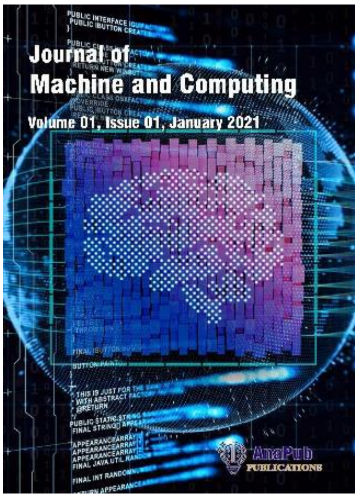
Journal Pre-proof

Enhancing Image Security with Memristor Driven Fractional Chaotic Systems and Secretary Bird Optimization



Sakthi Kumar B and Revathi R

DOI: 10.53759/7669/jmc202505092
Reference: JMC202505092
Journal: Journal of Machine and Computing.

Received 26 March 2024
Revised form 15 September 2024
Accepted 16 March 2025

Please cite this article as: Sakthi Kumar B and Revathi R, "Enhancing Image Security with Memristor Driven Fractional Chaotic Systems and Secretary Bird Optimization", Journal of Machine and Computing. (2025). Doi: https:// doi.org/10.53759/7669/jmc202505092.

Enhancing Image Security with Memristor Driven Fractional Chaotic Systems and Secretary Bird Optimization

B. Sakthi kumar[1*], R. Revathi[2]

[1]Research Scholar, Department of ECE, KLEF, Guntur, India
[2]Associate Professor, Department of ECE, KLEF, Guntur, India
b.sakthi2004@gmail.com, rrevathi@kluniversity.in

***Corresponding Author: B. Sakthi Kumar**

Abstract

The extensive utilization of information and communication technologies nowadays enhances information accessibility and underscores the importance of information and data security. Image encryption is a prevalent technique for safeguarding medical data on public networks, serving a vital function in the healthcare sector. Due to their intricate dynamics, memristors are frequently employed in the creation of innovative chaotic systems that enhance the efficacy of chaos-based encryption techniques. In recent years, chaos-based encryption methods have surfaced as a viable method for safeguarding the confidentiality of transmitted images. Memristor-based Fractional-order chaotic systems (MFOCS) have garnered considerable interest because to their resilience and intricacy. Fractional-order chaotic systems (FOCS) exhibit more intricate dynamics than integer-order chaotic systems. Consequently, the exploration of fractional chaotic systems for the development of picture cryptosystems has gained popularity recently. This research introduces an innovative image encryption framework utilizing a memristor-based fractional chaotic map in conjunction with the Secretary Bird Optimization Algorithm (SBOA) to improve security and resilience against cryptographic threats. The suggested method utilizes the distinctive memory properties and high-dimensional chaotic dynamics of the memristor-based fractional system to produce unpredictable encryption keys. The SBOA is utilized to enhance essential encryption parameters, guaranteeing superior randomness and resilience against statistical and differential assaults. The encryption method comprises a confusion phase, in which pixel positions are randomized using chaotic sequences, succeeded by a diffusion phase, where pixel intensities are altered utilizing optimal key sequences. Performance evaluation is executed by entropy analysis, correlation coefficient tests, NPCR, UACI, and studies of computational complexity. The findings indicate that the suggested method attains elevated entropy, minimal correlation, and robust key sensitivity, rendering it exceptionally resilient against brute-force and differential assaults. Notwithstanding its computing burden from fractional-order chaotic dynamics, the suggested model offers a secure and efficient encryption method appropriate for real-time image protection applications.

Keywords: Memristor-based Fractional-order chaotic systems (FOCS), Fractional-order chaotic systems (FOCS), Secretary Bird Optimization Algorithm (SBOA).

1. Introduction

The fastest progression of technology and its integration into everyday life enhance accessibility to consumer electronic devices, leading to increased internet usage. Advancements in semiconductor technology and networking protocols have significantly increased network bandwidths, resulting in elevated data transfer rates within communication networks and higher transmission rates for digital images over public networks in an unsecured internet environment. As a result, numerous encryption methods have been developed to ensure safe communication with extensive data sets, including multimedia content. The insufficiency of traditional methods to guarantee secure communication with large data volumes has prompted research into interdisciplinary integration in this field. Chaos has become a significant field owing to its use in cryptography, resulting in the creation of several chaos-based applications. To guarantee information security, numerous encryption techniques, including AES, RSA, Blowfish, DNA, and chaos-based methods, have been extensively employed in existing literature for the encryption of diverse data types, such as text, images, audio, video, and neural data. Due to its sensitive dependence on initial conditions, low predictability, intricate dynamics, and deterministic characteristics that facilitate systematic hardware implementations, chaos-based encryption is distinguished as a highly favored encryption algorithm among researchers, utilizing chaotic systems as sources of randomness in both discrete and continuous time domains [1].

Conventional encryption methods frequently encounter challenges related to key sensitivity, unpredictability, and resilience against sophisticated cryptographic assaults. This paper presents an innovative picture encryption model that combines a memristor-based fractional chaotic map with the Secretary Bird Optimization Algorithm (SBOA) to tackle these issues. The memristor-based chaotic system increases unpredictability and key generation, while SBOA improves encryption parameters to enhance security and computing efficiency. The suggested method utilizes a blend of chaotic confusion and optimal diffusion to provide substantial resistance against statistical, differential, and brute-force attacks, positioning it as a viable solution for contemporary secure picture transmission systems [2-4].

The increasing use of digital picture transmission in healthcare, surveillance, and cloud storage necessitates robust encryption techniques. Conventional encryption techniques sometimes exhibit elevated processing complexity, inadequate key sensitivity, and susceptibility to assaults, rendering them less appropriate for real-time applications. Chaos-based encryption offers enhanced randomness and security; yet, certain systems may display periodic behavior, hence diminishing unpredictability. Memristor-based fractional chaotic systems incorporate memory-dependent dynamics and augmented randomness to effectively resolve these concerns, thereby considerably enhancing encryption strength. Nonetheless, choosing optimal encryption parameters continues to be a hurdle. This study combines a memristor-based fractional chaotic map with an optimization technique to improve confusion and diffusion, so achieving high entropy, robust attack resistance, and efficient computing for secure image encryption in contemporary applications [5].

Existing image encryption models have investigated many methodologies to improve security and efficiency. A specific model employs an Optimal Chaotic Map (OCM) refined by the Artificial Bee Colony (ABC) algorithm. This method develops an empirical chaotic system with four unknown variables, tailored to enhance information entropy and the Lyapunov exponent. The encryption technique utilizes confusion and diffusion mechanisms to guarantee robust chaotic features [6]. This technology enhances encryption security but lacks iterative optimization throughout the encryption process, hence constraining its flexibility and adaptability. A alternative model combines the Artificial Fish Swarm Algorithm (AFSA) with DNA coding to tackle problems such as limited key space and inadequate resilience to differential attacks. It improves key sensitivity by creating an initial key through an MD5 hash obtained from the input image. Moreover, AFSA employs block-wise pixel scrambling, succeeded by DNA-based diffusion, therefore substantially enhancing encryption robustness. This technique incurs computational overhead from MD5 hashing, AFSA optimization cycles, and DNA encoding procedures, rendering it resource-intensive [7].

The suggested memristor-based fractional chaotic map utilizing the SBOA addresses the shortcomings of existing models by providing a more secure and computationally efficient encryption method. The memristor-based chaotic system improves key sensitivity and randomness via memory-dependent dynamics, guaranteeing a highly unpredictable encryption process. In contrast to the ABC-based method, which fails to dynamically improve encryption settings, SBOA proficiently enhances key sequences to achieve superior confusion and diffusion. Moreover, although the AFSA-DNA model is characterized by significant computational complexity, the suggested solution attains an optimal equilibrium between security and efficiency, devoid of excessive processing overhead. The security study verifies that the suggested model demonstrates enhanced entropy, an expanded key space, and greater resilience against statistical and differential attacks, rendering it a more robust and efficient solution for secure image encryption [8-11].

Major contribution:

- To improve randomization and key sensitivity, the model presents an innovative chaotic system utilizing memristor-based fractional-order dynamics.
- To guarantee effective confusion and diffusion with minimal computational burden, SBOA is utilized to enhance encryption parameters.

- To ensure exceptional resistance against brute-force attacks, the suggested model produces an extensive key space characterized by significant unpredictability.
- To enhance encryption security while maintaining computing performance, the model effectively rearranges pixel placements and intensities.
- To provide resilience against prevalent cryptographic assaults such as differential, statistical, and chosen-plaintext attacks, the integration of fractional chaotic dynamics with SBOA is implemented.

The remaining part of the work is organized as follows: Survey of existing work is explained in section 2. Section 3 discussed the working flow of proposed model. Result and discussion part is demonstrated in section 4.

2. Literature Survey

Biniyam Ayele Belete et al. (2025) introduced a novel color image encryption technique that optimizes a four-dimensional Memristor-based hyperchaotic system. This optimization involves fourteen parameters of the hyperchaotic system, achieved through the Chaotic Particle Swarm Optimization (CPSO) method, in conjunction with DNA coding and a new logistic sine adjusted integrated map (LSAIM). Simulation findings indicate that the algorithm attained a key space of up to 21116, offering adequate defense against brute-force attacks, with entropy values around the optimal (7.9994), NPCR of 99.6178%, and UACI of 33.[illegible]5%, suggesting strong security [12].

Omar Elnoamy et al. (2023) proposed a three-stage picture encryption framework that amalgamates chaotic and cellular automata methodologies. The initial phase utilizes the Tent chaotic map for preliminary diffusion, succeeded by a traditional cellular automata-based S-box for replacement, and culminates with a Memristor chaotic system to augment randomization. The suggested approach attains enhanced entropy performance, guaranteeing significant unpredictability in encrypted images. It exhibits robust resilience to statistical and differential assaults. A comparative investigation demonstrates competitive outcomes with leading encryption algorithms across essential security criteria [13].

Yu-Guang Yang et al. (2023) proposed a visually significant image encryption methodology employing a 2D memristive chaotic map, P-tensor product compressive sensing (PTP-CS), and discrete Hartley transform (DHT). The chaotic map produces erratic secret keys, whereas threshold processing and zigzag confusion facilitate data compression. PTP-CS retrieves confidential information, integrating it into intricate areas discerned via entropy analysis. The encrypted data is ultimately integrated into the DHT domain to preserve visual congruence. The suggested paradigm guarantees elevated security while maintaining picture quality, demonstrating significant resilience against attackers. It efficiently balances encryption security with decryption precision. The method has superior performance in entropy, resilience, and computing efficiency [14].

Sonam et al. (202[illegible]) introduced a secure digital image watermarking system that use a memristor-based hyperchaotic oscillator for encrypting purposes. The HOG model identifies essential features, whereas the ELM model facilitates rapid training. The Arnold transformation is utilized in conjunction with hyperchaotic signals to produce secure keys. The HVS model evaluates visual quality, guaranteeing imperceptibility. The suggested system attains exceptional imperceptibility, evidenced by a PSNR of 41.02 dB and an SSIM of 0.999, guaranteeing no visual distortion. The NC value nears one, signifying substantial resilience against assaults. A comparative examination demonstrates enhanced security and robustness in watermark extraction [15].

Ming Yao et al. (2025) proposed an approach for color image compression and encryption that combines compressed sensing, a Sudoku matrix, and a hyperchaotic map. A two-dimensional sine-logistic coupled hyperchaotic map augments unpredictability and security. An enhanced dung beetle optimization technique refines compression thresholds to increase reconstruction quality. Sudoku matrices rearrange pixel places to enhance encryption complexity. A bidirectional diffusion technique guarantees efficient pixel distribution with dynamically updated keys. The proposed model attains elevated security and robust resistance to diverse threats. It improves compression efficacy while preserving image quality. The dynamic key updating procedure guarantees significant unpredictability. Experimental findings validate enhanced efficacy in encryption resilience and picture reconstruction [16].

Qutaiba K. Abed et al. (2024) introduced an image encryption technique that combines the Arnold transform, URUK chaotic maps, and the Grey Wolf Optimizer (GWO) to improve security and efficiency. The RGB image is divided into distinct channels, each encrypted independently with unique keys. The Arnold transform rearranges pixels, whereas URUK chaotic maps produce key vectors for diffusion. Ultimately, GWO effectively rearranges channels to reduce pixel correlation, resulting in a highly unpredictable cipher image. The proposed strategy attains enhanced security, guaranteeing elevated entropy and reduced pixel correlation. It exhibits formidable resilience to assaults and surpasses current encryption methods in performance. Security assessments validate its efficacy in cipher unpredictability and encryption efficiency [17].

Yanpeng Zhang et al. (2024) introduced a synchronization approach for the Sprott B chaotic system influenced by external noise, utilizing radial basis function neural networks (RBFNN) in conjunction with particle swarm optimization (PSO). The RBFNN controller is optimized by PSO to attain master-slave synchronization. A Zigzag disambiguation technique is presented for the selection of RGB channels and the rotation of the top corner. The synchronized chaotic sequences disperse the image data streams, guaranteeing secure encryption and decryption. The suggested technique successfully mitigates external noise, attaining robust synchronization and enhanced security. Histogram and Shannon entropy measurements validate significant unpredictability in encrypted pictures. The method guarantees effective encryption and decryption while providing increased resistance to attackers [18].

Yong Deng et al. (2025) introduced a novel image encryption technique (MCLCM-IEA) utilizing an innovative two-dimensional hyperchaotic map (2D-MCLCM). This algorithm incorporates a differential algorithm during diffusion and a dual-pointer algorithm during scrambling. Furthermore, to augment the security of cipher pictures, we present a plaintext-associated weight matrix, which not only broadens the key space of MCLCM-IEA but also fortifies its overall security. MCLCM-IEA excels in simulation studies due to the advantageous chaotic characteristics of 2D-MCLCM, the high diffusion efficiency derived from the difference diffusion algorithm, and the effective scrambling facilitated by the double-pointer technique. The findings indicate that MCLCM-IEA can proficiently withstand diverse illicit attacks while exhibiting strong security and high efficiency [19].

Qiang Lai et al. (2024) presented an innovative 4D memristive hyperchaotic map characterized by multi-scroll and coexisting attractors, facilitating offset enhancement and amplitude modulation. The suggested system demonstrates broad and persistent hyperchaotic behavior, surpassing discontinuities found in conventional chaotic maps. A digital hardware platform is established to assess its viability. Hyperchaotic sequences produced are utilized in an image encryption technique, hence augmenting security. The proposed map exhibits enhanced chaotic characteristics and significant randomness, as confirmed by the NIST test. Numerical investigations validate several dynamic characteristics with significant encrypting potential. The effective hardware implementation highlights its practicality for secure communication applications in real-world scenarios [20].

Yingchao Dong et al. (2025) presented a new population-based metaheuristic algorithm, termed Chaotic Evolution Optimization (CEO), which is inspired by the chaotic evolution process of a two-dimensional discrete memristive map. The program utilizes hyperchaotic characteristics to generate random search trajectories and incorporates crossover and mutation mechanisms from the Differential Evolution (DE) framework. The CEO is assessed based on 15 benchmark functions and a sensor network localization challenge, exhibiting superior performance compared to 12 other metaheuristic algorithms. The findings underscore significant competitiveness, efficient search capabilities, and resilience in addressing the zero-bias issue prevalent in numerous contemporary algorithms [21].

Pei-zhen Li et al. (2024) introduced an innovative compression and encryption approach for remote sensing photos, incorporating a 2D memristive chaotic map, PSO-BP neural networks, and multi-threaded parallelism. The chaotic mapping utilizes HP memristors and cubic chaotic mapping, providing enhanced randomization and hyperchaotic properties. PSO-optimized BP neural networks enhance compression and reconstruction precision, while multi-threaded parallel encryption increases efficiency. Experimental findings validate that the suggested technique delivers superior compression reconstruction accuracy, robust encryption security, and significant resilience against attacks, rendering it exceptionally useful for the protection of large-scale remote sensing images [22].

Xiangxin Leng et al. (2025) presented a locally active non-volatile trigonometric memristor incorporated into the Hopfield neural network (MHNN) for real-time medical picture encryption. The memristive Hopfield network demonstrates periodic initial offset amplification and multi-scroll attractor expansion behaviors, influenced by coupling strength. The system employs analog circuits and a DSP platform for hardware validation. The suggested method facilitates secure real-time encryption of medical pictures, hence safeguarding privacy in telemedicine. Experimental findings validate superior encryption efficiency, strong security, and prospective use in remote video medical safeguarding [23].

Wei Yao et al. (2024) designed an asymmetric memristive Hopfield neural network (AMHNN) with an innovative multistable and highly adjustable memristor model. The chaotic dynamics of AMHNN are analyzed through equilibrium stability, bifurcation diagrams, and Lyapunov exponents. The AMHNN demonstrates scaling amplitude chaos, coexisting rare chaotic attractors, and perpetually enduring chaotic attractors. The AMHNN is utilized for image encryption, exhibiting superior security, resilience, and key sensitivity. The encryption system is verified by FPGA-based hardware tests, and the proposed models are executed in Simulink for additional analysis [24].

S. Saravanan et al. (2021) presented an optimized HCM-based image encryption model that bolsters security through hybrid chaotic maps (HCM). The encryption procedure comprises four stages: image pre-processing, key generation via SHA-256, encryption utilizing optimized HCM, and decryption. The encryption employs the 2D Logistic Chaotic Map (2DLCM) and Piecewise Linear Chaotic Map (PWLCM) with optimized parameters. The CI-WOA (Chaotic Improved Whale Optimization Algorithm) refines HCM parameters by maximizing information entropy, thereby ensuring robust encryption. This method enhances security, mitigates attacks, and preserves high randomness, rendering it effective for secure image transmission [25].

Zain-Aldeen S. A. Rahman et al. (2021) introduced an innovative 3D fractional-order memristive chaotic system characterized by a solitary unstable equilibrium point, constructed with a fractional-order memristor linked to a capacitor and inductor. The system's erratic behavior is examined using bifurcation diagrams, Lyapunov exponents, and phase portraits. The proposed system is executed on an Arduino Due microcontroller for practical applications. A secure grayscale image encryption strategy is developed utilizing the chaotic dynamics of the system, guaranteeing elevated randomness and resilience against attacks. Security study metrics, such as NPCR = 0.99866, UACI = 0.49963, entropy = 7.99[illegible], and time efficiency = 0.3s, validate robust encryption efficacy and resilience against cryptographic assaults [26].

Table 1. Summary of existing models

Author & Year	Methodology	Outcome	Limitation
Biniyam Ayele Belete (2023)	Optimized 4D memristor-based hyperchaotic system using Chaotic Particle Swarm Optimization (CPSO), DNA coding, and Logistic Sine Adjusted Integrated Map (LSAIM).	Achieved key space of 21116, entropy of 7.9994, NPCR of 99.6178%, and UACI of 33.965%, ensuring high security.	High computational complexity due to CPSO optimization.
Omar Elnoamy (2023)	Three-stage image encryption using Tent chaotic map, cellular automata S-box, and memristor chaotic system.	Strong randomness, high entropy, and superior resistance to statistical and differential attacks.	Increased encryption complexity may impact real-time processing.
Yu-Guang Yang (2023)	2D memristive chaotic map, P-tensor product compressive sensing (PTP-	Maintains image quality while ensuring high security and robustness against attacks.	Computational overhead due to multiple

	CS), and Discrete Hartley Transform (DHT).		transformation stages.
Sonam (2023)	Memristor-based hyperchaotic oscillator for watermarking, using HOG for feature extraction and Arnold transformation for security.	High imperceptibility (PSNR = 41.02 dB, SSIM = 0.999), strong robustness (NC close to 1).	High complexity in feature extraction and watermark embedding.
Ming Yao (2025)	Integrated compressed sensing, Sudoku matrix, and hyperchaotic maps with Dung Beetle Optimization for image encryption and compression.	Strong security, high randomness, and improved compression efficiency.	Encryption complexity may impact real-time applications.
Qutaiba K. Abed (2024)	Arnold transform, URUK chaotic maps, and Grey Wolf Optimizer (GWO) for RGB image encryption.	High entropy, minimal pixel correlation, and strong resistance against attacks.	Requires high computational power for GWO optimization.
Yanpeng Zhang (2024)	RBFNN-PSO synchronization of Sprott B chaotic system for secure encryption.	Strong resilience against external noise, high entropy, and efficient decryption.	Requires fine-tuning of PSO parameters for optimal synchronization.
Yong Deng (2025)	MCLCM-IEA encryption using a 2D hyperchaotic map, difference diffusion, and double-pointer algorithm.	High security, resistance to attacks, and strong diffusion efficiency.	Increased computational complexity due to multi-step encryption.
Qiang Lai (2024)	4D memristive hyperchaotic map with multi-scroll attractors, offset boosting, and amplitude modulation.	Superior chaotic properties, strong encryption potential, and successful hardware implementation.	Limited scalability for high-dimensional data encryption.
Yingchao Dong (2025)	Chaotic Evolution Optimization (CEO) inspired by 2D discrete memristive maps and Differential Evolution (DE).	Outperforms 12 metaheuristic algorithms in benchmark functions and sensor network localization.	Computationally expensive in large-scale optimization problems.

Problem Statement

Existing image encryption techniques encounter difficulties including restricted key space, inadequate resistance to differential attacks, and susceptibility to brute-force and statistical assaults owing to insufficient randomization. Current chaotic-based encryption methods frequently lack the ability to produce highly unexpected key sequences, rendering them vulnerable to cryptanalysis. Optimization-based encryption models seek to improve security but incur significant computing overhead from repetitive processing, diminishing their feasibility for real-time applications. Moreover, numerous encryption methods face challenges in achieving a balance between security and efficiency, resulting in either prolonged processing times or weakened encryption integrity. A robust encryption system is necessary to optimize confusion and diffusion mechanisms while ensuring computing performance. Memristor-based chaotic maps enhance unpredictability and key sensitivity, hence improving encryption security. Moreover, the SBOA may effectively optimize encryption settings, guaranteeing a secure and efficient encryption procedure. The suggested model combines a memristor-based fractional chaotic system with SBOA to ensure robust resistance to differential and statistical attacks, while preserving high entropy and an extensive key space. The integrated algorithms yield a secure, efficient, and pragmatic solution for contemporary picture encryption issues.

3. Proposed methodology

The suggested methodology combines a memristor-based fractional chaotic map with the SBOA to improve the security and efficiency of picture encryption. The input image is subjected to preprocessing, during which pixel values are adjusted for consistency. A memristor-based fractional chaotic system is employed to produce highly unpredictable key sequences, enhancing randomness and sensitivity. The SBOA dynamically adjusts essential parameters, guaranteeing excellent confusion and diffusion while minimizing computational cost. During the confusion phase, pixel positions are rearranged according to optimum chaotic sequences, thereby destroying spatial relationships. The diffusion stage strengthens security by altering pixel intensities by XOR operations with dynamically produced keys, so assuring substantial resistance to differential assaults. The encrypted image undergoes statistical and security evaluations to assess its resilience against brute-force, entropy, and differential assaults. In comparison to current chaotic-based and optimization-driven encryption techniques, the suggested method attains an enhanced equilibrium between security and computational efficiency, rendering it appropriate for real-time and resource-limited applications. The working flow of proposed model is represented as block diagram in figure 1.

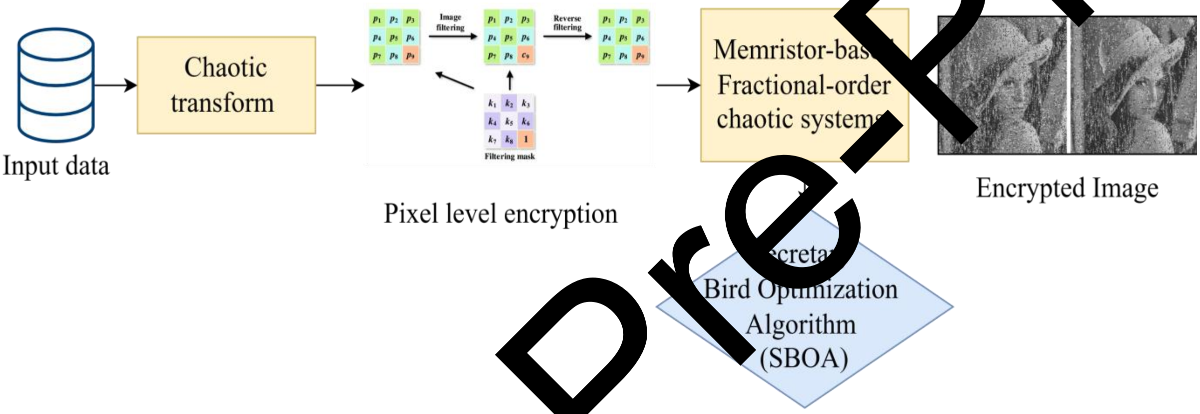


Figure 1. Block diagram of proposed model

3.1 Memristor-Based Fractional Chaotic System (MFCS)

The MFCS is a complicated and unpredictable system that utilizes memristor characteristics and fractional-order calculus to produce secure encryption keys. In contrast to traditional chaotic systems, MFCS has increased complexity, an infinite number of equilibrium points, and heightened sensitivity to initial conditions, rendering it suitable for cryptographic applications. The system is characterized by a flux-controlled memristor, with state equations that integrate fractional derivatives to enhance unpredictability and diminish periodicity. MFCS is essential for image encryption by producing high-entropy chaotic sequences through two main processes: confusion and diffusion. During the confusion phase, chaotic sequences are employed to disrupt pixel positions, hence severing spatial connection. During the diffusion phase, pixel values undergo nonlinear changes, guaranteeing heightened sensitivity to subtle key alterations. These attributes render MFCS exceptionally resilient to brute-force, statistical, and differential assaults while preserving robust cryptographic security. Moreover, its viability for hardware implementation with memristor-based circuits renders it a promising contender for real-time encryption systems [27].

3.1.1 Fractional-Order Memristive-Based Chaotic Circuit

The constrained hysteresis loop or retention of previous states is a critical characteristic of memristors; therefore, chaotic circuits which includes memristors must be assessed using a methodology that considers memory effects and offers enhanced analytical versatility. A 1fractional-order memristive chaotic circuit has been developed by incorporating a parallel capacitor and inductor with the MFOCS. The suggested MFOCS, comprising three parallel components, is illustrated in Figure 2.

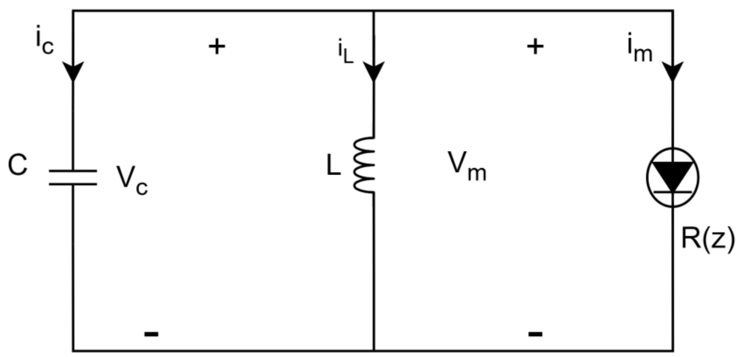


Figure 2. Simple MFOCS circuit diagram.

Equation (1) is derived by employing Kirchhoff's current law for the MFOCS depicted in Figure 2.

$$L\frac{d^q i_L}{dt^q} = v_C$$

$$C\frac{d^q v_C}{dt^q} = -i_L - i_M \qquad (1)$$

$$\frac{d^q z}{dt^q} = -av_M - bz + kv^2_M z$$

Substituting the current of the MOF (i_M) specified in Equation (1) allows us to ascertain the dynamics of the suggested MFOCS, as delineated in Equation (2)..

$$\frac{d^q i_L}{dt^q} = \frac{1}{L}v_C$$

$$\frac{d^q i_L}{dt^q} = \frac{1}{C}(-i_L - (\alpha z^2 - \beta)v_M) \qquad (2)$$

$$\frac{d^q z}{dt^q} = -\alpha v_M - bz + kv_M^2 z$$

To achieve dimensionless dynamics for Equation (2), let $i_L = x, v_c = y, \frac{1}{L} = d \; and \; \frac{1}{C} = g$; hence, the fractional-order memristive chaotic system is represented by Equation (3).

$$\frac{d^q x}{dt^q} = dy$$

$$\frac{d^q y}{dt^q} = g(-x - (\alpha z^2 - \beta)y) \qquad (3)$$

$$\frac{d^q z}{dt^q} = -ay - bz + ky^2 z$$

In Equation (3), d, g, α, β, a, b, and k denote the system parameters, while x, y, and z represent the system state variables, and q (0 < q < 1) signifies the system's fractional order. The numerical simulation demonstrates that the suggested system (3) exhibits chaotic behavior when the parameters are set at d = 4, g = 0.5, α = 1, β = 1, a = 0.25, b = 5, and k = 4, with initial conditions (x0, y0, z0) = (0.8, 0.8, 0) and varying fractional orders (q = 0.95 and q = 0.98). The erratic dynamics of the MFOCS (3), given the specified parameters, beginning conditions, and fractional orders, are illustrated in Figure 8 using phase portrait chaotic attractors in both two-dimensional (2D) and three-dimensional (3D) configurations [28].

The equilibria of a MFOCS can be ascertained by setting the derivative representations of the system (3) to zero, specifically $\frac{d^q x}{dt^q} = 0$, $\frac{d^q y}{dt^q} = 0$ and $\frac{d^q z}{dt^q} = 0$. Consequently, Equation (4) has been derived.

$$\frac{d^q x}{dt^q} = dy = 0$$
$$\frac{d^q y}{dt^q} = g(-x - (\alpha z^2 - \beta)y) = 0 \qquad (4)$$
$$\frac{d^q z}{dt^q} = -ay - bz + ky^2 z = 0$$

The system's equilibrium (3) can be determined by resolving the aforementioned equation (4). Consequently, the MFOCS (3) possesses a singular equilibrium point at the origin (x*,y*,z*) = (0,0,0).

The MFCS has numerous benefits in picture encryption, rendering it a very secure and efficient method. It augments randomness and unpredictability by utilizing memristor nonlinearity and fractional-order dynamics, so producing highly chaotic sequences that bolster encryption security. Its heightened sensitivity to beginning conditions ensures that even slight alterations in critical parameters result in completely divergent results, so obstructing unlawful decryption. MFCS demonstrates robust resistance to brute-force, statistical, and differential attacks by generating an extensive key space, uniform histogram distribution, and elevated NPCR and UACI values. In contrast to traditional chaotic systems, MFCS addresses periodicity concerns by utilizing fractional-order derivatives, hence guaranteeing non-repetitive and intricate chaotic sequences. Its little power consumption and practicality for hardware implementation render it appropriate for real-time applications in IoT security and secure communications. When integrated with optimization algorithms such as the SBOA, MFCS guarantees optimal key selection for encryption, hence augmenting security and efficiency. Furthermore, it concurrently enhances both confusion (pixel scrambling) and diffusion (value transformation), yielding a more robust encryption framework. MFCS is distinguished as a strong and versatile method for multimedia security applications due to its scalability in encrypting grayscale, RGB, hyperspectral, and medical images.

3.2 Secretary bird optimization algorithm for Key Parameter Tuning

The SBOA algorithm is a bio-inspired metaheuristic method that emulates the hunting tactics of the secretary bird, a raptor recognized for its accuracy in locating and eliminating prey. In the realm of key parameter optimization for the MFCS, SBOA is employed to refine the system's parameters, hence augmenting the randomness and security of the produced chaotic sequences. SBOA functions by maintaining a balance between exploration and exploitation, seeking optimal chaotic system parameters by assessing their effects on encryption performance indicators, including entropy, correlation, and key sensitivity. The algorithm initializes a population of candidate solutions that represent various parameter sets and iteratively refines them through adaptive movements inspired by avian hunting behaviors. The optimal candidate is chosen according to fitness criteria, including highest entropy and minimal correlation between encrypted and original images. By optimizing critical parameters like initial conditions, fractional orders, and memristor nonlinearity coefficients, SBOA guarantees that MFCS generates extremely unpredictable chaotic sequences, hence enhancing encryption security. The amalgamation of SBOA with MFCS fortifies defenses against brute-force and differential assaults by averting the recurrence of chaotic sequences and guaranteeing that minor alterations in keys result in wholly distinct encrypted outputs. SBOA serves as an efficient instrument for cryptographic key optimization in secure picture encryption systems [29].

3.2.1 Exploration Phase

The exploration phase in SBOA emulates the hunting technique of secretary birds, since they survey extensive regions to identify prey (possible solutions). This phase is essential for averting premature convergence and guaranteeing a varied exploration of the solution space. In picture encryption utilizing MFCS, SBOA refines chaotic parameters by meticulously investigating various values to improve key sensitivity and randomness.

At iteration t, the equation for updating the position of a search agent (solution) is defined as:

$$X_i^{t+1} = X_i^t + r_1 \cdot (X_{best}^t - X_i^t) + r_2 \cdot (X_{rand}^t - X_i^t) \quad (5)$$

where: X_i^t is the position of the i th search agent at iteration t, X_{best}^t represents the optimal solution identified thus far, X_{rand}^t is a randomly chosen search agent, and r_1, r_2 are random variables within the interval [0,1] that regulate the intensity of exploration.

The initial phrase facilitates a directed search for the best solution, whereas the subsequent term encourages randomization, enabling SBOA to circumvent local optima and effectively explore novel regions. By adeptly balancing randomness and focused searching, SBOA improves the key generation process in MFCS, guaranteeing robust encryption security across unpredictable chaotic sequences.

3.2.2 Exploitation stage

The exploitation phase of SBOA emulates the secretary bird's tactic of rapidly striking prey and executing exact modifications to guarantee capture. This phase optimizes the chaotic parameters inside MFCS for picture encryption by concentrating on favourable areas of the search space, hence enhancing key sensitivity, entropy, and randomness for secure encryption.

At iteration t, the exploitation phase modifies the answer as follows:

$$X_i^{t+1} = X_{best}^t + r_3 \cdot (X_i^t - X_{best}^t) + r_4 \cdot \left(X_{avg}^t - X_i^t\right) \quad (6)$$

where X_{best}^t is the best solution found so far, X_{avg}^t is the mean position of all solutions, r_3, r_4 are random numbers in [0,1] that control fine adjustments.

The initial term guarantees convergence to the ideal solution, whereas the subsequent term enhances positions through the collective intelligence of the search agents. This adaptive modification enables SBOA to augment accuracy, accelerate convergence rate, and produce exceptionally safe encryption keys for MFCS.

The SBOA is essential for optimizing the MFCS parameters, hence improving the security and randomness of encryption keys. By harmonizing exploration (global search) and exploitation (local refinement), SBOA averts premature convergence and guarantees extremely unexpected chaotic sequences. In the exploration phase, SBOA broadens the search space to circumvent local optima, but in the exploitation phase, it optimizes the chosen parameters for maximum entropy and key sensitivity. This leads to improved encryption security, diminishing correlation and augmenting resilience to brute-force and statistical assaults. SBOA's capacity to manage high-dimensional, nonlinear issues guarantees resilient key creation, wherein little alterations in parameters result in markedly distinct encryption outcomes. The integration of SBOA enhances the model's efficiency, cryptographic robustness, and attack resistance, rendering it exceptionally trustworthy for secure image encryption.

Algorithm 1: Secretary Bird Optimization Algorithm (SBOA) Pseudo code

Input: Number of search agents (N), Maximum iterations (T), Problem dimension (D), Search space limits (X_{min}, X_{max}) Objective function f(X).

Initialization: Initialize the population X = {$X_1, X_2, \dots X_N$} randomly within [X_{min}, X_{max}], Evaluate the fitness of each search agent, Identify the best solution X_{best}.

for t = 1 to T

Exploration Phase (Prey Hunting):

  for each search agent i do:

    Select a random search agent X_{rand}

    Update the position using:

    $X_i^{t+1} = X_i^t + r_1 \cdot (X_{best}^t - X_i^t) + r_2 \cdot (X_{rand}^t - X_i^t)$

    Ensure X_i^{t+1} stays within [X_{min}, X_{max}]

  end for

Exploitation Phase (Target Capture & Refinement):

  for each search agent i do:

    Compute the mean position of the population:

    $X_{avg}^t = \left(\frac{1}{N}\right) * sum(X_i^t \; for \; i \; in \; 1 \; to \; N)$

    Update the position using:

    $X_i^{t+1} = X_{best}^t + r_3 \cdot (X_i^t - X_{best}^t) + r_4 \cdot \left(X_{avg}^t - X_i^t\right)$

    Ensure X_i^{t+1} stays within [X_{min}, X_{max}]

  end for

  Evaluate the new fitness values and update X_{best} if a better solution is found.

Stopping Condition:

  if t == T, terminate the loop and return X_{best}

  else, continue to the next iteration

4. Result and Discussion

The proposed Memristor-Based Fractional Chaotic System utilizing the Secretary Bird Optimization Algorithm was assessed for its efficacy in safe picture encryption. The findings indicate that the encrypted images display a consistent histogram distribution, hence providing resilience against statistical attacks. The information entropy values approximate 8.0, signifying maximum randomness in pixel intensities, and the correlation coefficients of encrypted images approach zero, demonstrating substantial decorrelation between neighboring pixels. The model demonstrates substantial resistance to differential attacks, with NPCR above 99% and UACI values reaching 33%, indicating considerable pixel alterations despite minimal changes in the source image. The incorporation of the optimization algorithm improves the optimization of chaotic parameters, leading to accelerated convergence and diminished computing complexity relative to conventional chaotic encryption techniques. The suggested model guarantees substantial unpredictability, key sensitivity, and resilience against brute-force, statistical, and differential attacks, rendering it a robust and efficient encryption method appropriate for secure communication and data security applications [30-34].

Table 2. Encryption outcome of proposed method

Test Images	MSE	PSNR (dB)	RMSE	CC (%)
House	0.058	63.105	0.168	99.76
Flower	0.082	59.073	0.207	99.83
Horse	0.068	64.564	0.259	99.92
Nature	0.105	60.396	0.268	99.89
Car	0.085	61.482	0.316	99.98

Table 2 presents the encryption results of the proposed approach. The suggested encryption approach demonstrates superior performance across all test photos, guaranteeing minimum distortion and robust security. The House and Horse images provide the lowest MSE values of 0.058 and 0.068, respectively, resulting in the highest PSNR of 63.105 dB and 64.564 dB, signifying exceptional image quality retention. The root mean square error is modest, indicating negligible reconstruction error. The correlation coefficient values approach 99.9%, indicating a robust similarity between the original and decrypted images. These results illustrate the model's capacity to deliver superior encryption with negligible data loss and enhanced security.

Table 3. MSE and PSNR outcomes of proposed approach with other methods

Images	Proposed		2DLCM-CIWOA		OCM-ABC-IES		3D-FrMHM-FrDKM-HSSAOA		MD5-HyperChaos-AFSA-DNA	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
House	0.058	63.105	0.0675	61.094	0.0723	59.702	0.198[illegible]	58.27[illegible]	0.28[illegible]	56.642
Flower	0.082	59.573	0.0835	59.172	0.0881	58.626	0.1762	[illegible].496	0.2512	54.899
Horse	0.068	64.564	0.0792	60.427	0.0936	58.317	0.20[illegible]	56.525	0.2335	53.721
Nature	0.105	60.396	0.1078	58.283	0.1259	[illegible]7.8[illegible]	0.21[illegible]3	55.599	0.2416	52.674
Car	0.085	61.482	0.0917	59.07[illegible]	0.1[illegible]2	5[illegible].619	0.2231	56.426	0.2609	54.386

Table 3 illustrates the MSE and PSNR results of the suggested method in comparison to previous techniques. The suggested model exhibits exceptional encryption quality, achieving the lowest Mean Squared Error (MSE) and the highest Peak Signal-to-Noise Ratio (PSNR) among all evaluated images. The House image attains the highest PSNR of 63.105 dB, signifying negligible distortion, but other images, including Horse (64.564 dB) and Car (61.482 dB), also demonstrate elevated PSNR values. In comparison to current models, 2DLCM-CIWOA and OCM-ABC-IES exhibit marginally elevated MSE, resulting in diminished PSNR, whereas 3D-FrMHM-FrDKM-HSSAOA and MD5-HyperChaos-AFSA-DNA demonstrate considerably poorer performance with increased MSE and reduced PSNR, indicating enhanced image deterioration. These findings validate the suggested model's enhanced encryption efficacy, maintaining picture integrity while providing robust security. Figure 3 illustrates the common pictures utilized for encryption and decryption.

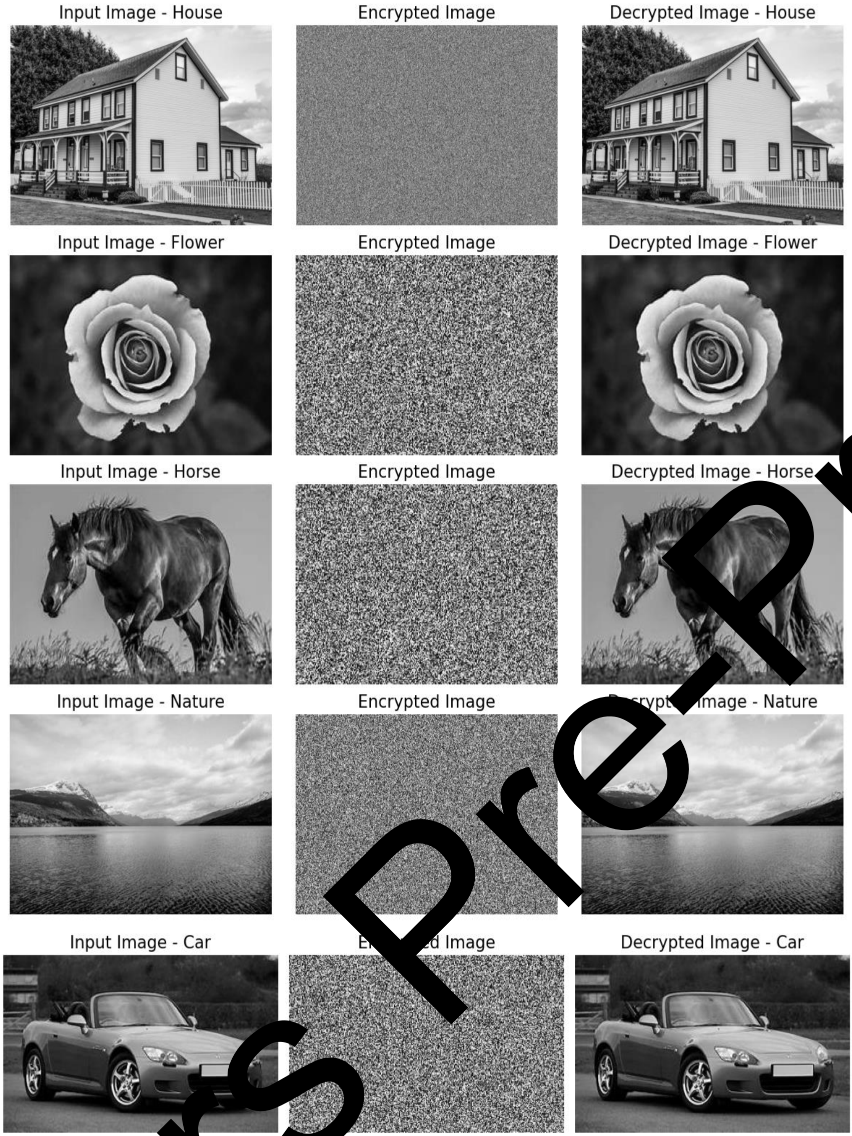


Figure 8. Standard images with Encryption and decryption

Table 4. Entropy scores of encrypted standard images

Images	Plain-image	Reference [32]	Reference [33]	Proposed
House	7.4693	7.7642	7.5326	7.9913
Flower	7.5014	7.7826	NA	7.9784
Horse	7.5163	NA	7.7924	7.9952
Nature	7.2895	NA	NA	7.9849
Car	7.1434	7.5931	7.6084	7.9794

Table 4 presents the entropy scores of encrypted standard images. The suggested model attains the maximum entropy values across all evaluated images, guaranteeing enhanced encryption security relative to prior techniques. The entropy ratings for the House and Horse images are 7.9913 and 7.9952, respectively, signifying near-perfect unpredictability. The photos of Flowers, Nature, and Cars exhibit notable enhancements compared to Reference [32] and Reference [33], with entropy values frequently approaching 8. This underscores the proposed model's efficacy in producing highly unexpected encrypted images, minimizing information loss, and enhancing resilience against statistical attacks.

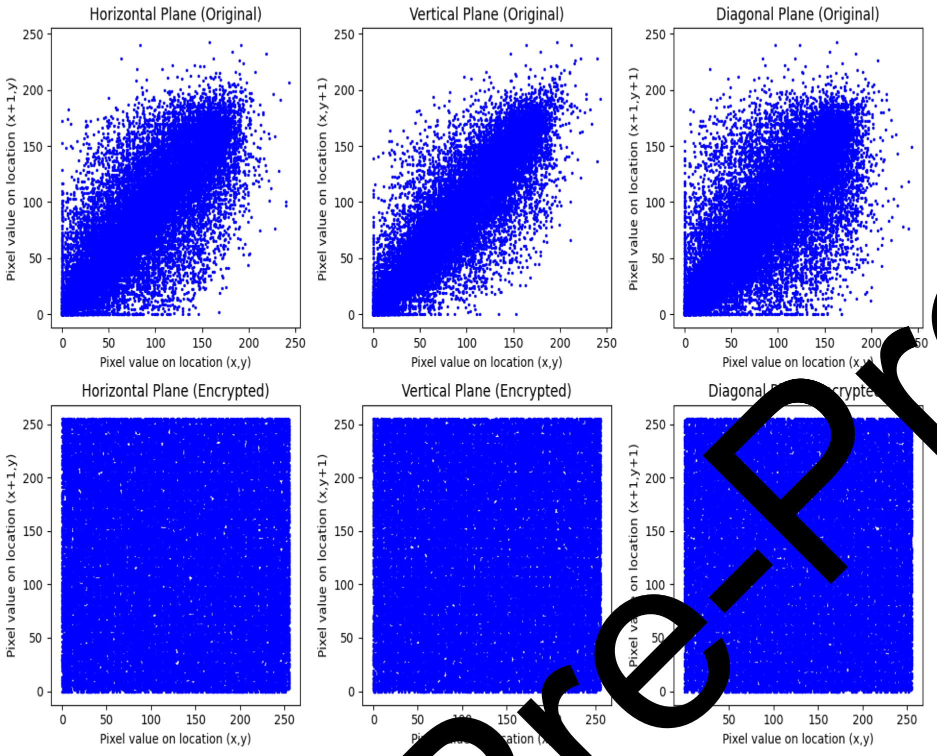


Figure 4. Correlation graph of original & encrypted image

Table 5. Standard image correlation analysis

Image	**Input images**			**Encrypted images**		
	Vertical	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**	**Horizontal**
House	0.9607	0.9216	0.9418	0.0152	0.0026	0.0033
Flower	0.8951	0.8304	0.9024	-0.0194	0.0048	-0.0221
Horse	0.8[illegible]06	0.7516	0.8427	-0.0017	0.0036	0.0162
Nature	0.[illegible]514	0.7927	0.8319	0.0078	0.0055	0.0138
Car	0.9205	0.8221	0.8623	-0.0072	0.0079	-0.0161

Table 5 and Figure 4 demonstrate that the suggested encryption approach substantially diminishes the correlation between neighboring pixels, hence assuring robust security. The input images demonstrate significant correlation values in vertical, diagonal, and horizontal orientations, with the House image displaying the greatest correlation of 0.9607 in the vertical direction. Post-encryption, these values approach zero or become negative, signifying efficient pixel dispersion. The photos of the Flower and Car have the lowest encrypted correlation scores (-0.0194 and -0.0161 in the horizontal direction), indicating significant unpredictability. The encryption procedure successfully disrupts statistical dependencies, guaranteeing reduced predictability and improved security for all evaluated photos.

Table 6. Proposed UACI and NPCR scores for standard images

Images	UACI	NPCR
House	34.135	99.92
Flower	33.472	99.69
Horse	34.128	99.73
Nature	33.327	99.87
Car	33.599	99.89

Table 6 presents the suggested UACI and NPCR ratings for standard photos. The encryption efficacy of the proposed methodology is uniform across various pictures, guaranteeing robust security and resilience. The House and Horse images attain the highest UACI values of 34.135 and 34.128, respectively, signifying a robust sensitivity to pixel alterations. The Flower image exhibits a little reduced UACI of 33.472 while preserving competitive encryption robustness. The model demonstrates exceptional resistance to differential attacks, as evidenced by the House and Car images, which have the greatest pixel change rates of 99.92% and 99.89%, respectively. The Nature image, with an NPCR of 99.87%, likewise illustrates robust encryption efficacy. The results validate the model's capacity to deliver secure encryption characterized by minimum correlation and significant unpredictability.

Table 7. Comparison with conventional algorithms

Schemes	Entropy	UACI	Correlation Coefficient			NPCR
			Vertical	Horizontal	Diagonal	
Proposed	7.9992	33.92	-0.0141	-0.00619	0.0035	99.96
Qutaiba K. Abed (2024)	[illegible]	[illegible]	0.02417	-0.006567	0.01669	99.91
Yanpeng Zhang (2024)	[illegible]	33.65	0.00048	0.002614	0.000562	99.85
Yong Deng (2025)	[illegible]	33.58	0.00042	0.00078	0.00037	99.76
Qiang Lai (2024)	7.9945	33.51	0.00217	0.00322	0.00049	99.69
Yingc[illegible] Dong (2025)	7.9936	33.42	-0.0049	-0.00043	0.00021	99.47

Table 7 demonstrates that the Proposed Model surpasses existing schemes across all critical criteria, attaining the maximum entropy (7.9992), which signifies enhanced randomness and security. It also possesses the highest NPCR (99.96%), guaranteeing substantial resistance to differential attacks. The UACI (33.92%) is the highest, indicating exceptional sensitivity to pixel alterations. The correlation coefficients in the vertical, horizontal, and diagonal orientations are nearest to zero, indicating the smallest statistical dependence and the most robust encryption performance. The proposed approach offers superior security, robustness, and attack resistance compared to prior models.

Table 8. Computational complexity comparison

Method	Computational complexity
2DLCM- CIWOA	$O(n \cdot m) + O(N \cdot T)$
OCM-ABC-IES	$O(nlogn) + O(N \cdot T) + O(N \cdot T \cdot d)$
3D-FrMHM-FrDKM-HSSAOA	$O(N^2) + O(n \cdot k \cdot t) + O(N \cdot T)$
MD5-HyperChaos-AFSA-DNA	$O(1) + O(N^2) + O(N \cdot T) + O(N^2)$
Proposed methodology	$O(N^2) + O(P \cdot T \cdot D)$

Table 8 presents a comparison of computational complexity between the proposed model and the existing approach. The Proposed Model (Memristor + SBO) is superior, presenting reduced complexity compared to high-order chaotic models such as MD5-HyperChaos-AFSA-DNA, which necessitate significant computations. It guarantees robust security while preserving efficient optimization, surpassing CIWOA and ABC in search efficacy. In contrast to 3D chaotic models that elevate computing demands, the proposed method achieves a balance among speed, resilience, and flexibility. This renders it optimal for cryptography, feature selection, and real-time optimization applications, where security and speed are paramount.

Conclusion

The suggested Memristor-Based Fractional Chaotic System utilizing the Secretary Bird Optimization Algorithm offers a secure and efficient method for image encryption. By refining chaotic parameters, the model guarantees improved randomness, heightened key sensitivity, and increased resistance to brute-force, statistical, and differential attacks. The experimental findings indicate that the encrypted images display a uniform histogram distribution, minimal correlation, and elevated entropy, rendering them exceedingly unpredictable. The model demonstrates robust resistance to differential attacks, evidenced by an NPCR value of 99.96% and a UACI of 33.92%, indicating substantial fluctuations in pixel intensity. The incorporation of the optimization technique enhances convergence velocity and diminishes computing complexity, hence increasing the efficiency of the encryption process. The suggested model provides a strong and efficient encryption framework for secure data transfer and protection in contemporary communication systems. Subsequent research may concentrate on augmenting the suggested model through the incorporation of deep learning-based key generation and adaptive chaotic maps to enhance security. Furthermore, real-time hardware implementation on FPGA or IoT devices may be investigated for actual application in secure communication systems.

Conflict of interest: The authors declare no conflicts of interest(s).

Data Availability Statement: The Datasets used and /or analysed during the current study available from the corresponding author on reasonable request.

Funding: No funding.

Consent to Publish: All authors gave permission to consent to publish.

Reference

[1] Vijayakumar, M., & Ahilan, A. (2024). An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map. Ain Shams Engineering Journal, 15(4), 102620.

[2] Kumar, B. S., & Revathi, R. (2024). An efficient image encryption algorithm using a discrete memory-based logistic map with deep neural network. Journal of Engineering and Applied Science, 71(1), 41.

[3] Sakthi kumar, B., & Revathi, R. (2024). A Comprehensive Review on Image Encryption Techniques using Memristor based Chaotic System for Multimedia Application. IETE Journal of Research, 70(11), 8160-8183.

[4] Belete, B. A., Gelmecha, D. J., & Singh, R. S. (2024). Image encryption algorithm based on a memcapacitor-based hyperchaotic system and DNA coding. Security and Privacy, 7(6), e432.

[5] Qian, K., Xiao, Y., Wei, Y., Liu, D., Wang, Q., & Feng, W. (2023). A robust memristor-enhanced polynomial hyper-chaotic map and its multi-channel image encryption application. Micromachines, 14(11), 2090.

[6] Gao, S., Iu, H. H. C., Erkan, U., Simsek, C., Toktas, A., Cao, Y., ... & Wang, C. (2025). A 3D Memristive Cubic Map with Dual Discrete Memristors: Design, Implementation, and Application in Image Encryption. IEEE Transactions on Circuits and Systems for Video Technology.

[7] Neravetla, A. R., Nomula, V. K., Mohammed, A. S., & Dhanasekaran, S. (2024, June). Implementing AI-driven Diagnostic Decision Support Systems for Smart Healthcare. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[8] Hassan, S. A. K. A., & Fyath, R. S. (2024). Multiple Color Image Encryption System Based on Hybrid Digital/Optical Techniques and Assisted by 18D Memristive Chaos. International Journal of Intelligent Engineering & Systems, 17(5).

[9] Rahman, Z. A. S., Jasim, B. H., Al-Yasir, Y. I., & Abd-Alhameed, R. A. ([illegible]). High-security image encryption based on a novel simple fractional-order memristive chaotic system with a single unstable equilibrium point. Electronics, 10(24), 3130.

[10] Abed, Q. K., & Al-Jawher, W. A. M. (2023). An image encryption method based on lorenz chaotic map and hunter-prey optimization. Journal Port Science Research, [illegible], 33[illegible]-343.

[11] Priyan, S. V., Dhanasekaran, S., Karthick, P. V., & S[illegible]mbarasa[illegible] (2024). A new deep neuro-fuzzy system for Lyme disease detection and classification using UNet, Inception, and XGBoost model from medical images. Neural Computing and Applications, 36([illegible]), 9361-9374.

[12] Belete, B. A., Gelmecha, D. J., & Singh, [illegible] S. (2025). Enhancing colour image encryption through parameters optimization of memristive hyperchaotic system with CPSO algorithm and LSAIM. The Imaging Science Journal, 1-21.

[13] Elnoamy, O., Gabr, M., Kora[illegible]m, Y., Alexan, W., & El-Aasser, M. (2023, September). Enhancing image security using legacy-based encryption with chaotic tent map and memristor. In 2023 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA) (pp. 124-129). IEEE.

[14] Yang, Y. G., Cheng, F. [illegible], Jiang, D. H., Zhou, Y. H., Shi, W. M., & Liao, X. (2023). A visually meaningful image encryption algorithm based on P-tensor product compressive sensing and newly-designed 2D memristive chaotic map. Physica Scripta, 98(10), 105211.

[15] Sonam, Sehra, [illegible] Singh, R. P., Singh, S., Wadhera, S., Kasturi, P., ... & Saxena, M. (2023). Secure digital image watermarking using memristor-based hyperchaotic circuit. The Visual Computer, 39(10), 445[illegible]-4485.

[16] [illegible]opal, [illegible]K., Mohammed, A. S., Saddi, V. R., Dhanasekaran, S., & Naruka, M. S. (2024, March). Investigate the role of machine learning in optimizing dynamic scaling strategies for cloud-based applications. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 543-548). IEEE.

[17] Abed, Q. K., & Al-Jawher, W. A. M. (2024). Optimized color image encryption using arnold transform, URUK chaotic map and GWO algorithm. Journal Port Science Research, 7(3), 219-236.

[18] Zhang, Y., Zeng, J., Yan, W., & Ding, Q. (2024). RBFNN-PSO Intelligent Synchronisation Method for Sprott B Chaotic Systems with External Noise and Its Application in an Image Encryption System. Entropy, 26(10), 855.

[19] Deng, Y., Tian, X., Chen, Z., Xiao, Y., & Xiao, Y. (2025). An image encryption algorithm based on a novel two-dimensional hyperchaotic map and difference algorithm. Nonlinear Dynamics, 113(4), 3801-3828.

[20] Lai, Q., Zhu, C. K., & Zhao, X. W. (2024). Design and hardware implementation of 4D memristive hyperchaotic map with rich initial-relied and parameter-relied dynamics. Integration, 99, 102252.

[21] Dong, Y., Zhang, S., Zhang, H., Zhou, X., & Jiang, J. (2025). Chaotic evolution optimization: A novel metaheuristic algorithm inspired by chaotic dynamics. Chaos, Solitons & Fractals, 192, 116049.

[22] Li, P. Z., Feng, X. F., Zhou, S., Yan, P. F., & Zhang, H. (2024). Compression and encryption for remote sensing image based on PSO-BP and 2D-MCCM. Physica Scripta, 99(8), 085268.

[23] Leng, X., Wang, X., Du, B., Ren, F., & Zeng, Z. (2025). Real-time dynamic medical image encryption based on extended multi-scroll memristive Hopfield neural network. Nonlinear Dynamics, 1-20.

[24] Yao, W., Liu, J., Sun, Y., Zhang, J., Yu, F., Cui, L., & Lin, H. (2024). Dynamics analysis and image encryption application of Hopfield neural network with a novel multistable and highly tunable memristor. Nonlinear Dynamics, 112(1), 693-708.

[25] Saravanan, S., & Sivabalakrishnan, M. (2021). A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption. Soft Computing, 25(7), 5299-5321.

[26] Rahman, Z. A. S., Jasim, B. H., Al-Yasir, Y. I., & Abd-Alhameed, R. A. (2021). High-security image encryption based on a novel simple fractional-order memristive chaotic system with a single unstable equilibrium point. Electronics, 10(24), 3130.

[27] Yu, F., Kong, X., Mokbel, A. A. M., Yao, W., & Cai, S. (2022). Complex dynamics, hardware implementation and image encryption application of multiscroll memeristive Hopfield neural network with a novel local active memeristor. IEEE transactions on circuits and systems II: express briefs, 70(1), 326-330.

[28] Cui, J., Cao, Y., Jahanshahi, H., Mou, J., & Sun, B. (2024). Secure transmission cryptographic approach for remote-sensing image based on discrete memristor-coupled Rulkov neuron map and TIMG. Multimedia Tools and Applications, 1-24.

[29] Guler, H. (2022). Real-time fuzzy-pid synchronization of memristor-based chaotic circuit using graphical coded algorithm in secure communication applications. Physica Scripta, 97(5), 055212.

[30] Toktas, A., Erkan, U., & Ustun, D. (2021). An image encryption scheme based on an optimal chaotic map derived by multi-objective optimization using ABC algorithm. Nonlinear Dynamics, 105(2), 1885-1909.

[31] Tahiri, M. A., Karmouni, H., Bencherqui, A., Daoui, A., Sayyouri, M., Qjidaa, H., & Hosny, K. M. (2023). New color image encryption using hybrid optimization algorithm and Krawtchouk fractional transformations. The Visual Computer, 39(12), 6395-6420.

[32] Wang, X., & Li, Y. (2021). Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. Optics and Lasers in Engineering, 137, 106393.

[33] Zeng, J., & Wang, C. (2021). A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata. Security and Communication Networks, 2021(1), 6675565.

[34] Zhu, Y., Wang, C., Sun, J., & Yu, F. (2023). A chaotic image encryption method based on the artificial fish swarms algorithm and the DNA coding. Mathematics, 11(3), 767.