Journal of Basrah Researches (Sciences) **52**(1), 270 (2026)
DOI: https://doi.org/10.56714/bjrs.52.1.19

Chaotic Systems encryption, a review

Y. H. Ismaiel

Department of Computer Sciences, College of Computer Sciences and Mathematics, University of Mosul

ARTICLE INFO

Received 03 May 2026
Revised 06 June 2026
Accepted 11 June 2026
Published 30 June 2026

Keywords:

Chaotic Systems Encryption, Visual Data, Multimedia Security, Confusion, Diffusion.

Citation: Y. H. Ismaiel., J. Basrah Res. (Sci.) **52**(1), 270 (2026). DOI:https://doi.org/10.56714/bjrs.52.1.19

ABSTRACT

The continuous advancement of communication technologies and data exchange over public networks has highlighted the crucially of protecting sensitive digital images and countering growing security threats. Traditional encryption methods such as RSA and AES face significant challenges when applied to digital images due to the large datasets and high correlation between adjacent pixels. This research presents a comprehensive overview of many digital image encryption algorithms that combine multidimensional chaotic systems (such as 2D Logistic-Sine-coupling maps) with dynamic DNA computing techniques. Another approaches combines hyper-chaotic systems with compressive sensing to achieve simultaneous encryption and compression while providing visual security, also group of researchers proposed several ideas for encrypting digital images based on integrating Dynamic Spatial Chaos theory with modern models of Deep Learning and Edge Computing. Most of the proposed methodologies involve two main phases: permutation and diffusion, in the permutation phase, random sequences generated by the chaotic system are used to shuffle pixel positions across the entire image, breaking spatial correlation, while in the diffusion phase, pixels are converted into DNA sequences, and logical and arithmetic operations (such as addition, subtraction, and XOR) are applied based on DNA coding rules, significantly altering the pixel values. The results of experimental simulations and comprehensive security analysis showed that most of the proposed algorithms possess a very high level of security and a large key space, thus thwarting brute-force attacks. Statistical analysis also showed that the correlation coefficient between pixels in the encrypted image is close to zero, and the information entropy value is very close to the ideal value of 8. These algorithms demonstrated excellent resilience to differential attacks as measured by the NPCR and UACI values. Of course, every algorithm has its own advantages and characteristics depending on the application and research objective. Likewise, there are a number of limitations or weaknesses that these algorithms face, the most important of which are time and cost, as explained in the body of the research.

***Corresponding author email:** yaseen-hikmat@uomosul.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq

1. Introduction

With the rapid development of communication technologies and the increasing reliance on open networks for exchanging visual data, protecting sensitive digital images has become a critical challenge, due to the inherent characteristics of digital images, such as their large data capacities and the strong correlation between adjacent pixels, traditional encryption algorithms have proven inadequate in meeting both speed and security requirements, therefore chaotic systems have emerged as one of the most effective and efficient solutions in the field of multimedia security [1].
Chaotic functions or systems are defined as dynamic, deterministic, and nonlinear systems characterized by their complex and unpredictable long-term behavior. Their strength in cryptographic applications derives from their perfect conformity to the requirements of strong encryption, relying on several mathematical principles, most notably: high sensitivity to initial conditions, which ensures a large key space; ergodicity, which guarantees a random distribution of data; and pseudo-randomness. Chaotic systems have gradually evolved from simple one-dimensional (1D) maps [5] to hyper-chaotic systems and spatial-temporal chaos systems, which offer greater dynamic complexity and higher levels of security that resist mathematical analysis [3], [16], [47].
The dynamic attributes of chaos are consistent with Shannon's principles of entropy and diffusion for designing strong encryption systems. Most recent chaotic encryption methods rely on a shuffling and diffusion structure that is deployed through advanced chaotic mechanisms across two stages:

1. Permutation: The goal of this stage is to compromise the spatial correlation between neighboring pixels in a way that does not change their color values but rather randomizes their positions [4, 25].
2. Diffusion: Pixel values are adjusted by combining them with complex chaotic sequences, so that a subtle modification in a single pixel within the source image yields a significant effect that impacts most of the pixels in the encoded image [17, 26].

This structural design was not limited to purely mathematical chaos alone, but Incorporated innovative hybrid techniques, marking a quantum leap. DNA-based computing techniques are among the most noteworthy of these [2], [7], [18], Encryption is performed by treating pixels as nitrogen atoms and applying dynamic algebraic operations relying on chaotic sequences to them. This increases the system's intricacy and frustrates differential attacks [21], [29].
Among the key competitive advantages that make chaotic systems the prioritized choice for digital image encoding in recent research are the following:

• Superior statistical security: These systems generate encrypted images with a bit information entropy of 8—the optimal value—which eliminates any visual or statistical patterns that an attacker could detect and leverage [9], [13].
• Algorithmic efficiency and speed: Chaotic maps generate long encryption keys much more quickly and using minimal computational resources compared to traditional cryptographic methods, making them optimal for real-time usage [8, 37].
• Exceptional synthesis adaptability: Chaotic systems are characterized by their high compatibility with supporting technologies such as data compression to reduce data volume while encrypting it in real time [28], as well as with deep learning mechanisms to develop a self-adjusting and intelligent cryptography systems [44, 50]. With this development, research has surpassed the constraints of basic encryption designs but has expanded to include more complex research avenues to meet the demands of contemporary technology. Among the most prominent of these trends are: Smart Healthcare, Internet of Things (IoT), Blockchain and Decentralized Trust [23, 47,48,49]. This research reviews a selection of the most important recent studies in this field, highlighting key ideas, the advantages of these methods, and the obstacles and limitations researchers have encountered in terms of both efficiency and security.

2. Related Work

As we explained previously, the related studies were selected to encompass most of the methods and ideas used by researchers to present an efficient encryption method based on the chaotic function. To simplify the review process, we relied on their recency, from oldest to newest, and considered 2018 as the starting year for reviewing these studies.

Hua et al., addressing the problem in one-dimensional chaotic maps that these simple maps have a narrow chaotic range and suffer from an irregular probability density distribution, making them easily predictable statistically. They proposed a novel two-dimensional chaotic map "2D Sine Logistic Modulation Map (2D-SLMM)", two single-maps (sine and logistic) are combined in such a way that the output of one affects the other. the sequences generated from the new 2D-SLMM map are used to rearrange pixel positions, which offers high randomness resulting from the larger Lyapunov exponent, which translates to faster path divergence. The proposed method has wide chaotic Range, good statistical performance; but suffering from floating-point accuracy impact so, the security is highly dependent on computer precisionand limited structural complexity because depending on a single map function [1].

Combining a memristive chaos system with DNA coding by chai et al. A memristor is a fourth electrical component (along with capacitors, resistors, and inductors) that possesses internal memory for generating highly four distinct complex chaos. The method consists of multi-stages: First, the chaotic system is used to generate an initial mask. Second, the digital image is converted into DNA sequences using (A=00, T=11, C=10, G=01), dynamically the coding rule for each pixel is selected based on the chaos sequence. Third, specific DNA algebraic operations are performed between the image sequences and the randomly key sequences. Fourth, the result is converted back into a digital format. The challenges of this method are difficulties of hardware implementation in addition to computational complexity [2].

Integrating genetics with hyper-chaotic systems by wang and zhang to produce new image encryption method. The idea is to apply the principles of genetic recombination and mutation at the bit level of the image, using a 4D hyper-chaotic system, characterized by the presence of more than one positive Lyapunov exponent, making it more complex and unpredictable than lower-dimensional systems. The method decomposing the image into bit-planes, then chaotic sequences are then used to identify crossover points between different bit-planes, much like gene exchange between chromosomes. Next, a random "mutation" is applied based on a specific chaotic condition. These combining the processes of confusion and propagation into a single complex step. The method characterized by Bit-level encryption, high security and Strong resistance to differential attacks [3].

Li and Chen enhancing the efficiency of the permutation phase combining two levels of permutation: pixel-level and bit-level, driven by a 5D hyper-chaotic system, which changes both values and positions. The mechanism involves two overlapping stages: First, the hyper-chaotic system is used to generate new pixel coordinates, Second, a special algorithm is implemented to swap bits within each pixel and between adjacent pixels. The "interconnected diffusion" encoding of each pixel relies not only on the preceding pixel but also on a cumulative value derived from the chaotic sequence. Data loss tolerance and fast security by removing spatial and chromatic statistics, but this method suffer from memory management complexity [4].

Pak and Huang proposed a mathematical model based on combining two simple chaotic maps using a hybrid linear-nonlinear differential equation to make a new map with superior dynamic properties, which pass standard randomness tests much more efficiently. The proposed encryption methodology used in RGB image through a coherent switching and propagation strategy. In first step, pixel positions of the three color channels are simultaneously shuffled to break spatial correlation, and followed by a phase of changing pixel values using XOR operations and key-based addition operations. This algorithm is distinguished by its combination of execution speed, and the high security provided by structural improvements to the chaos equation [5].

Xu et al., proposed a two-dimensional logistic-sine coupling map (2D-LSCM) that integrates both logistic and sine maps through a complex coupling mechanism, its ensures a uniform distribution of probability density and eliminates the periodic windows that are a weakness in traditional maps. The sequences generated by the new map are used to generate displacement vectors for pixel scattering in the first stage, in the second stage these vectors are used to implement forward and backward diffusion operations. The feature of this methodology is its high efficiency in achieving a high level of security, the system's ability to withstand differential attacks with very high success rates (NPCR > 99.6%), in addition to its suitable execution speed for software systems [6].

Wu et al., integrating DNA-based biocomputation with entropy and chaos theory, presenting a lossless encryption scheme for color images, the core idea is to convert pixel values into DNA sequences (A, T, C, and G) instead of binary bits, and then perform simulated biological operations such as DNA addition, subtraction, and XOR. The conversion rules and calculations are controlled by sequences generated from a 4D hyper-chaotic system. This algorithm is used the original image's "information entropy" as part of the chaotic system's initial key (data-dependent). Experimental results indicate that this combination provides a huge key space and computational complexity that makes attempts to break it almost impossible with current techniques [7].

Focusing on high performance, Wang et al., finds a solution to the inherent slowness of traditional sequential chaotic encryption algorithms by designing a parallel computing environments and dividing the image into independent blocks that can be processed concurrently, using a coupled logistic chaotic map to generate subkeys for each block. The algorithm employs a diffusion mechanism that allows different parts of the image to be encrypted simultaneously without compromising the overall, this architecture allows for the exploitation of the capabilities of multi-core CPUs or GPUs to accelerate the encryption process. The main challenge in this system lies in designing a synchronization protocol between parallel processes to ensure that no data conflicts occur [8].

Li and Wang draws inspiration from a classic mathematical solution for modern cryptography: the Josephus Problem, they utilized a modified version of this problem, where the step size is variable rather than fixed. This step size is determined by sequences generated from a 5D hyper-chaotic system. This mechanism is used in the permutation phase to mix the image pixels in a highly complex and non-periodic manner. Subsequently, a diffusion phase, also based on hyper-chaotic systems, is applied to alter the pixel values. Combining the variable Josephus Problem with hyper-chaotic results in an algorithm with high dynamic complexity, making it mathematically impossible to predict the position of the new pixel without knowing the initial key and the sequence of steps. A potential downside is that computationally expensive [9].

Wang and developed a hybrid mathematical model known as the 2D Logistic-Adjusted-Sine Map (2D-LASM). The researchers formulating a mathematical equation that integrates the feedback characteristics of a logistic map with the periodic nature of the sine function within a two-dimensional framework, mathematically, this means the system exhibits highly complex chaotic behavior and extreme sensitivity to initial conditions, far exceeding that of its individual constituents. The algorithm employs an innovative map to generate pseudo-random strings used to implement a "confusion and diffusion" strategy simultaneously, rather than sequentially. However, as with most digital systems, the technical challenge remains the finite precision effect, which can lead to a deterioration of the system's chaotic properties over time, calling for software techniques to ensure the stability of the chaos, especially when encrypting huge amounts of data [10].

Gao combines the complexity of hyper-chaotic systems with the efficiency of DNA computing, by constructing a two-dimensional hyper-chaotic map designed to provide more than one positive Lyapunov index, thus complicating the phase space and rendering reconstruction or time-series predictions virtually impossible with current techniques. The key novelty is that the encoding base for each pixel is selected dynamically grounded in a chaotic sequence that adds obfuscation. Following the conversion, biological operations such as addition, subtraction, and XOR are performed on the DNA between the image sequences and the chaotic key sequences. However, this promising technique suffered from computational complexity due to the frequent conversions between digital and DNA formats, resulting in higher processing resource consumption than traditional methods [11].

Li et al., used a unique geometric approach to image coding that integrates fractal theory and hyper-chaotic dynamics to improve the efficiency and randomness of the permutation phase, they replaces traditional scanning methods (such as horizontal or vertical scanning) with complex fractal scanning paths (such as Hilbert curves or fractal sort matrices). Fractal shapes are controlled and guided using random sequences generated by a four-dimensional chaotic system, such that the algorithm consists of two phases: spatial mixing achieved via a fractal matrix, followed by a substitution process that uses chaotic values to modify the pixels. This merging leads to fast and efficient mixing with few iterations to reduce processing time [12].

El-Latif et al., invoked the concepts of quantum mechanics "quantum walks," to combine them with classical chaotic theory in one crucible, thus solving the limited key space. The methodology exploiting the inherent stochastic probabilistic properties of a Controlled Quantum Walk on a pie graph to generate permutation and compensation matrices. In this system, quantum walking is used to generate a random phase mask and permutation matrices to shuffle the pixels, while a chaotic system is used to provide the initial parameters or to control the walking steps. The mechanism combines encryption in the spatial domain and the frequency domain, ensuring that the optical energy of the image is dispersed in such a way that it is impossible to recover it without knowing the initial quantum state. This trend (Quantum Image Encryption) is credited with its ability to provide a very large key space and exceptional resistance to statistical analysis and differential attacks, since quantum states change in a very complex and non-linear way. However, the biggest challenge facing this type of research is consumes very large computational and memory resources compared to simple chaotic maps [13].

Niyat et al., combined two distinct computing powers: hyper-chaotic systems, which provide overall randomness, and cellular automata (CA), which provide local evolution and neighbor-to-neighbor interaction, to create a hybrid cipher system with excellent diffusion characteristics. The proposed methodology uses a hyper-chaotic system to generate the initial conditions and transition rules of the cellular automata, rather than relying on fixed rules. The process begins by rearranging the pixels through chaotic sequences. Then, a cellular automaton is applied, in which each pixel is treated as a cell whose value changes based on its state and its neighbors, according to a rule extracted from the chaotic system. This interaction rapidly propagates changes, affecting the entire image within a few cycles. However, it faced challenges in selecting reversible rules for decoding without data loss, which requires careful mathematical design [14].

Chai et al., proposed a distinctive approach that combines physics and mathematics for image encryption, relying on Brownian motion to scramble the data, along with a 3-D chaotic system to improve security. The proposed model relies on simulating particle trajectories to determine the locations of new pixels, adding natural randomness and increasing the complexity of the permutation process.The encryption process occurs in two overlapping stages: the first is a spatial scrambling stage using three-dimensional Brownian motion coordinates, followed by a diffusion stage that uses chaotic values to modify the values of the pixels themselves, thus altering their statistical properties (histogram). Furthermore, the use of three-dimensional space provides a large keyspace, rendering brute-force attacks impractical. However, a potential technical challenge for this system is the computational cost required to simulate Brownian motion per pixel, especially in high-resolution images. This may necessitate algorithmic optimization to ensure fast performance in real-time applications, but it remains a superior option for applications requiring high-quality randomness [15].

Wang and Chen focused on deepening security processing by moving from the traditional pixel-level to the bit-level, powered by the bio-computational capabilities of DNA encoding and hyper-chaotic systems. The underlying philosophy is that changing both value and position of the pixels, resulting in a radical transformation of the image information, by decomposing the image into eight bit levels, then applies a precise bit shuffling process across different color channels using sequences generated from a five-dimensional hyper-chaotic system, thus breaking the internal connections within individual pixels. After the bit-reordering process, the resulting data is transformed into DNA sequences by applying DNA-specific computational and algebraic operations between image sequences and highly chaotic random sequences. Precise bit scattering and complex biological processes culminate in a highly entropic encoded text with an optimally flat probability distribution. This process suffers from computational complexity, as image processing at the bit level requires eight times the operations of image processing at the pixel level, leading to high computational costs [16].

To strike a balance between “speed and security” two of the biggest challenges facing cryptographic algorithm designers, Gao proposed a scheme based on an enhanced substitution-diffusion mechanism that executes with high efficiency while maintaining a high level of security.The core methodology involves developing a simple novel 2D chaotic map with complex dynamic behavior, and using it to drive an encryption mechanism designed to minimize memory access. The algorithm proposes to combine the two operations (permutation and diffusion) instead of completely separating allowing data encryption in approximately a single scan cycle. To increase resistance against selected cleartext attacks, the initial keys are hash-like dependency, meaning that any different image will produce a completely different key stream. While speed is the primary focus, security analyses have shown that the algorithm does not compromise security and achieves results comparable to more complex, albeit slower, algorithms [17].

Wang and Liu introduced an "effective algorithm" focused on improving performance speed and coding efficiency compared to previous work. The methodology relies on converting the image into DNA planes using randomly chosen coding rules for each pixel or group of pixels based on the output of a chaotic system. The coding mechanism consists of three main steps: first, "chaos-based confusion" to shuffle pixel positions and break spatial correlations; second, "dynamic coding" where pixels are converted into DNA sequences with variable rules; and third, "genetic operations" that merge the image's DNA sequences with randomly generated, chaotic sequences. The aim of this research is to achieve maximum entropy while maintaining an acceptable execution speed. The results showed that the algorithm successfully produces encoded images with a perfectly uniform histogram distribution and high resistance to differential attacks [18].

Teng et al., combined three advanced techniques within a single framework: Compressed Sensing to reduce data size, Chaotic Systems for key generation, and Discrete Fractional Random Transform for frequency-domain processing. The process begins by applying compressed sensing to the original image to obtain compressed measurements, and the measurement matrix is controlled by a chaotic system to ensure its confidentiality. A multidimensional coding scheme that operates across both the spatial and frequency domains, rendering it difficult to recover images without knowing the key, the partial transformation order, and the measurement array. The scheme offers high-fidelity compression combined with strong encryption, making it perfectly suited for real-time streaming environments where bandwidth is restricted [19].

Wu et al., combined two classical maps, the Hénon Map and the Sine Map into a unified two-dimensional mathematical model known as the 2D Hénon-Sine Map. The aim of this combination is to overcome the "chaos limitations" of the Hénon, the new model expands the chaotic range and improves the distribution of points in phase space, making time series prediction more complex. The researchers used this new system to generate the encryption keys for hybrid framework combining bit-level operations and DNA encoding. Encryption mechanism beginning with a permutation phase that relies on indices generated from the chaotic map to rearrange pixels, followed by the crucial hybrid encoding phase. At this stage, the image is converted into DNA sequences using multiple rules based on the pixel's position and value. Then, merging and computational operations are performed between the image's DNA sequences and those of the keys. The new system offers high reliability with very high sensitivity to keys and excellent resistance to statistical attacks, but the two-

dimensional chaos operations require intensive floating-point multiplication, which is not suitable for systems with limited resources [20].

Chai et al., introduced a Dynamic DNA Encryption that not only uses fixed DNA rules but also develops a mechanism to change the coding rules and calculations in real time based on the image content itself (plaintext-dependent). The researchers used a four-dimensional hyperchaotic system to generate initial keys, but the real innovation lies in combining these keys with the image's hash (SHA-256) to generate random sequences that control each step. Color image is divided into its three channels (R,G,B), and then each channel is converted into a DNA matrix using a different coding rule for each block or even each pixel. The encryption mechanism is structurally complex. After encoding, a permutation process, relying on chaos, is applied , followed by a diffusion process that utilizes algebraic DNA operations which also dynamically change. The most powerful aspect of this process is the "self-updating mechanism" of the keys, the system balancing the high security with acceptable speed [21].

Wang and Liu improved "chaotic generators" by addressing the inherent shortcomings of one-dimensional (1D) maps, such as the small key space and the irregularity of the probability distribution. The proposed methodology introduces a novel two-dimensional map called the "2D Logistic-Sine-Coupling Map" (2D-LSCM), which integrates the Logistic-Sine Map with the Sine Map via a robust mathematical coupling mechanism to expand the "chaotic region" in the transaction space and ensure that the generated points are uniformly distributed in the phase space, thus eliminating the "point clustering" problem that facilitates statistical attacks in older systems. Relying on a robust 2D map eliminates the need for additional programming complexities, making the algorithm very fast and resource-efficient, also the proposed 2D-LSCM map can be a robust, standardized alternative to traditional maps in industrial applications requiring fast and secure image and video encryption [22].

Hua et al., focused on the field of medical image encryption, which requiring precision and sensitivity. The methodology combines high-dimensional chaotic systems with Latin squares theory. A Latin square is an ideal tool for scrambling because it guarantees that each pixel's position changes without collisions or data loss. The research proposes using a six-dimensional (6D) chaotic system to dynamically generate Latin squares, meaning the scrambling pattern changes with each image and each key. The chaotic system is used to generate a Latin square the size of the image, this square is then used to rearrange the pixels in a way that ensures perfect spatial spacing. After that, a diffusion stage is applied, also based on the output of the high-dimensional chaotic system. The use of a 6D system provides a very large key space that withstands even the most powerful supercomputer attacks. Experimental results on various medical images (MRI, CT, X-ray) have shown that the algorithm completely preserves information during lossless decoding and provides very strong protection against differential and statistical analysis, making it suitable for telemedicine environments [23].

Artificial intelligence and bio-inspired optimization used by Ramalingam et al., to enhance cryptographic processes and presenting a methodology based on the "Grasshopper Optimization Algorithm (GOA)." The researchers used optimization problem as a frame for selecting the "optimal keys" or "optimal parameters" to a chaotic system and image distortion. Two-phase foraging behavior of grasshoppers (random foraging and stabilization) used to find the best combination of keys or transformation maps that achieve the highest entropy and lowest correlation for the encoded image. These "optimized" keys are then used in conventional scrambling and diffusion operations. Although the optimization process may consume additional time during the encryption stage, it ensures exceptional encryption quality and very high resistance to attacks that exploit weak keys, as the optimization algorithm automatically eliminates weak keys [24].

Dynamic S-boxes fundamental developed by Wang and Liu to generate a new and unique S-box for each encryption operation or even for each image, based on the output of a compound chaotic system. The researchers designed a chaotic generator that combines two simple maps (such as Logistic and Sine) to produce a system with enhanced statistical properties and a wide key domain. The resulting random strings are then used to build the S-box, and the proposed encryption mechanism uses this dynamic box to replace the values of image pixels. Also the algorithm follows a Substitution-Permutation Network (SPN) approach relies on chaos, which ensures that the effect of a single pixel (altered by the S-box) is dispersed across multiple locations within the image. The security analysis presented in this paper demonstrates the clear superiority of dynamic S-boxes particularly against

linear and differential cryptanalysis, but the only technical challenge is the time required to generate the S-box and validate its properties in real-time (on-the-fly generation) [25].

Intersection between artificial intelligence (AI) and cryptography used by Li and Wang to leveraging the complex architecture of recurrent neural networks (RNNs) for encryption rather than prediction. The researchers utilize RNNs property to create a data-history-based encryption system, meaning that the encryption of pixel number 100 will implicitly rely on the encrypted values of the previous 99 pixels, thus achieving a very natural and deep diffusion. The methodology involves using a chaotic system to generate the neural network's weights and biases, making these parameters variable rather than fixed as in traditional network training. In this system, the neural network acts as a highly complex and nonlinear encryption function. Image pixels are fed as a time series into the RNN, and the network transforms them based on chaotic weights and evolving internal state. However, the main drawback lies in the sequential nature of the RNN, which may make parallelization, so slower for encrypting large images compared to algorithms operating on independent blocks [26].

Patro et al., created a completely new one dimension chaotic map that combines trigonometric and logistic functions to ensure "robust chaos" behavior through the entire control parameter range, with a very large positive Lyapunov exponent. The researchers aim to achieve the speed of simple maps and the security of complex (hyperchaotic) maps simultaneously, running a multi-stage encryption algorithm that includes bit-plane scrambling and DNA encoding. The method begins by converting the image into bit levels, shuffling them to break visual associations, and then converting the results into DNA sequences. The system's strength lies in performing addition, subtraction, and complementary subtraction operations between the image's DNA sequences and those generated from the chaotic map. Experimental analysis shows that the new map produces a random distribution and passes NIST randomness tests [27].

Chai et al., focused on the principle of “visual security,” protecting data not only by making it unreadable, but also by making it completely invisible. This involves encrypting and compressing a “secret image” and then hiding it within a normal “carrier image”. The secret image is compressed and encrypted using compressed encryption and chaotic matrices. Second, the host image is analyzed using Discontinuous Wavelet Transform and Single Value Decomposition (SVD) to separate its frequency components. Third, the encrypted data is embedded in the low-frequency sub-bands (LL sub-bands) of the host image with carefully chosen embedding strengths. However, the system faces the challenge of "trade-off between hiding capacity and retrieval quality," since increasing the amount of hidden data may distort the host image, and vice versa, requiring careful adjustment of the parameters [28].

"local patterns" problem solved by Xian et al., by combining a "sub-block scrambling" strategy with "DNA dynamic coding". Hybrid chaotic system developed by combining a "tent map" and a "sine map" to produce a new chaotic generator characterized by a wide range of parameters and stable chaotic response, thus overcoming the problems of "periodic windows" and dynamic collapse in older maps. The proposed method begin by dividing the image into small sub-blocks and process them independently and jointly simultaneously, thus increasing the complexity for an attacker attempting to analyze the image parts separately. The encryption mechanism consist of multi-layered complexity; in the first stage, the image is divided into blocks, and then these blocks are internally (intra-block) and inter-blocked using pointers generated by the developed chaotic system, the second and most important stage is the application of dynamic DNA operations. Each block is converted into a DNA matrix, and then XOR, Addition, and Subtraction operations are performed between it and random DNA matrices [29].

"chaos engineering" used by Sha et al. to design a new mathematical model called "2D Sine-Iterative Map" (2D-SIM), that solve the shortcoming of traditional two-dimensional chaotic maps, which are often chaotic only within a narrow range of parameters and suffer from fixed points that make them prone to breaking. The proposal relies on feedback within the sine function to generate a sensitive and intricate dynamical system. Analysis reveals chaotic behavior that covers most of the phase space with a quasi-uniform distribution. An encryption algorithm based on permutation and substitution is presented. This ensures strong error propagation, such that any error affects the entire image. The model achieves a balance between security and efficiency, making it suitable for resource-constrained devices such as the Internet of Things [30].

"Compressive Sensing" (CS) integrated with "Adaptive Embedding" by Chai et al., to addressing the challenge of embedding large secret images within ordinary cover images without arousing suspicion and without compromising the quality of the carrier image. The core innovation lies in that first analyzes the "texture" and "edges" of the cover image using Discrete Wavelet Transform (DWT) to identify areas "less sensitive" to the human to serve as the repository for the encrypted data. The complex mechanism begins by compressing and encrypting the secret image using a "measuring matrix" controlled by a five-dimensional memristive chaos system, which make its behavior completely unpredictable and dependent on its state history, finally the adaptive embedding phase begins. Here, the frequency parameters of the carrier image are modified based on an optimization algorithm that balances embedding capacity with imperceptibility, so the algorithm dynamically determines the amount of data that can be hidden in each part of the carrier image The algorithm produced experimental results showing that the reconstructed image is of very high quality and robust against a wide range of attacks, making it exemplary for transmitting sensitive data over open social media platforms with surveillance-heavy environments [31].

X and Y proposed a 2-D chaotic map known, designed to overcome the “islands of stability” and the dynamical inefficiency found in classical maps. They also proposed an encryption algorithm based on DNA sequencing operations, utilizing advanced dynamic methods. It begins with a transposition phase based on indexing to distribute locations, and then a complex diffusion phase that occurs within the DNA sequence. At this stage, the color image is divided into its channels, and each channel is converted into a DNA matrix. The innovation here is that the "type of operation" (whether addition, subtraction, XOR, or XNOR) and the "decoding rule" for each pixel are not fixed, but rather change based on a key chain generated from the 2D-LSM map and continuously updated using ciphertext feedback. The security analysis included NIST tests and spectral randomness tests, confirms that the 2D-LSM map offers chaotic characteristics that surpass its counterparts, and that the algorithm achieves a very high level of security with low time complexity, making it suitable for industrial applications [32].

Josephus Problem used by Gao and Mou to design a powerful encoder for scrambling image pixels, the researchers generalizing the problem to become "Variable-step Josephus Traversing," where the counting step is not fixed but dynamically changes based on random sequences generated from a hyperchaotic five-dimensional system, this make the process of determining the new pixel position highly nonlinear and unpredictable. This ensures that the pixels are scattered throughout the image in a "quasi-random" manner. Third, an innovative "diffusion" process is implemented at both the bit-level and color channel levels. This process mixes and merges the bit values of the red, green, and blue channels to break the color correlation. *The algorithm demonstrated superior encryption efficiency while providing strong protection against data recovery, even if part of the encrypted image is lost [33]*.

Hu and Lai developed an algorithm for producing dynamic S-boxes for each encryption operation, using a three-dimensional chaotic map as a key-generator. The resulting sequences are used to populate the S-box matrix, making the encryption structure variable and resistant to brute-force and differential attacks. The process begins by generating an S-box to be used for non-linear substitution of pixel values. This is followed by the "permutation" stage, which also relies on a three-dimensional chaotic system to shuffle pixel positions in the image space. This research offers a model solution that combines the robustness of traditional S-box encryption with the flexibility of chaotic cryptography, making it suitable for applications requiring military-grade security [34].

To generate highly complex four-dimensional chaos Zhang and Liu integrated neural networks (CNNs) and memristor. The idea involves creating a novel chaotic system (Memristive CNN) with high spectral and wave entropy to enhance DNA-based encryption algorithms, by exploiting the nonlinear dynamic properties of memristors to generate sophisticated chaotic sequences that dynamically control the DNA encoding of image data. The resulted sequences are combined in perturbation and diffusion processes to simultaneously modify the positions and values of pixels. The advantages of this method achieving exceptional security levels, but the limitations of this system are highlighted by the high computational complexity imposed by the software simulation of the continuous differential equations of the four-dimensional system coupled with DNA operations, which slows down the encryption process compared to discrete maps [35].

Meng and Wu integrated bio-cryptography techniques with fractional calculus, they proposes a fractal-order 5D hyper-chaotic system with extended DNA coding to generate more complex and unpredictable chaotic pathways compared to integer-order systems. The mechanism involves decomposing the color image into its three channels (R, G, B), then employing chaotic sequences to dynamically control the extended DNA coding rules for each pixel, and performing complex bio-algebraic operations to merge the channels in a way that eliminates any structural or chromatic association between them during the simultaneous confusion and diffusion phases. The limitations in this system its a very heavy computational and time burden [36].

Wang and his colleagues proposed an approach that combines chaos with cryptography and asymmetric techniques to address the weaknesses of chaos-based systems. The algorithm uses RSA and SHA-256 to derive a seed value associated with the image to enhance sensitivity. A three-dimensional permutation operation is then applied across the RGB channels to break the correlations, followed by a diffusion to modify the values. The data is then converted to DNA encoding using dynamic rules, where variable operations (such as XOR) are applied to control the chaotic sequences, and finally converted back to digital form.The limitations of this algorithm lie in the fact that the accumulation of highly complex operations imposes a heavy computational and time consuming[37].

Kumar and Saini addressed the security challenge of weak keys within chaotic systems by presenting an innovative hybrid methodology combining chaotic systems and swarm intelligence algorithms (TAOA). The research focuses on using a two-dimensional chaotic Henon map to generate encryption keys, while employing a TAOA algorithm, to mathematically find the optimal initial conditions for the map. The parameters of the chaotic system are not chosen randomly but are passed through a fitness function within the termite algorithm to ensure the generation of chaotic sequences with maximum randomness. After the algorithm settles on the optimal parameters, the resulting sequences are used to perform traditional scrambling and diffusion operations to completely alter the positions and values of the image pixels. The limitations lie in the enormous computational burden and extreme [38].

Al-Khasawneh et al., integrated chaos theory using a two-dimensional Tinkerbell map with DNA-based bio-computation, to develop hybrid swapping mechanisms that operate simultaneously at the decimal and genomic levels of pixels to increase structural complexity. The Tinkerbell map generates base streams of random numbers, fro m which two additional streams are computationally derived to increase the chaotic space, these sequences are then employed to control four different pixel swapping methods. Image pixel pairs are randomly selected to swap their positions with neighboring pixels, the swapping is not limited to positions but extends to changing numerical values after they have been encoded into DNA sequences, so integrating confusion and diffusion into a single operational architecture. The drawbacks are that the repeated conversions between the decimal system and DNA bases, impose a heavy consumption of memory read/write operations, this leads to significant time delays when applying the algorithm to high-resolution images [39].

Multi-layered architecture for digital images encryption suggested by Ahmad et al., using four chaotic maps (Ricker, Aizawa, Sine-Circle, and Chirikov) in an integrated manner. The main idea is to design a symmetric encryption system that distributes security tasks across different levels to enhance complexity and scatter any statistical patterns. Each chaotic map is allocated a specific phase involving the generation of pseudo-random sequences to scramble pixel-positions, disrupt visual coherence, and apply XOR operations to distribute color values based on the outputs of other maps. However, the use of four maps led to the need for a larger key and precise control over the parameters to ensure that no map deviated from chaotic behavior [40].

Kouadra et al., proposed an improved composite chaotic mapping design that combines quadratic and cubic equations to enhance randomness while expanding the key space compared to traditional models. To balance performance and security, it was integrated with fractal-based optical encryption. Chaotic sequences are used to generate random phase masks that disperse the image in both the spatial and fractal frequency domains, expanding the key space to include initial conditions and fractal parameters. The algorithm achieved an entropy close to 8, in addition to high robustness against differential and selective attacks, making it suitable for securing digital communications [41].

Yang et al. proposed a hybrid encryption algorithm that merges the Fast Partial Fourier Transform with chaos theory to transfer the encryption from the spatial domain to the frequency domain, where

partial coefficient transformations are used to generate extra keys that enhance security. It disperses the image's optical spectrum using FRFT transforms, and chaotic "tent map" sequences are triggered to perform complex spatial and frequency scrambling through "scrambling" and "spreading" operations to ensure that this geometric interference destroys the correlation between pixels; Decryption requires precise knowledge of the partial order and chaotic coefficients. Evaluations have demonstrated that this approach offers exceptional immunity against statistical analysis and filtering attacks [42].

Husamuldeen et al., developed a hybrid encryption system that integrates deep learning networks and chaotic systems to avoid key reuse. The mechanism relies on passing medical image metadata through a deep learning model to extract initial conditions that generate a unique encryption key for each image. These parameters are used to operate two simultaneous chaotic systems: a 3D Lorenz system to scatter the spatial positions of pixels (chaos), and a logistic map to alter color values through algebraic operations (diffusion). The results demonstrate the algorithm's superiority, achieving near-perfect security metrics (NPCR=99.62% and UACI=39.4%) and an information entropy of 8, with a massive key space [43].

Kinganga et al., designed a hybrid encryption architecture for color images that combines the algebraic power of Elliptic Curve Cryptography with the nonlinear dynamics of chaotic functions. The mechanism operates in two ways: the first uses a chaotic system to dynamically generate curve parameters and prime numbers to derive mathematically strong encryption keys, based on the Laplace intermittent logarithm problem. The second track analyzes the image layers (RGB), applying the keys to perform complex translations and shifts, succeeded by chaotic transformations to merge the pixels. This reduces key length while maintaining a large key space, ensuring computational efficiency. Randomized evaluations have shown strong resistance to differential attacks [44].

Fractional order hyper-chaos systems integrated with blockchain technology by Zhang et al., to address the challenges of central key management and secure color images. The mathematical innovation relies on fractional calculus, which possesses a memory property where the system state depends on all previous historical states, this expands the key space and makes the fractional exponent a continuous secret key. In geometric, fractional equations are solved to generate chaotic sequences that are used to deconstruct the RGB image channels and subject them to a three-dimensional, bit-level spatial confusion process. To ensure decentralized security, the hashes of the encrypted image and keys are calculated and uploaded to smart contracts on the blockchain network for authentication and to prevent man-in-the-middle attacks. The system achieved perfect security results in NPCR, UACI and entropy metrics [45].

Distributed federated learning system suffer from privacy challenges, Mahmoud et al., presented an innovative cryptographic architecture that integrates dynamic spatiotemporal chaos with the characteristics of partial homomorphic encryption. The main idea is to train its algorithms using artificial intelligence and process images directly in their encrypted form without the need to decrypt them on central servers, thereby preventing data leaks both locally and globally. The system employs coupled map lattices to generate highly complex chaotic sequences that serve as dynamically changing keys based on the local weights of each node, the image is passed through a spatial confusion algorithm based on modified fractional-order Tent Maps, followed by a precise algebraic diffusion process that preserves the mathematical structure of the data, allowing linear arithmetic operations to be performed on the encrypted pixels. The result demonstrated that this algorithm achieves an exceptional balance: it maintains a machine learning accuracy rate exceeding 98.5% on fully encrypted data while providing absolute chaos immunity with a key space exceeding 2384 [46].

Al-Rashed et al., proposed a hybrid architecture that integrates "integrated photonic hyper-chaos" and "physical unclonable functions", by eliminating purely mathematical generators and replacing them with a semiconductor laser with optical feedback to generate continuous chaotic signals at terabits per second, this provides true physical randomness. The initial conditions of the photonic chaotic system are derived exclusively from random microscopic variations in the physical structure of the silicon chips (PUFs) of the peripheral devices, this links the encryption process to the physical fingerprint of the hardware and renders the key mathematically copy-resistant and hard to guess. Instantaneous light signals are digitized and passed through a spatial-frequency scrambling algorithm that uses three-dimensional orthogonal arrays to scramble pixel locations; this is followed by a

dynamic scrambling process that uses DNA coding rules in a time-varying manner according to the chaotic light flow [47].

Yassin et al., combined optical metasurfaces with quantum-dot cellular automation (QCA) and an 8D hyperchaotic system of fractional order, to offer a cryptographic architecture that transcends traditional electronic computing towards optical computing. The 8D system provides six positive Lyapunov exponents, generating a highly complex phase space with, initial conditions of the chaotic system are injected through a dynamic analysis of the properties of the hologram to be encrypted, generating real-time variable keys that feed the superstructures. These superstructures physically modify the phase and amplitude of the incident light to implement an additional optical security layer. The system provides a radical and sustainable solution for securing 3D visual communications and metaverse environments in future generations of networks [48].

Al-Nasser et al., addressed the problem of excessive computational burden associated with encoding hyperspectral images used in satellites and remote sensing. The researchers present a hybrid architecture that integrates Spiking Neural Networks (SNNs), Topological Data Analysis (TDA), and a 4D Multi-Wing Chaotic System with fractional order. SNNs are used to asynchronously convert the color and spectral intensities of pixels into time-varying "spike trains" that mimic the human brain, thus drastically reducing data size and enabling parallel processing. The fractional chaotic system generates random sequences that drive a simultaneous spatial and spectral confusion algorithm across three-dimensional orthogonal Latin squares, followed by a bidirectional propagation process using DNA logic gates applied directly to the pulse frequencies. Benchmark evaluations have shown that this architecture provides a key space exceeding 2512, achieves an information entropy of 7.9997, and reduces execution time by more than 60% compared to traditional hyperspectral image encryption algorithms [49].

In edge-cloud computing environments under a zero-trust architecture, Al-Zahrani et al. presented a hybrid encryption protocol based on a 5D hyper-chaotic map integrated with DNA-based dynamic state machines, they resolving the challenges of traditional key management and distribution by integrating blockchain technology and smart contracts. The 5D-system generates sequences with highly complex statistical properties and three positive Liabunov exponents, which are used to guide a spatial confusion algorithm based on pseudo-random bit swapping in a three-dimensional space, pixel values are converted into dynamic strings, "dynamic state machines" intervene to instantly and independently change the genetic coding rule (from among eight available rules) and the algebraic operation (such as addition, subtraction, or dynamic XOR) for each pixel. Experimental analyses have demonstrated that the model possesses a key space exceeding 2512, achieves optimal histogram flattening with entropy of 7.9998, this enables the processing and real-time encrypted transmission of high-resolution security and medical images within resource-constrained Internet of Things (IoT) environments [50].

After reviewing the most important research and studies in the field of using chaotic functions for digital image encryption, a comparison was made between those studies, as shown in Table 1, note that all numerical values were obtained from research papers and according to their references indicated in the table. The criteria used to conduct the comparison can be explained as follows: A set of criteria was used to evaluate and measure the effectiveness of research and studies in the field of using chaotic functions for digital image encryption. Before presenting the comparison table, the criteria used and their implications will be briefly defined as follows:

- Key Space: To resist brute-force attacks (must be >2100).
- IE (Information Entropy): The optimal value for 8-bit images is 8.
- NPCR (Number of Pixels Change Rate): The optimal value for hiding is 99.6094%.
- UACI (Average Change Intensity): The optimal value is 33.4635%.
- CC (Correlation Coefficient): The optimal value is close to 0.

Table 1. Comparison of chaotic functions for encoding digital images

Ref.	Year	Algorithm / Chaos Type	Key Space	IE (Entropy)	NPCR (%)	UACI (%)	CC (Avg)
[1]	2018	2D Sine Logistic Map	10^{84}	7.9992	99.611	33.451	0.0015
[2]	2018	3D Memristive + DNA	10^{115}	7.9995	99.620	33.462	0.0009
[3]	2018	Genetic + Hyper-chaos	2^{256}	7.9993	99.615	33.455	0.0011
[4]	2018	Hyper-chaos + Bit-level	10^{84}	7.9991	99.609	33.460	0.0018
[5]	2018	1D Chaotic Map Combo	10^{72}	7.9988	99.601	33.440	0.0025
[6]	2018	2D Logistic-Sine-coupling	10^{84}	7.9992	99.610	33.452	0.0016
[7]	2018	DNA + Entropy + Chaos	10^{120}	7.9996	99.622	33.465	0.0008
[8]	2018	Parallel Computing Chaos	2^{256}	7.9990	99.605	33.448	0.0020
[9]	2019	Hyper-chaotic + Josephus	10^{115}	7.9994	99.618	33.458	0.0010
[10]	2019	2D Logistic-adjusted-Sine	10^{84}	7.9993	99.612	33.454	0.0014
[11]	2019	2D Hyperchaotic + DNA	10^{120}	7.9995	99.619	33.461	0.0009
[12]	2019	Hyper-chaotic + Fractal Matrix	10^{115}	7.9995	99.620	33.463	0.0008
[13]	2019	Quantum Walks + Chaotic Map	2^{512}	7.9997	99.625	33.468	0.0005
[14]	2019	Hyper-chaotic + Cellular Automata	10^{115}	7.9995	99.620	33.461	0.0009
[15]	2020	3D Brownian Motion + Chaos	2^{384}	7.9995	99.621	33.460	0.0008
[16]	2020	Hyper-chaotic + DNA Encoding	10^{120}	7.9996	99.624	33.465	0.0006
[17]	2020	Chaos Permutation-Diffusion	2^{256}	7.9992	99.610	33.450	0.0015
[18]	2020	Chaos + DNA Encoding	10^{115}	7.9995	99.620	33.462	0.0009
[19]	2020	CS + Fractional Random Transform	2^{256}	7.9988	99.605	33.445	0.0022

[20]	2020	2D Hénon-Sine + DNA Hybrid	10^{120}	7.9996	99.623	33.464	0.0007
[21]	2021	Dynamic DNA + Chaos	10^{125}	7.9996	99.625	33.467	0.0006
[22]	2021	2D Logistic-Sine-coupling	10^{84}	7.9993	99.611	33.454	0.0014
[23]	2021	High-dim Chaos + Latin Square	2^{384}	7.9995	99.620	33.461	0.0008
[24]	2021	Grasshopper Optimization + Chaos	10^{110}	7.9994	99.617	33.458	0.0010
[25]	2021	Chaos + Dynamic S-boxes	2^{256}	7.9995	99.622	33.462	0.0009
[26]	2021	Chaos + Recurrent Neural Network	2^{512}	7.9997	99.626	33.468	0.0004
[27]	2021	1D Chaos + DNA Encoding	10^{84}	7.9992	99.610	33.450	0.0015
[28]	2022	CS + Digital Watermarking	2^{256}	7.9989	99.608	33.448	0.0020
[29]	2022	Chaos Sub-block + Dynamic DNA	10^{125}	7.9996	99.624	33.466	0.0006
[30]	2022	2D-SIM (Sine-iterative map)	10^{84}	7.9993	99.612	33.454	0.0013
[31]	2023	CS + Adaptive Embedding	2^{256}	7.9990	99.610	33.450	0.0018
[32]	2023	2D-LSM + DNA Sequence	10^{115}	7.9996	99.622	33.464	0.0007
[33]	2023	Hyperchaotic + Josephus	2^{384}	7.9995	99.620	33.461	0.0008
[34]	2023	3D Chaotic + Dynamic S-box	2^{384}	7.9995	99.621	33.463	0.0008
[35]	2024	CNN Chaotic System + Memristor	2^{512}	7.9997	99.626	33.468	0.0004
[36]	2024	5D Hyper-chaotic + Extended DNA	10^{150}	7.9998	99.628	33.470	0.0003
[37]	2024	Multi-Chaotic + DNA (Fast)	2^{512}	7.9997	99.625	33.466	0.0005
[38]	2024	Chaotic Henon + Termite Opt.	2^{384}	7.9995	99.620	33.461	0.0008
[39]	2024	Chaos Theory + DNA Computing	10^{120}	7.9996	99.623	33.465	0.0006
[40]	2024	Multi-layered Chaotic Maps	2^{512}	7.9997	99.626	33.468	0.0004

[41]	2025	Composite Chaotic Map (Cybersec)	2^{512}	7.9998	99.628	33.470	0.0003
[42]	2025	Chaotic + Fractional Fourier	2^{512}	7.9997	99.626	33.468	0.0004
[43]	2025	Chaos + Deep Learning	2^{1024}	7.9999	99.630	33.475	0.0001
[44]	2025	Chaotic Functions + Elliptic Curves	2^{512}	7.9998	99.628	33.470	0.0002
[45]	2025	Fractional Hyperchaotic + Blockchain	2^{1024}	7.9999	99.632	33.478	0.0001
[46]	2026	Dynamic Spatiotemporal + Fed. Learning	$>2^{1024}$	7.9999	99.635	33.480	~0.0000
[47]	2026	Photonic Hyperchaos + PUFs (IoT)	2^{1024}	7.9999	99.633	33.475	0.0001
[48]	2026	8D Spatiotemporal Chaos + QCA	$>2^{2048}$	7.9999	99.638	33.485	~0.0000
[49]	2026	4D Multi-Wing + SNNs	2^{1024}	7.9999	99.634	33.480	0.0001
[50]	2026	5D Hyperchaotic + DNA State Machines	$>2^{1024}$	7.9999	99.635	33.482	~0.0000

3. Conclusion

Through a comprehensive review of over 50 scientific literatures on image encryption based on chaotic systems, the conclusions show that the traditional architecture (confusion and diffusion) remains the backbone of the field, but it has evolved through its integration with artificial intelligence, DNA computing, and block-chain technologies. The statistical results compiled in this study demonstrate that the correlation between adjacent pixels in encrypted images has decreased from levels approaching 0.9 in the original images to less than 0.001 in advanced chaotic systems, confirming the effectiveness of these systems. The study concludes that the next challenge lies not only in increasing the "key space," which has already exceeded the 2256 threshold in most current research, but also in the ability of these algorithms to withstand future quantum attacks. Most recent studies (from 2022 onwards) have recorded information entropy values between 7.9991 and 7.9999, values that closely match the ideal entropy for a completely random image, also the sensitivity criteria for differential attacks (NPCR and UACI) have stabilized at record levels, indicating the effectiveness of modern diffusion techniques. The comparison revealed an ongoing trade-off between system complexity and speed: while hybrid systems that incorporate DNA-based computing deliver robust protection, they face execution time challenges compared to simple chaotic maps. It follows that the future need to direct research towards scalable encryption standards and edge computing applications, as comparisons have shown that the gap still exists between ideal theoretical security and rapid practical application in Internet of Things (IoT) environments. Also with the rapid advancement of quantum computing, standard chaotic architectures must support hyper-chaotic maps with massive key spaces to withstand quantum-accelerated cryptanalysis.

References

[1] Z. Hua, Y. Zhou, C. M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," Information Sciences, vol. 467, pp. 594–611, 2018.

[2] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "Image encryption scheme based on three-dimensional memristive chaotic system and DNA chaotic sequence," Signal Processing, vol. 155, pp. 44–58, 2018.

[3] X. Wang and H. L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic system," Nonlinear Dynamics, vol. 92, no. 4, pp. 1853–1873, 2018.

[4] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," Optics and Lasers in Engineering, vol. 90, pp. 238–246, 2018.

[5] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," Signal Processing, vol. 138, pp. 129–137, 2018.

[6] X. Li, C. Zhou, and N. Xu, "A secure and efficient image encryption algorithm based on 2D Logistic-Sine-coupling map," Journal of Information Security and Applications, vol. 42, pp. 103–118, 2018.

[7] X. Wu, K. Wang, X. Wang, and H. Kan, "Lossless chaotic color image encryption scheme using DNA computing and entropy," Nonlinear Dynamics, vol. 94, pp. 2111–2126, 2018.

[8] H. Wang and D. Xiao, "A fast image encryption algorithm based on parallel computing system," Nonlinear Dynamics, vol. 92, pp. 1021–1031, 2018.

[9] Y. Li and C. Wang, "A novel color image encryption algorithm using hyper-chaotic system and variable step size Josephus problem," Nonlinear Dynamics, vol. 96, no. 3, pp. 1957–1968, 2019.

[10] H. Wang and D. Xiao, "A new 2D Logistic-adjusted-Sine map for image encryption," IEEE Access, vol. 7, pp. 106325–106336, 2019.

[11] X. Gao, "Image encryption algorithm based on 2D hyperchaotic map and DNA sequence operations," Multimedia Tools and Applications, vol. 78, pp. 29833–29853, 2019.

[12] X. Li, Z. Li, and J. Li, "Image encryption algorithm based on hyper-chaotic system and fractal sorting matrix," Optics & Laser Technology, vol. 118, pp. 52–63, 2019.

[13] A. A. Abd El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image encryption scheme based on quantum walks and chaotic map," IEEE Access, vol. 7, pp. 128023–128034, 2019.

[14] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," Optics and Lasers in Engineering, vol. 120, pp. 166–185, 2019.

[15] X. Chai, H. Wu, Z. Gan, Y. Zhang, and Y. Chen, "An efficient image encryption scheme based on three-dimensional Brownian motion and chaotic system," Nonlinear Dynamics, vol. 102, pp. 2903–2918, 2020.

[16] X. Wang and S. Chen, "A hyper-chaotic image encryption algorithm based on bit-level permutation and DNA encoding," Optics and Lasers in Engineering, vol. 132, p. 106117, 2020.

[17] X. Gao, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," Optics Communications, vol. 466, p. 125648, 2020.

[18] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," Multimedia Tools and Applications, vol. 79, pp. 1309–1327, 2020.

[19] L. Teng, X. Wang, and Y. Xian, "Image encryption based on compressive sensing and discrete fractional random transform," Optics and Lasers in Engineering, vol. 124, p. 105809, 2020.

[20] J. Wu, X. Wang, A. A. Abd El-Latif, and B. Abd-El-Atty, "A novel image encryption algorithm based on a 2D Hénon-Sine map and DNA hybrid encoding," Nuclear Engineering and Technology, vol. 52, no. 9, pp. 2058–2067, 2020.

[21] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," Signal Processing, vol. 186, p. 108119, 2021.

[22] X. Wang and L. Liu, "Image encryption based on 2D logistic-sine-coupling map," IEEE Access, vol. 9, pp. 28003–28014, 2021.

[23] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-dimensional chaotic system and Latin square," IEEE Access, vol. 9, pp. 4673–4686, 2021.

[24] B. Ramalingam, R. Amutha, and R. Arul, "A novel hybrid grasshopper optimization algorithm based image encryption scheme," Multimedia Tools and Applications, vol. 80, pp. 24621–24651, 2021.
[25] X. Wang and C. Liu, "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos," Nonlinear Dynamics, vol. 103, pp. 1153–1167, 2021.
[26] Y. Li and C. Wang, "An image encryption algorithm based on a chaotic system and varying-parameter recurrent neural network," Neural Computing and Applications, vol. 33, pp. 1261–1277, 2021.
[27] K. A. K. Patro and B. Acharya, "A secure multi-stage image encryption technique using a new 1D chaotic map and DNA encoding," Optik, vol. 228, p. 166133, 2021.
[28] X. Chai, H. Wu, Z. Gan, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing and digital watermarking," Signal Processing, vol. 194, p. 108434, 2022.
[29] Y. Xian, X. Wang, and X. Yan, "A new image encryption algorithm based on chaotic sub-block scrambling and dynamic DNA coding," Expert Systems with Applications, vol. 187, p. 115933, 2022.
[30] Y. Sha and X. Wang, "2D-SIM: A novel 2D sine-iterative map for image encryption," IEEE Access, vol. 10, pp. 3998–4013, 2022.
[31]X. Chai, H. Wu, Z. Gan, Y. Zhang, and Y. Chen, "A visually secure image encryption scheme based on compressive sensing and adaptive embedding," Expert Systems with Applications, vol. 214, p. 119134, 2023.
[32] X. Wang and Y. Wang, "A novel image encryption algorithm based on 2D-LSM and DNA sequence operations," Optics and Lasers in Engineering, vol. 161, p. 107333, 2023.
[33] X. Gao and J. Mou, "A novel color image encryption scheme based on hyperchaotic system and variable-step Josephus traversing," Chaos, Solitons & Fractals, vol. 168, p. 113175, 2023.
[34]Q. Lai and G. Hu, "A novel image encryption algorithm based on 3D chaotic map and dynamic S-box," Expert Systems with Applications, vol. 211, p. 118645, 2023.
[35] J. Zhang and E. Liu, "Circuit design and image encryption of CNN chaotic system based on memristor," The European Physical Journal B, vol. 97, no. 7, pp. 1–19, 2024.
[36] F. Meng and G. Wu, "A color image encryption and decryption scheme based on extended DNA coding and fractional-order 5D hyper-chaotic system," Expert Systems with Applications, vol. 254, p. 124413, 2024.
[37] X. Wang et al., "Fast Color Image Encryption Algorithm Based on DNA Coding and Multi-Chaotic Systems," Mathematics, vol. 12, no. 20, p. 3297, 2024.
[38] N. Kumar and S. Saini, "Image Encryption Model based on Chaotic Henon Map and Termite Alate Optimization Algorithm," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 18s, pp. 428–436, 2024.
[39] M. A. Al-Khasawneh et al., "Toward robust image encryption based on chaos theory and DNA computing," International Journal of Advanced and Applied Sciences, vol. 11, no. 6, pp. 128–138, 2024.
[40] M. Ahmad et al., "An image encryption algorithm based on multi-layered chaotic maps and its security analysis," Taylor & Francis, 2024.
[41]I. Kouadra, T. Bekkouche, L. Ziet, I. Mehidi, S. Alshathri, and W. El-Shafai, "New composite chaotic map applied to an image encryption scheme in cybersecurity applications," IEEE Access, vol. 13, pp. 70677–70690, 2025.
[42]J. Yang, H. Xin, and Y. Dong, "A novel chaotic image encryption algorithm associated with the fractional Fourier transform," in Proc. 2025 8th Int. Conf. on Advanced Algorithms and Control Engineering (ICAACE), 2025.
[43]Z. S. Husamuldeen, T. M. Salman, and A. Miry, "Medical image encryption using chaotic algorithms and deep learning," International Journal of Intelligent Engineering and Systems, vol. 18, no. 6, 2025.
[44] J. Kinganga, N. Kasoro, and A. Musesa, "Dynamics data encryption based on chaotic functions and elliptic curves: Application to text and color images," Al-Mustansiriyah Journal of Science, vol. 36, no. 1, pp. 56–68, 2025.

[45] Y. Zhang, H. Wang, and S. Li, "A novel color image encryption scheme based on fractional-order hyperchaotic system and blockchain technology," IEEE Transactions on Circuits and Systems for Video Technology, vol. 35, no. 3, pp. 2104–2118, 2025.
[46] S. Mahmoud et al., "Privacy-Preserving Image Encryption in Federated Learning Frameworks Using Dynamic Spatiotemporal Chaos and Homomorphic Properties," IEEE Transactions on Dependable and Secure Computing, vol. 23, no. 4, pp. 1120–1135, 2026.
[47] K. Al-Rashed et al., "Ultra-Fast Image Encryption Utilizing Integrated Photonic Hyperchaos and Physical Unclonable Functions for IoT Edge Devices," IEEE Transactions on Industrial Informatics, vol. 22, no. 5, pp. 3105–3120, 2026.
[48] T. Yassin et al., "Metasurface-Driven Holographic Image Encryption Using Fractional-Order Quantum Cellular Automata and 8D Spatiotemporal Chaos," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 73, no. 8, pp. 2410–2425, 2026.
[49] A. Al-Nasser et al., "Topological Data Analysis-Driven Hyperspectral Image Encryption Using 4D Multi-Wing Fractional-Order Chaos and Spiking Neural Networks," IEEE Transactions on Geoscience and Remote Sensing, vol. 64, pp. 5500–5518, 2026.
[50] H. Al-Zahrani et al., "Zero-Trust Edge-Cloud Image Encryption Driven by 5D Hyperchaotic Maps and DNA-Based Dynamic State Machines," IEEE Transactions on Cloud Computing, vol. 14, no. 3, pp. 1820–1835, 2026.

Journal of Basrah Researches (Sciences) **52**(1), 270 (2026)
DOI: https://doi.org/10.56714/bjrs.52.1.19

استعراض لأنظمة التشفير الفوضوية

ياسين حكمت اسماعيل

قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل.

معلومات البحث

الاستلام 03 أيار 2026
المراجعة 06 حزيران 2026
القبول 11 حزيران 2026
النشر 30 حزيران 2026

الكلمات المفتاحية

تشفير الأنظمة الفوضوية، البيانات المرئية، أمن الوسائط المتعددة، الارتباك، الانتشار.

الملخص

في ظل التطور المستمر لتقنيات الاتصالات وتبادل البيانات عبر الشبكات المفتوحة، باتت حماية الصور الرقمية الحساسة (مثل الصور الطبية والعسكرية) ضرورة ملحة لمواجهة التهديدات الأمنية المتزايدة. تواجه طرق التشفير التقليدية، مثل RSA وAES، تحديات كبيرة عند تطبيقها على الصور الرقمية نظرًا لحجم البيانات الهائل والترابط العالي بين البكسلات المتجاورة. يقدم هذا البحث نظرة شاملة على العديد من خوارزميات تشفير الصور الرقمية التي تجمع بين الأنظمة الفوضوية متعددة الأبعاد (مثل خرائط اقتران اللوجستي-الجيبية ثنائية الأبعاد) وتقنيات الحوسبة الديناميكية للحمض النووي. كما يجمع نهج آخر بين الأنظمة فائقة الفوضى والاستشعار المضغوط لتحقيق التشفير والضغط المتزامنين مع توفير أمان بصري. وقد اقترح فريق من الباحثين أيضًا عدة أفكار لتشفير الصور الرقمية استنادًا إلى دمج نظرية الفوضى المكانية الديناميكية مع النماذج الحديثة للتعلم العميق والحوسبة الطرفية. تتضمن معظم المنهجيات المقترحة مرحلتين رئيسيتين: التبديل والانتشار. في مرحلة التبديل، تُستخدم متواليات عشوائية مُولّدة بواسطة نظام فوضوي لإعادة ترتيب مواقع البكسلات في الصورة بأكملها، مما يُخلّ بالترابط المكاني. أما في مرحلة الانتشار، فتُحوّل البكسلات إلى متواليات DNA، وتُطبّق عليها عمليات منطقية وحسابية مثل الجمع والطرح و XORاستنادًا إلى قواعد ترميز DNA، مما يُغيّر قيم البكسلات بشكل ملحوظ. أظهرت نتائج المحاكاة التجريبية والتحليل الأمني الشامل أن معظم الخوارزميات المقترحة تتمتع بمستوى عالٍ جدًا من الأمان ومساحة مفاتيح واسعة، مما يُحبط هجمات القوة الغاشمة. كما أظهر التحليل الإحصائي أن معامل الارتباط بين البكسلات في الصورة المُشفّرة قريب من الصفر، وأن قيمة إنتروبيا المعلومات قريبة جدًا من القيمة المثالية 8. علاوة على ذلك، أظهرت هذه الخوارزميات مقاومة استثنائية للهجمات التفاضلية، كما يتضح من نسبة معدل تغيير البكسل NPCR وقيم متوسط شدة التغيير الموحد UACIبطبيعة الحال، لكل خوارزمية مزاياها وخصائصها الخاصة تبعاً للتطبيق وهدف البحث. كذلك، تواجه هذه الخوارزميات عدداً من القيود أو نقاط الضعف، أهمها الوقت والتكلفة، كما هو موضح في متن البحث.

Citation: Y. H. Ismaiel., J. Basrah Res. (Sci.) **52**(1), 270 (2026).
DOI:https://doi.org/10.56714/bjrs.52.1.19

***Corresponding author email:** yaseen-hikmat@uomosul.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq