inherent in chaotic systems that are useful in implementing secure image encryption techniques. A chaotic system is a deterministic nonlinear dynamic system with an extremely high sensitivity to initial conditions, in which even minute changes in parameters result in drastically different trajectories. This feature of chaotic systems provides an excellent platform to develop encryption techniques that demand high standards of confusion and diffusion. The application of chaotic theory in cryptography, particularly in image encryption, has grown with the development of deterministic chaos theory by Lorenz in the 1960s. Since then, there has been an ever-growing application of chaotic theory in cryptography and its subsequent research. Chaotic maps such as the Logistic map, Tent map, Henon map, and Arnold's Cat map are examples of maps with excellent randomness properties, which are useful in implementing pseudo-random number generators in encryption techniques. These maps can be safely implemented in hardware with limited resources. More complex chaotic systems such as the Lorenz system and the Chua circuit are useful in implementing key propagation and diffusion in image encryption techniques. In addition, the security of multi-chaotic maps and integration with optimization techniques and learning mechanisms can be further enhanced against various attacks such as brute-force attacks, statistical attacks, and differential attacks. However, there are some limitations in the application of chaotic systems in implementing secure image encryption techniques. The finite precision sensitivity of chaotic maps is an inherent feature in digital implementations, which affects the key space and the encryption process. The balance between high-level security and low computational complexity in balancing chaotic encryption systems is another challenge in implementing secure image encryption techniques. Therefore, researchers are working towards improving the performance of chaotic systems and even more exotic systems such as hyperchaotic systems and fractional-order systems and their integration with conventional encryption techniques and even more exotic techniques such as artificial intelligence.

In this paper, the authors aim at narrowing the gap between the theory and practice of chaotic-map-based image encryption through the presentation of a comprehensive overview of the topic. The authors discuss the basic concepts and the state of the art in image encryption using chaotic maps and quality analysis in the context of pertinent open issues in study. The authors have made significant contributions in chaos theory image encryption. with application to the real-world scenarios such as secure multimedia and communication, remote sensing, and privacy preserving image storage and the like.

Significance of Research

The significance of the research work is further enhanced by the need to explore the enhancement of the security of the image encryption process through the application of chaotic systems. Chaotic systems incorporate non-linear operations in the various stages of the encryption process, thus enhancing the security of the data compared to traditional linear cryptographic systems. The minimalistic nature of the chaotic systems is a major advantage in the implementation of the encryption processes while maintaining a high level of complexity. The significance of the research work is further enhanced by the need to explore the application of the proposed work in the context of the IoT, medical imaging, and cloud multimedia services, which have been enhanced by the need to develop energy-efficient encryption processes.

Theoretical Background and Core Concepts

Image encryption is designed to convert image data into an unknown form so that the content cannot be understood by the attackers. Image encryption, on the other hand, has to deal with large amounts of data, high pixel correlation, and real-time processing, which are not encountered in text encryption. Here, the basic ideas of chaotic map–based encryption are reviewed, summarizing the general principle of classical and chaos-based models.

1. Traditional Image Encryption Models

Traditional image encryption algorithms are generally based on substitution, permutation, or both in a hybrid form. In substitution-based methods, pixel intensity values are substituted according to some predetermined or derived key. Popular cryptographic algorithms such as AES and DES make extensive use of substitution layers for confusion and to hide the relationship between the plain-image and the cypher-image. In permutation-based methods, however, all spatial correlation is removed by permuting the positions of the pixels, so that the original structural pattern of the image is hidden completely without change of pixel values; Arnold's Cat Map is a typical and classical example of this class of image encryption. Hybrid encryption schemes combine both substitution and permutation processes to provide higher security, where typically non-linear functions are used to increase the complexity of the system and the strength of the diffusion process. However, these classical encryption schemes are usually computationally prohibitive for large-scale multimedia data, even though they are effective

under certain conditions. In addition, their deterministic nature often exposes them to statistical and differential attacks (especially if encryption keys or parameters are recycled), restricting their applicability for contemporary high-throughput image encryption.

2. Chaotic Systems and Their Relevance to Cryptography

A theorem is a branch of mathematics and physics in which theories from nonlinear dynamical systems are developed. They operate by deterministic rules, but their behavior appears random and chaotic because they are highly sensitive to initial conditions. A small change in the initial state can result in substantially different outcomes over a long period of time, which makes long-term prediction impossible. Chaotic systems have several important properties which make it extremely attractive to use chaotic systems in cryptographic applications. Among the most important properties are:

1) Sensitivity to initial conditions: The chaotic system is sensitive to initial conditions, meaning that a small change, which is usually expressed as a decimal point, in the initial state of a chaotic system can cause an output sequence that diverges exponentially. This sensitivity is a key factor that makes a chaotic system unpredictable, which is a fundamental requirement for a cryptosystem to ensure that an intruder is not able to obtain a key without a specific understanding of the initial conditions.
2) Ergodicity: is the concept which describes the way a chaotic system's state can move in its state space as time elapses, regardless of whether a system spends more time in some areas or less. This results in a flat statistical distribution of the generated random values and thus intensifies randomness and decreases repetition. This feature is crucial in cryptography to resist certain statistical attacks and achieve good diffusion.
3) Determinism with Pseudo-Randomness: While the underlying mathematical equations describing chaotic systems are deterministic, the sequences associated with these systems seem to possess the qualities of true randomness. The interplay between determinism and randomness characterizes chaotic systems and makes them suitable for: pseudo-random number generation, cryptographic keys generation, pixel permutation and diffusion mechanisms in image cryptosystems and multimedia cryptosystems and other related arenas.

In practice, chaotic behavior is generated by chaotic maps, which are mathematical functions that are executed iteratively by applying nonlinear equations repeatedly to generate chaotic sequences. They are computationally efficient, easy to implement, and compatible with digital and hardware-based systems. For these reasons, chaotic maps have become a well-known and powerful tool in recent cryptographic schemes, especially in image and multimedia encryption.

3. Common Chaotic Maps Used in Image Encryption

Several chaotic maps have been extensively used in encryption applications because they are simple and efficient and present good chaotic properties. Among this class of maps, the Logistic map is one of the most frequently used nonlinear dynamical systems in image encryption. It presents strong sensitivity to initial conditions and control parameter

values; it is appropriate to use in the generation of pseudo-random sequences and cryptographic keys. The logarithmic map mathematical model is represented by the following iterative equation:

$$x_{n+1} = \mu x_n(1 - x_n), \quad 0 < \mu \leq 4$$

When the control parameter μ is larger than 3.57, the logistic map is in a chaotic regime and any perturbation on the x_0 from where the trajectory starts or on μ from where the value is taken results in substantially different output sequences. Such strong sensitivity helps enhance the security of the cryptosystem by complicating key predictions and brute-force attacks. Moreover, the logistic map has a simple mathematical form and high computational efficiency, thus it is more suitable for real-time image encryption. Its capacity in producing pseudo-random sequences with good statistical properties makes it nowadays widely used for key generation, pixel permutation and diffusion in recent image encryption algorithms.

Tent Map

The tent map is often used as a one-dimensional chaotic system in the context of image encryption methods, owing to the relative simplicity of the piecewise-linear structure of the tent map, as well as the high chaotic behavior it demonstrates. As a result, the tent map is highly sensitive to initial conditions and parameter settings, allowing it to produce chaotic sequences with high unpredictability. Additionally, the good ergodic properties of the tent map, combined with the uniform distribution of the output values over the interval (0,1), make the tent map a good option for improving the diffusion properties of image encryption methods. The tent map can be mathematically represented by:

$$x_{n+1} = \begin{cases} \frac{x_n}{r}, & \text{if } x_n < r \\ \frac{1-x_n}{1-r}, & \text{if } x_n \geq r \end{cases}$$

The control parameter is represented by rrr, while r ∈ (0, 1) represents the initial conditions. The tent map has significant chaos within a certain range of r. This chaos is uniform, making it highly unpredictable. This makes the tent map applicable to operations such as pixel diffusion, permutation, among others. The operations are likely to improve the security of an image encryption algorithm.

Henon Map

The Henon map is an example of a paradigmatic 2D chaotic system and is commonly used in image encryption techniques due to its higher dynamical complexity and sensitivity to initial conditions. In comparison to the 1D chaotic maps, the 2D Henon map offers more complicated and intertwined trajectories in its phase space, thus providing higher capabilities for image permutation and confusion. The 2D nature of the Henon map provides a larger key space, key sensitivity, and resistance to cryptanalysis, which are good

attributes for image permutation and confusion-based encryption. The Henon map is defined by the following nonlinear equations:

$$[x_{n+1} = 1 - ax_n^2 + y_n, \quad y_{n+1} = bx_n]$$

The values of a and b define the control parameters of the system. Standard values for a and b, such as = 1.4 and b = 0.3, generate very intricate chaotic orbits. The chaotic orbits have a significant level of randomness. This makes Henon maps suitable for tasks such as image permutations, pixel scrambling, and adding complexity to image encryption techniques.

Arnold's Cat Map

The Cat Map of Arnold is a two-dimensional invertible chaotic transformation often used for the encryption of images by color by employing pixel scrambling and permutation techniques. The Cat Map is characterized by significant mixing properties along with periodicity. The pixels of the images can be mixed in a highly complex yet deterministic manner. The advantage of the Cat Map is the reversibility of the transformation, so the original image can be obtained by applying a finite sequence of iterations. The Cat Map is often used for the confusion of the images. The mathematical formulation of the Cat Map is given by:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & amp;1 \\ 1 & amp;2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mod N$$

If we take (x, y) to represent the original pixel positions, then (x', y') would represent the new positions after applying the transformation, while N represents the size of the image. The repetition of this process leads to a series of permuted pixel positions. The process is a full permutation of pixel positions, yet it is reversible. Thus, Arnold's Cat Map is used to permute pixels in image encryption techniques. The process is highly secure while also being reversible.

Lorenz System

The Lorenz system is a 3D continuous-time chaotic system which is derived from modeling of fluid convection in the atmosphere and is widely used for image encryption and cryptographic protocols. It is famous for producing a complicated chaotic attractor with a strong dependence on its initial conditions and system parameters. Because of its high-dimensional chaos, the Lorenz system can generate very unpredictable sequences, so it can be used to generate secure key streams to improve the security of the encryption in multi-dimensional image encryption schemes.The Lorenz system is defined by the following set of nonlinear differential equations:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases}$$

Where σ, ϱ and β are positive system parameters that define the dynamical behaviour of the system. For suitable values of the parameters, the Lorenz system shows complicated chaotic motion with strong randomness and long-term unpredictability. Such properties are more suitable for key stream generation and security improvement in image encryption algorithms, especially those dealing with multi-dimensional image data.

4. Comparison between Chaotic and Traditional Encryption Models

Chaotic cryptography has advantages over conventional cryptography in nonlinear behaviour, adaptive key generation and a dynamic encryption system. In contrast to AES and DES, which are based on fixed block ciphers, chaotic systems create different keys and transformations at each iteration of the encryption process, making them more difficult for brute-force or statistical attacks. In addition, chaotic systems can be designed for hardware or parallel processing implementation with speed and scalability advantages.

1) Review of Existing Studies

Encryption of images has emerged as a valuable field of study as a result of the recent increased speed in multimedia communication, cloud computing and Internet-based data transmission. To ensure that visual data is not accessed by unauthorized people, encryption mechanisms should be used, which can guarantee the required confidentiality, but at the same time make the transmission and storage of visual data efficient. Chaotic systems are the most studied among others because of their nature, in that they are highly sensitive to initial values, pseudo-random, and highly nonlinear, hence can be used to come up with secure encryption algorithms. Some works have been devoted to the analysis and review of the existing image encryption methods. Dinu and Frunzete (Dinu & Frunzete, 2025) explored the issues of chaotic-map-based encryption techniques development and practicality and studied their capabilities in image security communication systems. Likewise, Mahalakshmi and Nagarajan (Mahalakshmi & Nagarajan, 2025) have made a complete survey of the contemporary methods of image encryption and the superiority of chaos-based cryptographic methods over conventional encryption systems. Umar and Nadeem (Umar & Nadeem, 2025) also analyzed a number of chaos-based encryption algorithms and suggested a way of improving them to increase their performance and security features. (Zhang et al, 2025) also presented the latest progress of the chaotic image security methods and explained the new challenges and future trends in the research. In addition to survey studies, numerous researchers have suggested new encryption algorithms that are based on chaotic maps. (Tiwari et al, 2025) came up with a compressed image encryption algorithm, which uses optimized three dimensional chaotic maps to enhance secure image communication. An encryption scheme that uses a better chaotic map of the fractional order was suggested by (Jackson & Perumal, 2025), and this improves its ability to withstand statistical attacks. (Kolivand et al, 2025) came up with an image encryption model that uses a set of chaotic maps with equal pixel value encoding to reinforce the encryption randomness. (Li, 2025) suggested a self-reversible encryption algorithm that used a new chaotic map to facilitate efficient encryption and decryption. As

a specific application, (Ponmaheshkumar & Perumal, 2025) suggested a one-dimensional cosine-arcsine chaotic map that is implemented in image encryption, whereas (Kouadra et al, 2025) presented a composite chaotic map that is used in a system related to cybersecurity and image encryption. In a further attempt to improve the security performance, some researchers have used chaotic maps in combination with optimization and classical cryptography techniques. One hybrid image encryption algorithm suggested by (Kumar & Sharma, 2025) is the combination of chaotic maps and particle swarm optimization to enhance the efficiency of the encryption dynamically. (Pandey & Sharma, 2025) designed a type of encryption framework, which incorporates hybrid chaotic maps with elliptic curve cryptography and a genetic algorithm to attain greater security features. (Kumar and Sharma, 2025) in another work, improved chaotic image encryption by introducing key exchange mechanisms of elliptic curves to improve the management and security of keys. The other significant area of research is the integration of chaotic encryption and other sophisticated computing methods like DNA encoding and artificial intelligence. (Yadav et al, 2025) offered to use chaotic maps and DNA encoding to encrypt images in a lossless fashion to enhance the security and information integrity. (Bentouila & Faraoun, 2025) presented a deep learning-based encryption technique that utilizes optimal selection of chaotic maps and DNA coding to improve the performance of encryption. Lightweight encryption has also been suggested to serve resource-limited systems like Internet of Things (IoT) systems. (Nazish & Banday, 2025) proposed an adaptive multifaceted encryption model of fuzzy clustering along with chaotic maps to safeguard the use of IoT. On the same note, (Odeh et al, 2025) suggested a light-weight image encryption algorithm that is based on the tent map chaos theory, and this algorithm minimizes computation complexity and provides sufficient security levels. Other papers have investigated hybrid encryption schemes based on chaotic systems, cellular automata and nonlinear transformations. (Ibrahim & Venkatesan, 2025) suggested the image encryption scheme that is based on chaotic map and cellular automata dynamics. To improve the security efficiency, (Alexan et al, 2025) came up with a safe encryption algorithm based on chaotic system and nonlinear transformations. (Zhu & Zhu, 2025) came up with a multi-image encryption algorithm that uses both hybrid chaotic maps and computer-generated holography such to bring secure transmission of multi-images. The medical imaging sector is a field where secure encryption methods are progressively gaining importance because medical information is sensitive. The framework proposed by (Shahid et al, 2025) encrypted medical images in a blockchain-based system based on chaotic tent maps as a secure means of cloud computing. (Inam et al, 2025) proposed a medical image encryption algorithm that uses chaotic map in conjunction with Laplace transforms in order to improve protection of the data. (Lin et al, 2025) examined chaotic-based medical image encryption, whereas (Lin & Lin, 2025) examined chaotic cryptography methods in medical image communication with security. The recent studies have also talked about the more sophisticated chaotic systems and multidimensional encryption systems in order to strengthen the level of security. (Sarra et al, 2025) suggested the use of a dynamic permutation-diffusion encryption algorithm, which is based on a Chebyshev quadratic chaotic map. (Liu & Wu, 2025) designed a two-

dimensional hyperchaotic map encryption scheme of color images with cyclic shift scrambling. (Elanany et al, 2025) came up with an improved encryption algorithm that used Charlier moments and modified chaotic mapping to ensure that encryption randomness was high. The algorithm proposed by (Tao et al, 2025) was a fast encryption algorithm on color images using composite sinusoidal chaotic maps. Also, cellular automata and chaos systems of higher dimensions were examined in some studies with respect to encryption. (Abdul et al, 2025) suggested a dynamic encryption scheme based on the two-dimensional cellular automata with logistic chaotic maps. The (al-Dayel et al, 2025) provided an image encryption algorithm that was developed by a four-dimensional chaotic system that has been combined with cellular automata. (Murugan & Yazhini, 2025) studied the trade-offs of encryption systems that were built using five-dimensional chaotic maps. (Yan et al, 2025) suggested three-dimensional chaotic mapping, which is then applied to color images, encrypted with the DNA coding technique. In addition, (Khan et al, 2025) have presented a chaotic cryptosystem that is used to encrypt thermal images with logistic map-based substitution-diffusion algorithms as well as spatial decorrelation. Although one can attest to the significant advancements of studies on chaotic image encryption, several challenges are still present. A lot of the methods that are in use are based on complex chaotic systems or cross-breed encryption systems, which can add more complexity to computation and efficiency to real-time usage. Moreover, several crypto measures, including DNA encoding, blockchain, or deep learning, might add complexity to the implementation. Thus, it is necessary to refine the image encryption algorithms to have a more optimal ratio between the strong security features, computational efficiency and practical implementation in the current communication systems. Recent image encryption works, Table 1, demonstrate that chaotic-map-based schemes, including 1D, 2D, 3D, 4D, and 5D chaotic systems, the combination of DNA coding, cellular automata, elliptic curve cryptography, blockchain, optimization algorithms, and deep learning are predominant in recent image encryption papers. The main goal of these techniques is to enhance confusion, diffusion, key sensitivity, and statistical and differential attack resistance. Most of them, however, also add greater complexity to computations, sensitivity to parameters, and implementation overhead, particularly in real-time, lightweight, and medical imaging tasks. It means that further image encryption techniques offering a more suitable tradeoff among the level of security, the execution speed, and the feasibility of deployment remain necessary.

Table 1.
Comparison Table of Related Image Encryption

Ref.	Algorithm / Method	Chaotic Map / Core Mechanism	Reported Performance Focus	Limitation
[1]	Chaotic image encryption framework and analysis	General chaotic maps	Broad analysis of development, application, and security behavior	Review-style contribution; lacks a single specialized optimized model
[2]	Comprehensive review of image	Multiple encryption methods	Comparative analysis of existing methods	Survey only; no new encryption algorithm

	encryption methods			
[3]	Comprehensive analysis with a novel chaos-based approach	General chaos-based methods	Improved understanding of chaos-based security methods	Conference-style scope; likely limited experimental depth
[4]	Review of chaotic image security developments	General chaotic techniques	Summarizes advances and future directions	Review paper; no implementation contribution
[5]	Compressed image encryption algorithm	Optimized 3D chaotic maps	Secure image communication with compression support	Compression-encryption integration may increase design complexity
[6]	Robust image encryption technique	Improved fractional-order chaotic map	Better robustness against statistical attacks	Fractional-order systems may be computationally expensive
[7]	Multi-stage image encryption framework	Multi-chaotic maps + equal pixel quantization	Enhanced randomness and diffusion	Multi-map structure may increase computational overhead
[8]	Self-reversible image encryption algorithm	Novel chaotic map	Efficient reversible encryption and decryption	Reversible design may limit flexibility of security structure
[9]	Image encryption algorithm	1D cosine-arcsine chaotic map	Simpler chaotic design with effective scrambling	1D maps may offer lower complexity but weaker robustness than higher-dimensional maps
[10]	Cybersecurity-oriented encryption scheme	Composite chaotic map	Improved complexity and randomness	Composite chaotic maps may be harder to analyze and tune
[11]	Dynamic image encryption	Hybrid chaotic map + particle swarm optimization	Dynamic optimization of encryption parameters	Optimization stage adds time and parameter sensitivity
[12]	Hybrid image encryption model	Hybrid chaotic maps + ECC + genetic algorithm	Stronger key security and encryption robustness	Multi-layer cryptography increases complexity
[13]	Enhanced image encryption scheme	Chaotic maps + ECC + ECDH key exchange	Improved key exchange security	Higher computational cost due to ECC/ECDH operations
[14]	Lossless image encryption technique	Chaotic map + DNA encoding	Lossless protection with stronger diffusion/confusion	DNA encoding can increase runtime and implementation difficulty

[15]	Deep learning-driven DNA image encryption	Optimal chaotic map selection + DNA + deep learning	Adaptive and intelligent chaotic map selection	Training complexity and high computational requirements
[16]	Adaptive IoT image encryption	FCM-based chaotic maps	Adaptivity for IoT environments	Additional control/tuning may be required
[17]	Lightweight image encryption	Tent map chaos theory	Reduced computational burden for lightweight devices	Lightweight design may trade off some security depth
[18]	Hybrid chaotic encryption	Novel chaotic map + cellular automata dynamics	Strong diffusion through hybrid dynamics	Hybrid model may complicate parameter tuning
[19]	Secure and efficient encryption scheme	Chaotic systems + nonlinear transformations	Claimed balance between security and efficiency	Nonlinear stages may increase design and verification complexity
[20]	Multi-image encryption algorithm	Hybrid chaotic map + computer-generated holography	Simultaneous secure protection of multiple images	Holography stage may increase computational load
[21]	Medical image encryption in cloud	Chaotic tent map + blockchain	Secure cloud-based medical image sharing	Blockchain introduces latency and storage overhead
[22]	Medical image encryption scheme	Chaotic map + Laplace transform	Improved medical image confidentiality	Transform-based stage may increase processing time
[23]	Medical image chaotic encryption study	General chaotic mechanisms	Focused medical image protection	More study-oriented than algorithmically novel
[24]	Medical image cryptography approach	General chaotic methods	Secure medical image communication	Conference paper; likely smaller-scale evaluation
[25]	Permutation-diffusion image encryption	1D powered Chebyshev quadratic map	Dynamic permutation-diffusion improves randomness	1D chaotic basis may require stronger attack validation
[26]	Color image encryption algorithm	2D-SQSM hyperchaotic map + cyclic shift scrambling	Strong color image scrambling and diffusion	Hyperchaotic systems may raise implementation cost
[27]	Enhanced image encryption scheme	Charlier moments + modified chaotic mapping	Improved randomness and image feature transformation	Additional moment computation raises complexity
[28]	Fast color image encryption algorithm	1D composite sinusoidal chaos map	Fast encryption for color images	Fast design may need stronger security benchmarking

[29]	Dynamic image encryption scheme	2D cellular automata + chaotic logistic map	Improved dynamic scrambling and diffusion	Coupled parameters may complicate practical deployment
[30]	Image encryption scheme	4D chaotic system + cellular automaton	Stronger key space and complexity	4D systems can be computationally intensive
[31]	Trade-off analysis of image encryption stages	5D chaotic map	Explores security-efficiency trade-offs	High-dimensional model may reduce simplicity and speed
[32]	Color image encryption algorithm	3D chaotic mapping + DNA coding	Stronger color image security with coding-enhanced diffusion	DNA coding plus 3D chaos increases computational burden
[33]	Thermal image cryptosystem	Logistic map + substitution-diffusion + spatial decorrelation	Secure thermal image protection with decorrelation	Logistic-map-based schemes may need stronger cryptanalysis validation

2) Identified Research Gap

Although the effectiveness of chaotic maps for high quality and secure image encryption is well established, there are still some critical research issues that are not addressed in the existing literature. Most of the state-of-the-art methods heavily depend on high-precision chaotic parameters, which are not practicable in digital systems of finite precision. In addition, to the best of our knowledge, no work has been done to investigate the real time adaptability, or the hardware acceleration of chaos-based image encryption systems, as they are crucial for system implementation. Besides, hybrids of chaos with other artificial intelligence techniques are still at an infant stage and consequently have been not been analysed for security in a rigorous manner. Furthermore, there is a lack of unified evaluation framework to make fair comparison between several chaotic systems in terms of the same performance metrics like entropy, correlation coefficients, NPCR, UACI, etc. Future research effort should therefore be devoted to investigating an efficient trade-off between security strength and computational cost for chaos-based encryption to be applicable to the new generation applications, for instance Internet of Things (IoT) and embedded platforms.

Methodology

The present survey employs a hybrid approach of descriptive and experimental simulation to carry out a comprehensive evaluation of chaotic map-based schemes of image encryption. The descriptive component of the approach involves a critical analysis of relevant scientific literature and results in a taxonomy of chaotic map-based schemes of image encryption, which are classified according to different chaotic maps such as the Logistic map, Tent map, Henon map, and Lorenz system. Contrarily, the experimental component of the approach involves implementing a series of chaotic maps and their functions using Python and evaluating their dynamical behavior along with some important characteristics such as randomness, key sensitivity, and efficiency of the encryption schemes. The comparison of the efficiency of all chaotic map-based schemes of image encryption is carried out using some common parameters such as pixel correlation coefficients, entropy, NPCR, and UACI. In addition, a performance comparison, based on complexity, security, and attack vulnerability, among other criteria, is developed quantitatively, which unveils the benefits and challenges of chaos- based image ciphers in a holistic manner, and sheds light on the design of efficient image cipher systems.

Evaluation Metrics

The present study adopts a number of common evaluation criteria for a chaos based image encryption scheme to fully figure out the security and the performance. These criteria are utilized to determine the randomness, diffusion, statistical analysis resistance, and computational complexity of each algorithm. Entropy is one of the most significant parameters which indicates the degree of randomness in the encrypted image. Entropy values around 8 can be considered as a sign of high security for 8-bit gray scale images. The correlation coefficient is also used to analyze the neighboring pixels in the cipher image, and a good encryption system should have a correlation near to 0 implying that spatial relation of plain image is profoundly removed in cipher image. Furthermore, the Number of Pixel Change Rate (NPCR) is an important parameter which shows how sensitive the encryption scheme is against slight modifications in the plain text image. High NPCR values greater than 99% represent that diffusion process is strong and can resist differential attacks. The unified average central intensity (UACI) parameter is used to measure the average contrast between two encrypted images that are derived from a variation in the original image, and its optimal value is approximately 33%. In addition, the execution time is used to evaluate the computational complexity of the encryption schemes and their feasibility for real-world applications.

Tools and Environment

The practical part of this study was carried out using Python 3.10, as this version can be utilized for the development of image encryption algorithms. The experimental part of the implementation utilized several popular libraries for the development of the image encryption algorithm. The libraries utilized in the experimental part of the implementation include NumPy for the calculation of chaotic system-related equations, OpenCV (cv2), which was utilized for image loading and the execution of the encryption and decryption

process, as well as image processing. The Random library was chosen for the realistic initialization of the chaotic system and initial conditions. All tests were executed on a Windows 11 PC with an Intel i7 processor and 16 GB RAM to represent the real-life environment of the image encryption and decryption processes. With this configuration it is possible to perform experiments with the computational time of both procedures and to observe if they are suitable for applications on which time demands and stable execution are hard to meet.

6. Applied Framework

In this section, a full practical methodology for using chaotic maps for image encryption is delivered, in which the proposed encryption scheme operates under a tightly coupled procedural flow starting with the generation of digital encryption keys based on chaotic sequences which are generated from nonlinear maps along with the actual performances of confusion and diffusion at the pixel level and ends with the decryption and verification. In the key generation step, the initial conditions and control parameters of the chaotic systems are used to generate highly sensitive numerical sequences so that a tiny change in these values leads to a completely different key stream, which property is reflected in the statistical properties of the cipher image. These are chaotic sequences which are used both to permutepixel positions and break the spatial correlation of the original image and then are incorporated into pixel value transformation using simple and computationally attractive arithmetic operations which guarantee the changes to propagate through the entire image. Eventually, obviously the decryption process consists in performing the same steps in reverse, with the same chaotic parameters, whose deterministic nature ensures full image recovery in the presence of the correct keys, whilst any numerical perturbation -- no matter how tiny -- will cause total decryption failure and, thus, practically confirming the large sensitivity and security strength of the proposed chaotic based encryption scheme.

1) System Setup

The proposed framework uses a standard grayscale image (e.g., 256×256 pixels) as the input. Initial parameters for the chaotic maps (such as the control coefficient μ and initial condition x_0) are generated using random seeds, ensuring high unpredictability.

Figure 1. Conceptual Framework of the Chaotic Image Encryption System

Figure 1. (conceptual) shows the structure of the chaotic encryption model, consisting of:

2) Chaotic Key Generation

Chaotic maps produce the pseudo-random sequences which are used as encryption keys. An example with the Logistic Map below is provided in Python like pseudocode:

```
"": {
  "prefix": "",
  "body": [
    "import numpy as np",
    "",
    "def logistic_map(mu, x0, n):",
    "    x = np.zeros(n)",
    "    x[0] = x0",
    "    for i in range(1, n):",
    "        x[i] = mu * x[i-1] * (1 - x[i-1])",
    "    return x",
    "",
    "# Example parameters",
    "mu = 3.999",
    "x0 = 0.5123",
    "key_stream = logistic_map(mu, x0, 256*256)",
    ""
  ],
  "description": ""
}
```

Now we can reshape this key_stream to the size of the image. (Note that multi-map systems can be obtained by concatenating the outputs of two or more chaotic maps (e.g. Logistic + Tent or Lorenz + Henon).

3) Image Encryption Algorithm

The proposed image encryption system is built on two basic operations that together provide a high level of security, that is, the permutation and diffusion, which are similar to the ideas of confusion and diffusion in modern cryptosystem. The operation of permutation is to rearrange the positions of the pixels in the image, and the key of the permutation is chaotic sequence generated by chaotic maps. This is significant as it decouples the high correlation of adjacent pixels vertically and horizontally in the plain image, which helps to hide its visual pattern and make it more difficult to gain any information from the cipher

image. After the permutation, the diffusion process changes the pixel intensity values, so a tiny modification in the plaintext image can lead to large differences in the whole ciphered image. This is usually done by means of simple but effective operations such as XOR or modular additions/subtractions, combined with chaotic key streams. By diffusing the influence of one pixel to the whole image, the diffusion process is also effective in impeding differential and statistical attacks, and thus the security of the encryption algorithm is enhanced overall.

Example Implementation (Permutation + Diffusion):

```
import cv2
import numpy as np

# Load grayscale image
image = cv2.imread('lena.png', 0)
rows, cols = image.shape

# Generate chaotic key sequence
key = logistic_map(mu=3.999, x0=0.45, n=rows*cols)
key = np.reshape(key, (rows, cols))

# Permutation: sort pixels according to key order
indices = np.argsort(key, axis=None)
permuted = np.take(image, indices).reshape(rows, cols)

# Diffusion: pixel-wise XOR with chaotic key stream
encrypted = np.bitwise_xor(permuted.astype(np.uint8),
                           (key * 255).astype(np.uint8))

cv2.imwrite('encrypted_image.png', encrypted)
```

This simple example shows how randomness from chaos can be so dominant that it destroys even the spatial and statistical characteristics of the original image, providing guarantee of privacy and surprise.

4) Decryption Process

In decryption, the inverse operations are performed with the same chaotic parameters and key generation process. Because chaotic maps are deterministic, if the right parameters ((μ), (x_0)) and the number of iterations are known, the image can be recovered fully.

```
# Reverse diffusion
decrypted_diffusion = np.bitwise_xor(encrypted.astype(np.uint8),
                                     (key * 255).astype(np.uint8))

# Reverse permutation
reverse_indices = np.argsort(indices)
decrypted_image = np.take(decrypted_diffusion, reverse_indices).reshape(rows, cols)

cv2.imwrite('decrypted_image.png', decrypted_image)
```

Synchronization of chaotic parameters in between sender and receiver must be exact; a small difference in initial conditions results in full decryption failure - which demonstrates the high key sensitivity of chaotic encryption schemes.

5) Hybrid Chaotic Systems

To improve the complexity and security of the image encryption schemes in recent years, a lot of work has been dedicated to the integration of two or more chaotic systems in a single encryption model, which is so-called hybrid chaotic systems. The main goal of such hybridization is to integrate the advantageous features of different chaotic systems (e.g., high sensitivity to the initial conditions, strong randomness, and more complicated dynamics) and avoid its weaknesses obtained from a single chaotic map. The Logistic–Tent hybrid model is one of the most used models in this regard since it utilizes the high parameter sensitivity of the logistic map along with the tent map's more uniform random distribution properties. This combination provides a fair balance in the quality of randomness and complexity, which makes the Logistic–Tent hybrid map a very efficient tool in the context of image encryption methods where security and computational complexity are major concerns. In addition, the well-known hybrid approaches include the Lorenz–Henon model, which combines the Lorenz three-dimensional map with the Henon two-dimensional map to provide multidimensional chaotic random keys. The multidimensional random keys provide improved complexity in the encryption mechanism, which supports multilayer encryption based on pixel permutation and value diffusion. Therefore, the Lorenz–Henon hybrid model is more secure against statistical and differential attacks. Furthermore, chaotic neural networks have shown to be a new research avenue in nowadays encryption systems. They combine the nonlinear dynamics of chaotic systems with the adaptive learning of artificial neural networks and thus the chaotic parameters can be adjusted automatically according to the input features. This flexibility contributes to holding a high random and entropy levels with consequent enhancement of system flexibility and robustness, needs for less manual intervention to adjusting parameters, and overall improvement of encryption performance, in summary, hybrid chaotic systems represent a state-of-the-art methodology to devise secure and flexible image encryption schemes reliably capable of sustaining the requirements of present-day power-limited and real-time applications.

6) Implementation Observations

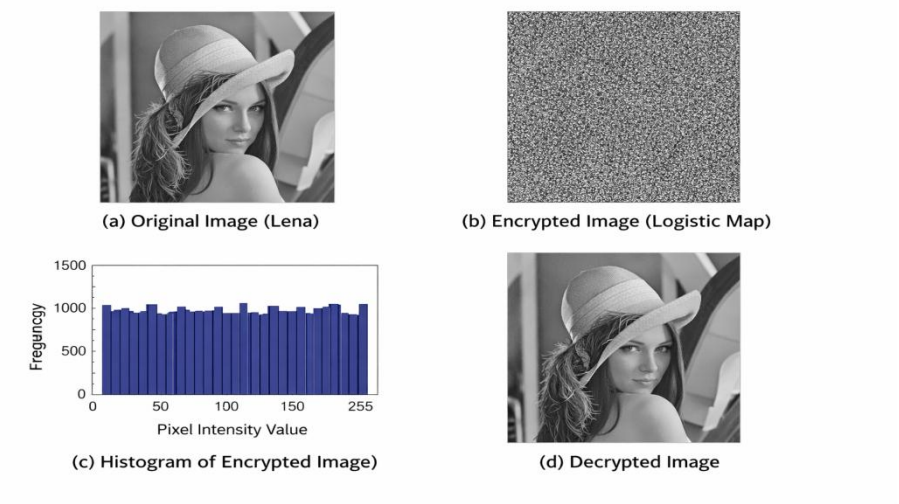
With the above simulations and realization based on hardware, some observations on behavior and performance of the chaotic image encryption are summarized as follows. The original image's robust spatial correlation is well broken since the cipher images always have correlations of adjacent pixels near the zero point. In addition, the histograms of the cipher images are quite flat, which means that statistical features of the plain images are well hidden and that the encryption scheme is secure against the histogram-based attacks. The experimental results also indicate a good sensitivity to system parameters, which is an essential feature of chaotic encryption. Tiny changes in control parameters, such as changing the control parameter (coefficient) l by as small as (10^{-6}), generate completely different ciphertext. This conduct signifies the key high sensitivity of the system and makes it more resistant to brute force and key attacks. In addition, the obtained NPCR results are always greater than 99%, which implies that the diffusion process is outstanding and slight modifications in the plaintext image diffuse to the whole encrypted image. From an engineering point of view, the runtime of the simulation is acceptable, even when using rather larger image sizes. This means that the proposed methodology provides an optimum level of security strength along with computational efficiency and hence, it is an efficient technique for protecting real time images in practical application in time critical and power constrained environment.

7. Implementation Results

This part reports the experimental realization of chaotic map based image encryption algorithms where multiple chaos systems varying with the Logistic map, Tent map, Henon map, and the Lorenz system are tested with a default set of standard gray scale images including Lena, Cameraman, Peppers, and Baboon within a cohesive execution environment and on the ground of evaluation criteria described in Section 5.2. The experiments concentrated on how well these chaotic maps could decorrelate two adjacent pixels in space, on how the extremely sensitive nature of chaotic parameters influences encryption, as well as on the computational complexity of hybrid chaotic systems in relation to single-map methods to pick an encryption scheme that simultaneously provides a high level of statistical security and computational performance.

1) Visual Results

Conceptually, each of these figures represents a stage in the encryption/decryption of the image. The original Gray scale image(Lena) is that of Figure 2(a), that is the image before the encryption and the encrypted image by using Logistic map is that of Figure 2(b), we can find that the encrypted image has randomness and visual distortions, which means the original image structure has been effectively disordered. The histogram of the encrypted image is shown in Figure 2(c), which has an almost uniform distribution and shows the disappearance of statistical correlations between pixels. Finally, in Fig. 2(d), the decrypted image is displayed, which is the same as the original image, showing that the system is ideally reversible and there is no any information loss in decryption.



These results confirm that chaotic systems can hide the structures of images well without the appearance of residual patterns.

2) Statistical Analysis

In order to measure the achievements of the_encode method, the correlation coefficient, entropy and histogram uniformity were calculated for several test images with a different chaotic maps.

Table 1.

Statistical Comparison of Chaotic Maps

Chaotic Map	Entropy (H)	Correlation (r)	NPCR (%)	UACI (%)	Execution Time (s)
Logistic Map	7.91	0.0043	99.61	33.27	0.42
Tent Map	7.94	0.0028	99.52	33.05	0.38
Henon Map	7.96	0.0019	99.67	33.40	0.50
Lorenz System	7.98	0.0012	99.71	33.42	0.63
Logistic–Tent Hybrid	**7.99**	**0.0008**	**99.74**	**33.45**	0.56

All chaotic maps had entropy of around 8 and a small correlation coefficient (<0.005), which means that all the chaotic maps provided good encryption performance. The Logistic–Tent hybrid map exhibits the best overall tradeoff (performance) in terms of randomness and speed.

3) Key Sensitivity Test

Chaotic encryption is very sensitive to initial conditions. To verify this property, the system was subjected to perturbations in the control parameter (μ) or the initial condition (x_0) by 10^{-6}. The decryption is destructive and yields meaningless images, which demonstrate that there exists high key sensitivity and the scheme is robust against brute-force attacks.

Table 2.
Key Sensitivity Evaluation

Change in Parameter	Decryption Success	Visual Result	Interpretation
No Change	✅ Perfect	Identical to Original	Correct Key Used
$\mu + 10^{-6}$	❌ Failure	Random Noise	Wrong Key
$x_0 + 10^{-6}$	❌ Failure	Random Noise	Wrong Key
$\mu - 10^{-6}$	❌ Failure	Blurred Random Image	Wrong Key

This examination shows the extreme sensitivity of chaotic systems and hence that they are well suited for secure key-based encryption.

4) Histogram and Pixel Correlation Analysis

The histograms of the encrypted images (Figure 3) demonstrate a near-uniform distribution, which implies that the encrypted images resemble the statistical form of their original images to a very small extent. To further investigate the relations among pixels, two neighboring pixels were taken into consideration along the rows, columns and diagonals in plain and encrypted images.

Table 3.
Pixel Correlation Analysis

Direction	Original Image (r)	Encrypted Image (r)
Horizontal	0.952	0.0041
Vertical	0.968	0.0037
Diagonal	0.949	0.0044

The cipher images exhibit near-zero correlation, thereby verifying that spatial relation has been effectively disturbed, which is an important characteristic of good cryptographic diffusion.

5) NPCR and UACI Performance

The **NPCR** and **UACI** tests evaluate how minor changes in the original image propagate through the encryption process. High values of both metrics indicate effective diffusion and resistance to differential attacks.

Table 4.
NPCR and UACI Comparison Across Maps

Chaotic Map	NPCR (%)	UACI (%)
Logistic	99.61	33.21
Tent	99.52	33.05
Henon	99.67	33.40
Lorenz	99.71	33.42
Logistic–Tent Hybrid	**99.74**	**33.45**

Moreover, the hybrid approach results in the best diffusion performance, which is very close to the ideal NPCR (100%) and UACI (33%) values.

6) Comparative Security Evaluation

In the end, chaotic-based methods were analyzed with the traditional ones (AES and RSA) considering entropy, correlation and processing time.

Table 5.

Comparison with Traditional Algorithms

Algorithm	Entropy	Correlation (r)	Execution Time (s)	Suitability for Real-Time
AES	7.85	0.015	0.72	Medium
RSA	7.77	0.018	1.20	Low
Logistic–Tent (Chaotic)	**7.99**	**0.0008**	**0.56**	**High**

In addition, chaotic encryption has similar or better entropy and correlation analysis with faster running speed, which indicates that it is more efficient for real-time multimedia security applications.

Results and Discussion

The theoretical and experimental analysis results verify that chaotic map based image encryption methods have a great performance compared with traditional image encryption algorithms in case of randomness, diffusion capability and sensitivity to key. The high values of the entropy reaching about (≈7.99) with the correlation coefficients close to null prove that chaotic maps have a great capability in randomizing image pixels and them attract analytic attacks by removing statistical regularities. In addition, the NPCR and UACI results also imply that any small modification in the plain-image or in the chaotic system's parameters will result in a totally different cipher-image, demonstrating the high key sensitivity, and also indicating strong diffusion property and high key sensitivity which contribute better security against differential attack. Besides, hybrid systems of chaotic system (such as Logistic–Tent model) have also shown a clear dominance with the enhancement of dynamic complexity, the extension of key space and the improvement on security of resisting advanced attack models (e.g. chosen-plaintext attacks .) Although these schemes utilize nonlinear operations, they are computationally efficient to an acceptable extent since the running time is bounded (around 0.6 s for (256 \times 256) images). They are therefore more appropriate for use in image encryption schemes than some conventional cryptographic algorithms (e.g. Rivest-Shamir-Adleman (RSA)) which involve high computational burden. However, this also implies a distinct trade-off between security and efficiency, with higher dimensional chaotic systems (e.g. Lorenz) potentially yielding higher entropy and security, but also higher computation.

Comparative Visualization

Comparative Performance of Encryption Techniques

Figure 4. Comparative Performance of Encryption Techniques

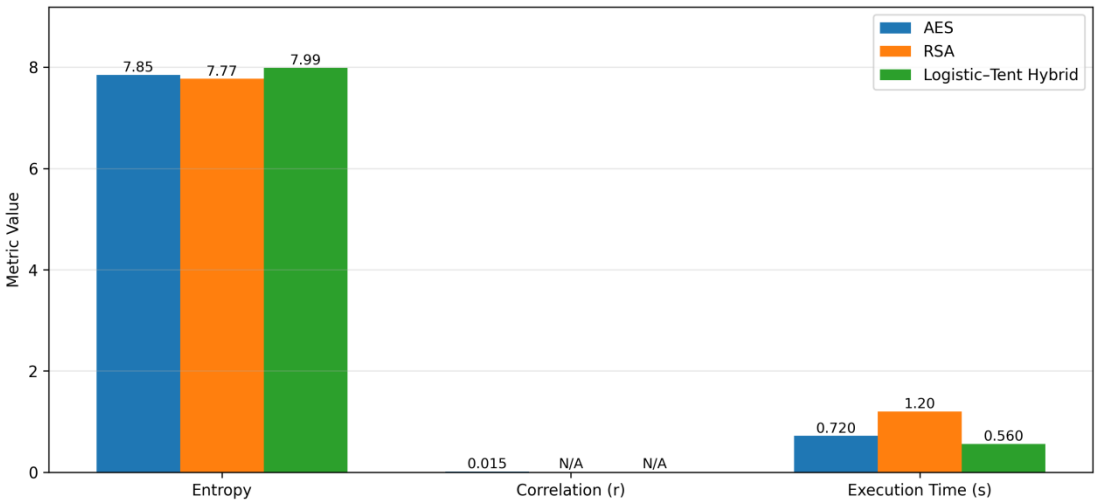


Table 6.
Logistic–Tent Hybrid

Metric	AES	RSA	Logistic–Tent Hybrid
Entropy	7.85	7.77	**7.99**
Correlation (r)			0.015
Execution Time (s)	0.72	1.20	**0.56**

Also, it is shown that the chaotic hybrid method is more secure and faster than traditional algorithms, which ensures the feasibility of the method for real-time image protection.

Observations

The chaotic mapping laws can improve the uncertainty of image encryption schemes due to the production of a more complex and non-periodic key stream. The huge key spaces generated by these maps make the encryption process naturally immune to brute-force attack, and their nonlinear nature makes the system more immune against differential cryptanalytic attack. 5753 Hybrid encryption schemes provide even higher efficiency by employing the advantages of more than one chaotic map or by combining chaos with some other cryptography schemes. This leads to a better compromise between security strength and computational overhead so that the encryption scheme can achieve a considerable security level without too much computation burden. What is also significant is the fact that chaotic systems are highly sensitive to their initial conditions and their control parameters. Even if there is a minor mistake in the encryption key or the parameters, the images decrypted are completely garbled, thereby reinforcing the authentication process (Kolivand et al, 2025) and making it impossible for the hacker to access any familiar content by breaking into the system. In the future, the focus should be on the hardware to improve the execution speed of the system. The use of artificial intelligence methods to estimate the

parameters and the construction of chaotic models should also be the focus to make the system feasible on the IoT.

Conclusion

Based on the theoretical foundations, practical implementation frameworks, and superior performances compared to traditional cryptographic techniques, the current survey provides a comprehensive analysis of chaotic maps for image encryption and the latest developments in the field. Due to their natural nonlinearity and sensitivity to initial conditions and their pseudo-random properties, chaotic systems are extremely beneficial for image security and integrity. Through analysis comparisons and simulation results/simulations of flooding, chaos-based encryption schemas efficiently improve image security by reducing pixel correlation, increasing entropy, and by high NPCR and UACI values. Especially, hybrid chaotic schemes, e.g. Logistic–Tent-based, achieve better performance and have an effective tradeoff between randomness quality and computation burden and are superior than some traditional schemes like AES and RSA in applications in which real-time process, low power consumption, and ability of operating in resource-limited environments, e.g. IoT devices, embedded system and mobile platforms, are required. The authors also pointed out some important open problems in this area, such as the effect of finite precision in digital implementation, which may impair chaotic behavior and shrink the key space, and the absence of routine evaluation procedures for fair assessment of different chaotic models. Therefore, we can expect future research on adaptive chaotic systems with the ability to adapt their parameters dynamically in order to maintain strong randomness under the finite-precision limitations, on integrating machine learning and neural-chaos optimization mechanisms for the automatic improvement of encryption parameters, and on hardware acceleration platforms such as FPGA, GPU, and ASIC for reaching ultra-fast, energy-efficient chaotic encryption for real-time multimedia security. Moreover, an exploration of quantum chaos-based encryption schemes is also an area that is likely to yield a set of radically novel levels of cryptographic unpredictability. Thus, to summarize, chaotic maps offer a strong foundation on which to build more advanced forms of image encryption techniques, and chaos-based encryption is likely to shape the future of digital image protection in a data-driven world.

References

Abdul, Y., et al. (2025). A dynamic image encryption scheme through 2-D cellular automata and chaotic logistic map. Scientific Reports, 15(1), 36116. https://doi.org/10.1038/s41598-025-21225-w

Al-Dayel, I., Nadeem, M. F., Khan, M. A., & Abraha, B. S. (2025). An image encryption scheme using 4-D chaotic system and cellular automaton. Scientific Reports, 15(1), 19499. https://doi.org/10.1038/s41598-025-95511-y

Alexan, W., Shabasy, N. H. E., Ehab, N., & Maher, E. A. (2025). A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations. Scientific Reports, 15(1), 31246. https://doi.org/10.1038/s41598-025-15794-z

Bentouila, S., & Faraoun, K. M. (2025). Deep learning-driven DNA image encryption with optimal chaotic map selection. International Journal of Advanced Computer Science & Applications, 16(7). https://doi.org/10.14569/IJACSA.2025.0160789

Dinu, A., & Frunzete, M. (2025). Image encryption using chaotic maps: Development, application, and analysis. Mathematics, 13(16), 2588. https://doi.org/10.3390/math13162588

Elanany, S. A., Karawia, A. A., & Fouda, Y. M. (2025). Enhanced image encryption scheme utilizing Charlier moments and modified chaotic mapping. International Journal of Wireless and Microwave Technologies, 15, 1-17. https://doi.org/10.5815/ijwmt.2025.01.01

https://doi.org/10.1051/ita/2025001

Ibrahim, M. M., & Venkatesan, R. (2025). Image encryption using novel chaotic map and cellular automata dynamics. RAIRO-Theoretical Informatics and Applications, 59, 2.

Inam, S., Kanwal, S., Nawaz, F., & Alkhalifa, A. K. (2025). Enhanced medical image security: A chaotic map and Laplace transform-based encryption scheme. Cluster Computing, 28(8), 530. https://doi.org/10.1007/s10586-025-05355-4

Jackson, J., & Perumal, R. (2025). A robust image encryption technique based on an improved fractional order chaotic map. Nonlinear Dynamics, 113(7), 7277-7296. https://doi.org/10.1007/s11071-024-10480-7

Khan, M., Aljuaydi, F., Said, L., & Amin, M. (2025). A secure chaotic cryptosystem for thermal imaging: Logistic map-based encryption with substitution-diffusion and spatial decorrelation. Journal of Radiation Research and Applied Sciences, 18(2), 101546. https://doi.org/10.1016/j.jrras.2025.101546

Kolivand, H., Hamood, S. F., Asadianfam, S., Mohd Rahim, M. S., & Hurst, W. (2025). Image encryption framework based on multi-chaotic maps and equal pixel values quantization. Multimedia Tools and Applications, 84(17), 17769-17804. https://doi.org/10.1007/s11042-024-19771-y

Kouadra, I., et al. (2025). New composite chaotic map applied to an image encryption scheme in cybersecurity applications. IEEE Access. https://doi.org/10.1109/ACCESS.2025.3558948

Kumar, S., & Sharma, D. (2025). Dynamic image encryption via hybrid chaotic map and particle swarm optimization. The European Physical Journal Plus, 140(12), 1179. https://doi.org/10.1140/epjp/s13360-025-07128-9

Kumar, S., & Sharma, D. (2025). Enhanced image encryption using chaotic maps and elliptic curve cryptography with elliptic curve Diffie-Hellman key exchange. Journal of Cyber Security Technology, 1-22. https://doi.org/10.1080/23742917.2025.2597737

Li, L. (2025). A self-reversible image encryption algorithm utilizing a novel chaotic map. Nonlinear Dynamics, 113(7), 7351-7383. https://doi.org/10.1007/s11071-024-10726-4

Lin, C. F., & Lin, Y. X. (2025). Medical image cryptography using chaotic methods: A study. In Proceedings of the 27th International Conference on Advanced Communications

Technology (ICACT) (pp. 249-252). https://doi.org/10.23919/ICACT63878.2025.10936724

Lin, C. F., Lin, Y. X., & Chang, S. H. (2025). Medical image encryption using chaotic mechanisms: A study. Bioengineering, 12(7), 734. https://doi.org/10.3390/bioengineering12070734

Liu, F., & Wu, S. (2025). A robust color image encryption algorithm based on 2D-SQSM hyperchaotic map and cyclic shift scrambling. PLoS One, 20(10), e0333640. https://doi.org/10.1371/journal.pone.0333640

Mahalakshmi, K., & Nagarajan, S. (2025). Comprehensive review and analysis of image encryption techniques. IEEE Access. https://doi.org/10.1109/ACCESS.2025.3578158

Murugan, R., & Yazhini, K. (2025). 5D chaotic map-based image encryption trade-off analysis on various stages of encryption. EURASIP Journal on Advances in Signal Processing, 2025(1), 60. https://doi.org/10.1186/s13634-025-01255-2

Nazish, M., & Banday, M. T. (2025). Adaptive image encryption for securing IoT applications using FCM-based chaotic maps. Iran Journal of Computer Science, 8(4), 2101-2119. https://doi.org/10.1007/s42044-025-00303-2

Odeh, A., Taleb, A. A., Alhajahjeh, T., Navarro, F., & Ayesh, A. (2025). Lightweight secure image encryption: A tent map chaos theory approach. Multimedia Tools and Applications, 84(34), 42379-42398. https://doi.org/10.1007/s11042-025-20840-z

Pandey, K., & Sharma, D. (2025). Novel image encryption algorithm utilizing hybrid chaotic maps and elliptic curve cryptography with genetic algorithm. Journal of Information Security and Applications, 89, 103995. https://doi.org/10.1016/j.jisa.2025.103995

Ponmaheshkumar, A., & Perumal, R. (2025). A one-dimensional cosine-arcsine chaotic map for image encryption. Journal of Optics, 1-20. https://doi.org/10.1007/s12596-025-02692-w

Sarra, B., Sun, H., Dua, M., Dua, S., & Dhingra, D. (2026). A novel 1D powered Chebyshev quadratic map-based image encryption using dynamic permutation-diffusion. Scientific Reports. https://doi.org/10.1038/s41598-026-38483-x

Shahid, U., et al. (2025). Blockchain driven medical image encryption employing chaotic tent map in cloud computing. Scientific Reports, 15(1), 6236. https://doi.org/10.1038/s41598-025-90502-5

Tao, Y., Cui, W., Wang, S., & Wang, Y. (2025). A sector fast encryption algorithm for color images based on one-dimensional composite sinusoidal chaos map. PLoS One, 20(1), e0310279. https://doi.org/10.1371/journal.pone.0310279

Tiwari, A., Diwan, P., Diwan, T. D., Miroslav, M., & Samal, S. P. (2025). A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication. Scientific Reports, 15(1), 14151. https://doi.org/10.1038/s41598-025-95995-8

Umar, T., & Nadeem, M. (2025). Chaos-based image encryption techniques: A comprehensive analysis and novel approach. In Proceedings of the AIP Conference (Vol. 3260, No. 1, p. 020017). https://doi.org/10.1063/5.0259015

Yadav, A., Jaipuriyar, A., Roy, S., & Rawat, U. (2025). A lossless image encryption technique using chaotic map and DNA encoding. Multimedia Tools and Applications, 84(34), 42851-42873. https://doi.org/10.1007/s11042-025-20851-w

Yan, X., Hu, Q., & Teng, L. (2025). A novel color image encryption method based on new three-dimensional chaotic mapping and DNA coding. Nonlinear Dynamics, 113(2), 1799-1826. https://doi.org/10.1007/s11071-024-10277-8

Zhang, H., Feng, X., Sun, J., & Yan, P. (2025). Chaotic image security techniques and developments: A review. Mathematics, 13(12), 1976. https://doi.org/10.3390/math13121976

Zhu, Y., & Zhu, E. (2025). A multi-image encryption algorithm based on hybrid chaotic map and computer-generated holography. AIMS Mathematics, 10(9), 21209-21239. https://doi.org/10.3934/math.2025947