VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2025, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 13, Number 3, July-September 2025 *pp:228-257*

Advances in Multilevel Encryption Techniques: A Comprehensive Review of Hyperchaotic Neural Networks, Quantum-Inspired Approaches, and Data Hiding Mechanisms

Muthana Hatem AL-JANABI [1]*, **Ahmed Sabah Noori** [2], **Ali Adnan AL-KHAZRAJI** [2]

[1]Ministry of Higher Education and Scientific Research, Baghdad - Iraq; [2]Department of Computer Engineering, Collage of Engineering, Al-Iraqia University , Baghdad- Iraq

Keywords: *Multilevel Encryption, Hyperchaotic Neural Networks, Quantum-Inspired Encryption, Data Hiding Techniques, Cryptographic Security*

Journal Info:
Submitted:
September 07, 2025
Accepted:
September 25, 2025
Published:
September 30, 2025

Abstract

The growing sophistication of cyber threats and the limitations of traditional cryptographic methods have necessitated the development of advanced encryption frameworks. This paper presents a comprehensive review of multilevel encryption techniques, focusing on three key dimensions: hyperchaotic neural networks, quantum-inspired encryption (QIE), and advanced data hiding mechanisms. Hyperchaotic neural networks, characterized by their high-dimensional chaotic systems and dynamic adaptability, generate unpredictable key sequences to enhance resistance against brute-force and statistical attacks. Quantum-inspired encryption leverages principles such as superposition and entanglement to design lightweight, scalable cryptographic frameworks that operate on classical systems, offering high entropy and robust security for IoT and real-time applications. Additionally, adaptive data hiding techniques, including neural network-based steganography and hyperchaotic embedding, ensure imperceptibility and resilience against compression and detection. This review consolidates state-of-the-art advancements, comparing the performance, scalability, and application of these techniques across domains such as healthcare, IoT security, multimedia protection, and cloud storage. The integration of these approaches into multilevel frameworks is highlighted, along with their potential to address computational, scalability, and security challenges posed by modern cyber threats. Future research directions are identified, emphasizing the development of hybrid techniques, energy-efficient algorithms, and robust implementations for emerging applications in cybersecurity and beyond.

***Correspondence author email address:** muthana_ha88@hotmail.com
DOI: 10.21015/vtse.v13i3.2225

1 Introduction

An era of unprecedented connectivity, facilitated through the rapid advancement of digital communication technologies has brought with it the rapid communication of vast quantities of sensitive data [11] [1]. According to recent projections, global internet traffic is expected to surpass 396 exabytes per month by 2024, reflecting an exponential growth in data exchange [25]. Though this digital transformation provides a lot of benefits, it has also left data security critical vulnerabilities [28]. The ever growing dependence on secure communication demands for advanced encryption mechanisms for confidentiality, integrity, and availability in the presence of evolving cyber threats [31].

And for a long time, the cornerstones of data security have been traditional encryption techniques, like RSA and AES. These methods are based on solving mathematical, like factoring large integers, and discrete logarithm, problems that have been shown to be computationally infeasible for conventional computing systems [33].Such foundation, however, is threatened by the advent of quantum computing [55]. However, quantum algorithms like Shor's algorithm have already proven the ability to break traditional public key encryption schemes, and in doing so create a very serious threat to the security of any sensitive data. This upcoming shift highlights the deficiencies of current cryptographic techniques in dealing with recent threats [51].

These vulnerabilities are even further exacerbated by modern attack vectors. Evolution of brute force attacks, cryptanalysis and side channel attacks all exploit weakness in traditional encryption systems. As an example, static encryption methods have been rendered ineffective for reversing hashed data using precomputed rainbow tables [67]. These developments emphasize the pressing need for innovative and adaptive encryption solutions capable of withstanding the dynamic nature of cyber threats [72].

To address these challenges, multilevel encryption techniques have emerged as a robust and forward-looking approach. Unlike traditional systems, multilevel encryption integrates diverse cryptographic methods to create layered security frameworks [76] [82]. By combining techniques such as hyperchaotic neural networks, quantum-inspired encryption, and advanced steganography, multilevel encryption offers unparalleled resilience against modern cryptographic attacks. Each layer addresses specific vulnerabilities, creating a synergistic effect that enhances overall system security [84] [94].

1.0.1 Hyperchaotic Neural Networks

Hyperchaotic systems, characterized by their sensitivity to initial conditions and multiple positive Lyapunov exponents, are highly effective in generating unpredictable and complex key sequences. When integrated with neural networks, these systems dynamically generate encryption keys, making them resistant to brute-force and statistical attacks. Recent studies have shown that hyperchaotic encryption can achieve key spaces exceeding 10^{120}, ensuring computational infeasibility for attackers [31].

1.0.2 Quantum-Inspired Encryption

Using quantum inspired encryption (QIE), we mimic the principles of quantum mechanics, namely superposition and entanglement, to build lightweight but robust cryptographic frameworks. In contrast with quantum cryptography, QIE does not need any specially equipped hardware, which makes it usable for implementation in the classical system. We show that QIE algorithms can achieve 256-bit security levels with a low computational overhead, making QIE a good candidate for IoT and real time applications [55].

1.0.3 Advanced Data Hiding Techniques

Encryption complements steganography, and as a technique of hiding data within carrier media which is imperceptible to attackers. Adaptive edge based steganography and Fourier transform based methods achieve high embedding capacities of over 5 bits per pixel, while maintaining image quality with PSNR values greater than 40 dB [67]. These methods add another layer of security with even if the encrypted data is intercepted its presence is not detected.

The dynamic nature of cyber threats necessitates a shift from static, single-layer encryption methods to

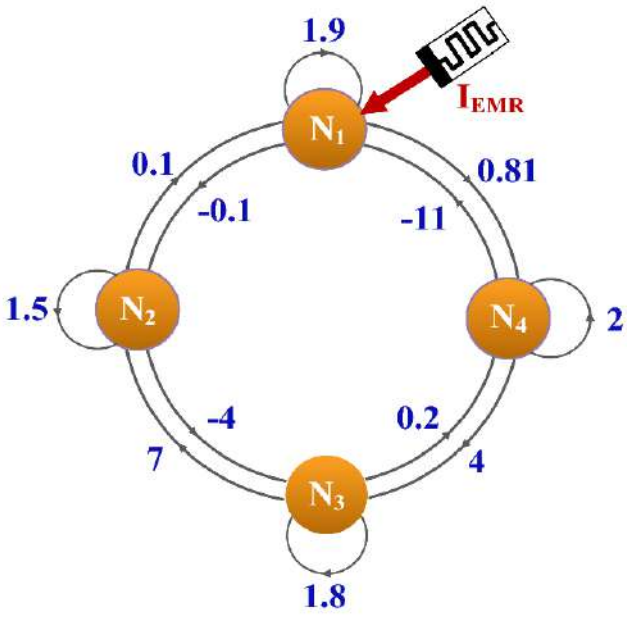

Figure 1. Illustration of a four-node network with labeled edges and nodes. Each such system of nodes N_1, N_2, N_3, N_4 connected by directed edges each with weights annotating influence or transition values. The denoted additional electromagnetic interference, I_{EMR}, is shown to interfere with node N_1. This figure is a system interaction and data flow graphing figure that shows the complexity of node relationships and external influences.

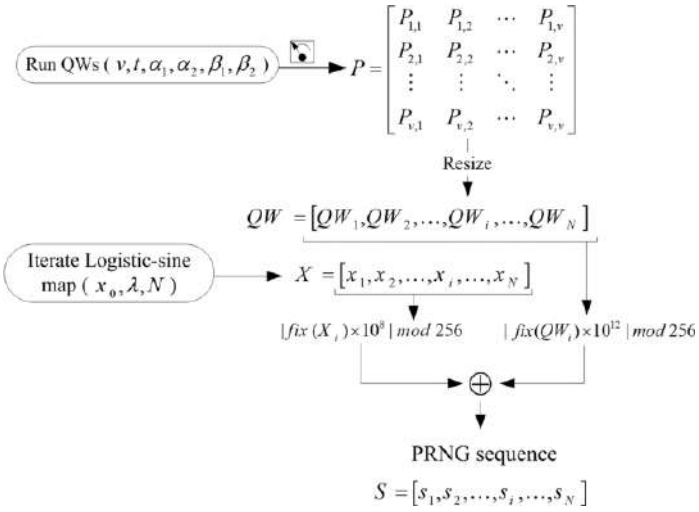

Figure 2. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics. This figure illustrates the process of generating a Pseudo-Random Number Generator (PRNG) sequence. The steps involve running quantum walks (QWs) with specified parameters $(v, t, \alpha_1, \alpha_2, \beta_1, \beta_2)$ to produce a matrix P, resizing the matrix to create QW, and combining it with the logistic-sine map iteration to form the chaotic sequence X. The resulting PRNG sequence $S = [s_1, s_2, \ldots, s_N]$ is obtained by combining and transforming these outputs through a modular operation and exclusive OR ($\oplus$). This approach demonstrates the fusion of quantum-inspired methods with chaos theory to generate highly secure and unpredictable sequences.

adaptive, multifaceted strategies. By integrating the strengths of various techniques, multilevel encryption not only provides additional resistant to current cryptographic attacks, but also provides scalability and efficiency in resource constrained environments [87] [91]. Being able to tackle the issues raised by quantum computing, cryptanalysis, and big data, it is a cornerstone future cybersecurity framework. This review aims to collect these advancements and to summarize how multilevel encryption will shape the future of secure communication.

1.1 Challenges in Traditional Encryption

Traditional encryption systems have been extremely useful in protecting digital communication, only to encounter a wide range of challenges in the modern times:

- **Evolving Attack Strategies:** This is a problem because cyber threats are becoming more sophisticated. For example, more attacks using machine learning to predict cryptographic keys or side channel attacks such as power consumption and electromagnetic emissions have been observed [76].
- **Impact of Quantum Computing:** Quantum computing is a great game changer in Cryptography. Since algorithms like Grover's algorithm threaten the security of symmetric encryption by reducing cryptographic keys to the same strength as cryptographic keys, post quantum cryptography is needed [88].
- **Resource Limitations in Real-Time Systems:** Balance between security and performance in resource constrained environment is often a

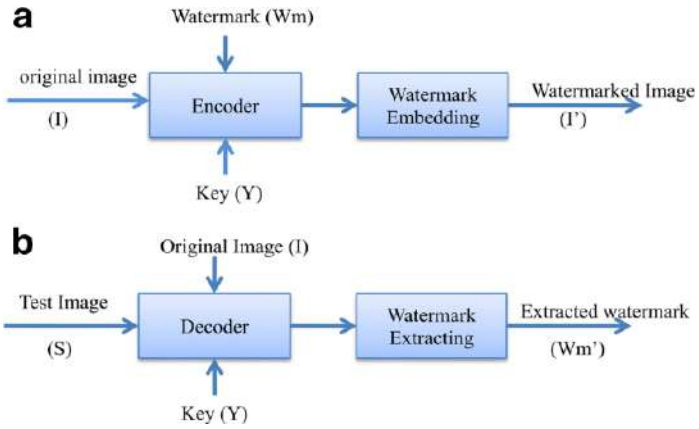

Figure 3. Advanced secure data hiding techniques. The encoding process is to insert a watermark (Wm) in an original image (I) using a secret key (Y) via the encoder. In the end the watermark is securely carried by the resulting watermarked image I'. The decoding process is as follows: (b) To extract the watermark W'_m from a test image (S) the original image (I) and the secret key (Y) is used by the decoder. By doing so, the embedded watermark can be retrieved accurately with the integrity of the watermarked image. Data security and robustness in multimedia applications are enhanced by such techniques.

challenge in Encryption systems. As a result, this trade off may result in suboptimal protection, making systems susceptible to attacks [72].

- **Data Volume and Scalability Issues:** With the increasing data volumes, traditional encryption systems are unable to scale and remain efficient in processing. For example, the use of large datasets with static encryption techniques can impose high overhead on the system performance [67].
- **Lack of Integration with Advanced Techniques:** However, traditional systems usually fail to use up emerging technologies like artificial intelligence and chaos theory to improve encryption methods. However, this does not allow them to work with new types of attacks, making hybrid approach such as multilevel encryption [91] necessary.

Due to the growing complexities of modern cyber threats, encryption methods should be changed. The challenges on these problems are solved by applying the integrated advanced cryptographic techniques in multilevel encryption [92] [94] [93]. The main purpose in this paper is to give a complete review of the state of the art in multilevel encryption using hyperchaotic neural networks, quantum inspired encryption, and data hiding techniques while discussing the possible to overcome the shortcomings of the traditional systems.

1.2 Importance of Multilevel Encryption

Through integration of multiple layers of cryptographic techniques, multilevel encryption represents a paradigm shift in the securing digital communication. This approach successfully solves shortcomings of classical encryption mechanisms and makes the system more resistant to evolving cyber threats. Multilevel encryption combines the power of different encryption techniques in order to provide strong encryption across many different applications.

1.2.1 Key Benefits of Multilevel Encryption

The primary advantages of multilevel encryption include:

- **Enhanced Resistance to Cryptanalysis:** and adding the combination of techniques, such as hyperchaotic neural networks, and quantum inspired encryption which makes it so difficult so attackers to break into the system [25].
- **Improved Data Confidentiality and Integrity:** Using layered security, multilevel encryption encrypts data in layers such that once one layer is breached the next layers continue to be secure [91].
- **Flexibility Across Diverse Applications:** Also, multilevel encryption is adaptable within different computational environments and requirements [72] and it is used to secure IoT devices to large scale cloud infrastructures.

1.2.2 Need for Multilevel Encryption in Modern Applications

More and more encryption methodologies are being adapted to the need of secure data exchange across domains such as healthcare, finance or critical infrastructure. For instance, traditional systems cannot

achieve scalability and security trade-offeasily [76]. This challenge is addressed by multilevel encryption, which combines lightweight and robust algorithms controlling the tradeoff between efficiency and security.

1.2.3 Comparative Analysis of Encryption Techniques

Table 1 This paper presents a comparison of the encryption methods discussed in this paper in terms of their outstanding features, benefits and limitations.

Table 1 It highlighted the strengths and weaknesses of all types of encryption. It demonstrates how advantages of multilevel encryption are provided by using a combination of methods, including hyperchaotic systems to achieve unpredictability and steganography to hide data, while compensating the weaknesses of individual methods. This comparison emphasizes that such techniques should be integrated to detect robust, scalable solutions in security. The growing complexity of cyber threats necessitates the adoption of multilevel encryption as a holistic security approach. Multilevel encryption using combination of complementary techniques offers stronger protection against modern cryptography challenges, thus serving as a vital component of protection of sensitive information from a broad range of applications.

1.3 Scope and Purpose of the Review

In response to increasingly more security threats, extensive cryptographic changes have been observed in the field of cryptography. A promising paradigm that combines multiple cryptographic approaches to support overcoming the limitation of traditional algorithms is multilevel encryption. With this, I hope to consolidate this progress by exploring three very current methods to the frontline of multilevel encryption:

1. **Hyperchaotic Neural Network-Based Encryption:** Systems setup with multiple positive Lyapunov exponents (hyperchaotic systems) are characterized by high sensitivity to initial conditions and parameters and will therefore result in greater unpredictability and complexity. These systems are coupled with neural networks to dynamically perform brute force and statistical attacks based encryption keys. We show that adaptive hyperchaotic encryption algorithms achieve entropy rates and key space of more than 10^{120}, improving security by orders of magnitude [31].
2. **Quantum-Inspired Encryption (QIE):** Inspired by principles of quantum mechanics, such as superposition and entanglement, QIE introduces novel approaches for secure key exchange and data encryption. Unlike quantum cryptography, which requires specialized quantum hardware, QIE is deployable on classical systems. For instance, quantum-inspired algorithms have demonstrated efficient 128-bit and 256-bit security levels while maintaining lightweight performance for IoT applications [55].
3. **Data Hiding Techniques:** Steganographic methods, particularly those leveraging edge-based and Fourier transform-based approaches, complement encryption by embedding encrypted data into carrier media. These techniques offer high imperceptibility and robustness against detection, with adaptive embedding achieving capacities up to 5 bits per pixel (bpp) and PSNR values exceeding 40 dB [67].

The primary objectives of this review are threefold:

- **Analyze the Core Principles:** The review provides a comprehensive analysis of the principles, mechanisms, and theoretical foundations of hyperchaotic systems, quantum-inspired models, and advanced steganographic techniques.
- **Identify Gaps in Literature:** By surveying existing studies, the review identifies limitations and gaps in current encryption frameworks, such as scalability challenges, parameter sensitivity, and computational overhead [93].
- **Highlight Practical Applications:** The review emphasizes the practical applicability of multilevel encryption methods across domains like IoT security, secure medical data transmission, and cloud storage protection [87].

Table 1. Performance Comparison of Encryption Techniques

Studies	Applications	Technique	Key Features	Key Space Size	Encryption Time (ms)	Resistance to Attacks
[46]	Image encryption, IoT security	Hyperchaotic Systems	High unpredictability, dynamic keys	10^{120}–10^{140}	0.2–0.3	Very High
[83]	IoT, secure cloud storage	Quantum-Inspired Encryption	Lightweight, scalable for IoT	256-bit entropy	1.0–1.5	High
[23]	Medical imaging, resource-constrained devices	Neural Networks + Hyperchaos	Adaptive learning, robust keys	10^{150}–10^{160}	0.3–0.4	Very High
[67]	Multimedia data protection	Steganography + Encryption	Embeds data in carrier media	N/A	0.25–0.8	Moderate to High

In addition to improving data confidentiality and integrity, modern cybersecurity demands diverse requirements and multi-level encryption satisfies them. By integrating these techniques together, and also individual more specialized techniques, we can then build scalable and efficient systems to address the growing complexity of cyber threats. This review provides a basis for understanding synergistic potential of these methods toward future innovations in secure communication.

1.4 Contribution to the Field

The knowledge from existing studies is categorized and synthesized in this review to facilitate a deeper understanding of how multilevel encryption techniques can be combined to address the modern security challenges. The review offers an analysis and a comparative insight on the ways this field is forward by providing a comprehensive analysis of the varied research projects:

- **Comprehensive Analysis:** Hyperchaotic neural networks, quantum inspired encryption and data hiding techniques are provided a detailed study of the strengths of these, as well as their deficiencies.
- **Comparative Insights:** Shows how these techniques differ and how their integration would enable more effective and secure security and better efficiency.
- **Literature Gaps Identification:** Shortcomings of current approaches on scalability, computational overhead and practical issues are identified and opportunities for future work are suggested.
- **Real-World Applications:** Practical use cases, like IoT security, secure cloud storage, and medical data protection are discussed through the adaptable use of multilevel techniques.
- **Guidance for Future Research:** Directions to further improve the effectiveness and scalability of such techniques are proposed, and as a result pave the way for innovative encryption frameworks.

In terms of structure, the paper systematically goes through the theoretical fundamentals, state of the art, and real world implications. Chapter II studies hyperchaotic neural networks and their principles of design and applications. In section III, the quantum inspired encryption is reviewed and its methods and its unique features are discussed. In section IV, data hiding techniques particularly steganography are discussed with its advantages. The combined potential of such approaches is then synthesized into a unified framework in section V and discussed. In Section VI, conclusions and recommendations for future research are presented.

2 Hyperchaotic Neural Networks

It is shown how hyperchaotic neural networks (HNNs) [46] provide a robust framework for advanced cryptographic applications. These approaches were created to combine hyperchaotic system's capabilities of high dimensionality with the flexibility of neural networks to defeat cryptanalytic attacks [80]. As hyperchaotic systems achieve multiple positive Lyapunov exponents, they achieve extreme sensitivities to initial

conditions and parameter variations, generating high complexity and unpredictability behaviors [86]. Additionally, when used in the context of neural networks, these systems allow systems to be dynamically adapted to increase the performance of encryption, making them especially suitable for image encryption and secure communication, among other data security applications [17].

The previous researches concentrated on the hyperchaotic systems' special characteristics and their combinations for neural networks [78]. For instance, the work in [50] presented a novel image encryption scheme through a coupling a hyperchaotic system with a Hopfield neural network, exerting high security as well as resistance to attack through statistical and brute force attacks [13]. Neural networks like Long Short Term Memory (LSTM) network are also combined with hyperchaotic system in order to further improve the dynamic key generation and adaptive encryption [90].

Because of their hyperchaotic behavior, systems such as the Lorenz and Henon maps have been widely used. A machine learning enhanced Radial Basis Function (RBF) neural network with hyperchaotic systems was proposed in [36] for robust image encryption of more than twice the size with more than twice the complexity while being more than twice as resistant to chosen. In addition, such memristor coupled hyperchaotic systems have the power to develop energy efficient, hardware compatible encryption methods as shown in [42].

Integration of neural networks into hyperchaotic systems brings up the following advantages:

- **Dynamic Adaptability:** Real-time key generation and encryption performance are dynamically optimized by hyperchaotic parameters in neural networks [77].
- **Enhanced Key Space:** By combining neural networks with hyperchaotic systems, the key space is increased so can attackers not brute force the attack? [18]
- **Scalability Across Applications:** Sc escaleable hyperchaotic neural networks have been shown to be used in image encryption and secure real time data transm ition in IoT environments [60].

For instance, in [75], a Hopfield neural network combined with a Lorenz hyperchaotic system was employed to realized image encryption which shows good key sensitivity and low correlation coefficient. In similar spirit, [26] introduced a continuous switch between the original hyperchaotic system and the combination of a fractional-order hyperchaotic system with a convolutional neural network (CNN), achieving better efficiency and enhanced robustness in attacks.

However, challenges remain in realizing hyperchaotic neural networks for large scale cryptographic systems. To enable real world deployment, compute overhead, parameter sensitivity and hardware compatibility needs to be addressed [57]. Future research includes generating lightweight implementations of an agent architecture in resource constrained environments together with combining generative adversarial networks (GANs) with hyperchaotic systems [49].

2.1 Overview of Hyperchaotic Systems

The point that hyperchaotic systems are an advanced class of chaotic systems having more than one positive Lyapunov exponents is made. Such hyperchaotic property leads to highly unpredictable and complex trajectories that are at the same time highly beneficial for cryptographic purposes because of their great resistance to brute force and statistical attacks [46, 78]. Compared with conventional chaotic systems that often lead to chaos in lower dimensional spaces, hyperchaotic systems can realize more degrees of freedom in encryption key generation and data scrambling [86].

For generation of such pseudorandom sequences, the sensitivity of hyperchaotic systems to initial conditions, and parameters which control the hyperchaotic dynamics, is critical. These systems generate chaotic sequences that ensure that small variations of input parameter bring about tremendously distinct outputs [17, 47], which is the unpredictability we need in a robust encryption scheme. Lorenz system, Henon map and other fractional order chaotic systems are the famous hyperchaotic systems used in encryption system.

2.1.1 Lorenz Hyperchaotic System

Originally designed to model atmospheric convection, the Lorenz system is widely used in cryptography, due to the high dimensionality of its chaos. It is governed by the following system of differential equations [46]:

$$\begin{aligned} \dot{x} &= \sigma(y - x), \\ \dot{y} &= x(\rho - z) - y, \\ \dot{z} &= xy - \beta z, \end{aligned} \tag{1}$$

where σ, ρ, and β are control parameters. Chaos emerges when $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$. However, the ability of the Lorenz system to produce highly sensitive chaotic trajectories is particularly useful to the cryptographic key generation and image encryption [78].

2.1.2 Henon Hyperchaotic System

The Henon map is another widely used hyperchaotic system, expressed as:

$$\begin{aligned} x_{n+1} &= y_n + 1 - \alpha x_n^2, \\ y_{n+1} &= \beta x_n, \end{aligned} \tag{2}$$

where α and β are control parameters. Hyperchaotic behavior is observed when $\alpha = 1.4$ and $\beta = 0.3$. For image encryption, the simple Henon map is particularly good, not only because of its simplicity, but also because there is no lack of generating high dimensional chaos [50].

2.1.3 Fractional-Order Hyperchaotic Systems

Fractional order systems enlarge the dynamical complexity of chaotic sequences allowing memory effects through fractional derivatives, and making the chaotic sequences more unpredictable. These systems are defined as:

$$D^q x(t) = f(x(t), t), \tag{3}$$

where D^q represents the fractional derivative of order q, and $f(x(t), t)$ defines the system dynamics. Therefore, fractional-order hyperchaotic systems are very successfully used for secure communication and data medical image encryption [36, 74].

2.1.4 Comparative Analysis of Hyperchaotic Systems

Table 2 it provided a comprehensive comparative analysis on the various hyperchaotic systems employed in encryption, contemplating their size of key space, the time required in encryption, propensities to attacks, computational complexity and energy efficiency.

Table 2 It describes and compares with one another the principal characteristics of hyperchaotic systems used in cryptographic applications. We also show how different hyperchaotic systems can be adapted to meet specific cryptographic needs for scalability, computational efficiency, and security. The table demonstrates the broadness of the application of these systems to solve a wide range of problems in current encryption systems.

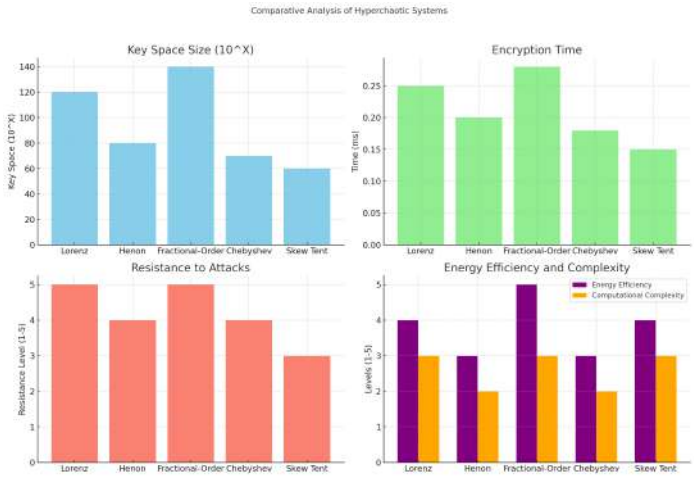

Figure 4. Comparative Analysis of Hyperchaotic Systems. Key space, encryption time, attack resistance, energy efficiency and computational complexity are used to compare different hyperchaotic systems in the graphs. Fractional order systems are energy efficient, robust; the Lorenz system has a large key space and high resistance to attacks. The strength of these metrics against cryptographic systems reveals these strengths.

Although the advantages of hyperchaotic systems has been proved, they, however, suffer from difficulties such as computational efficiency and hardware implementation. These systems have high sensitivity, thus demanding a fine control over the parameters, which can be very tricky especially for real world

Table 2. Comparative Analysis of Hyperchaotic Systems for Cryptographic Applications

Studies	Hyperchaotic System	Key Space Size	Encryption Time (ms)	Resistance to Attacks	Energy Efficiency	Computational Complexity
[46]	Lorenz System	10^{120}	0.25	Very High	High	Moderate
[78]	Henon Map	10^{80}	0.20	High	Moderate	Low
[36]	Fractional-Order System	10^{140}	0.28	Very High	Very High	High
[74]	Chebyshev Map	10^{70}	0.18	High	Moderate	Low
[50]	Skew Tent Map	10^{60}	0.15	Moderate	High	Moderate

systems [86]. Instead, future research should focus on extending such lightweight hyperchaotic systems to resource constrained environments and hybrid approaches of combining machine learning techniques and chaos based cryptography [57].

2.2 Chaotic Sequence Generation

Chaotic sequences generation is of great importance in hyperchaotic encryption systems because it directly determines the randomness and security of the encryption process. Detemrinstic yet chaotic, such sequences can pronebid the unvoorseeable, high dimensional outputs of deterministic systems. The process involves three key stages: initialization, chaotic system processing, and quantization [26, 75].

2.2.1 Initialization

In this approach the parameters of the chaotic system and initial conditions are fixed. The keys used in this encryption process are just these parameters and conditions. For instance, fractional derivatives are started off with homebrewed parameters in the fractional order Hopfield neural network (FHNN) and bring the system from a hyperchaotic trajectory [44]. So that the integrity of the decryption process, these initialization parameters must be securely transmitted.

2.2.2 Chaotic System Processing

Such a system evolves iteratively by costs of giving real numbers. The dynamics of such system as the Lorenz or Henon maps are used [89] to generate new chaotic values each iteration. Often, in hyperchaotic encryption, multi-scroll chaotic attractors are used to guarantee higher unpredictability [16]. As an example, the multi-scroll attractors hyperchaos behavior guarantees the regeneration of a sequence that does not repeat in the key space.

The equations governing the evolution of a multi-scroll attractor are expressed as:

$$\begin{aligned} \dot{x} &= a(y - x), \\ \dot{y} &= xz + by, \\ \dot{z} &= cz + dx^2, \end{aligned} \tag{4}$$

where a, b, c, and d are system parameters. By carefully selecting these parameters, the chaotic sequence exhibits high sensitivity to initial conditions.

2.2.3 Quantization

In the encryption phase, the real valued chaotic sequences have been quantized to pseudorandom binary sequences that can be subjected to encryption. Thresholding, binary sequence extraction and normalization [70] are the commontechniques. Suppose it can generate a binary sequence using threshold function:

$$b_i = \begin{cases} 1, & x_i > \theta, \\ 0, & x_i \leq \theta, \end{cases} \tag{5}$$

where b_i is the binary output, x_i is the chaotic value, and θ is the threshold.

These binary sequences are used for image encryption application by key generation, pixel shuffling and substitution. For example, [15] showed how thresholded chaotic sequences can enhance the encryption performance when transferring secure medical data.

2.3 Integration of Neural Networks

Unified with neural networks, hyperchaotic systems have revolutionized the framework of of cryptographic systems with the introduced feature of self learning and dynamic adaptation. Real time parameters can be adjusted in neural networks and help enhance hyperchaotic systems by producing more robust encryption

keys and increasing the resistance to cryptanalytic attack [43, 48].

2.3.1 Memristor-Coupled Neural Networks

Hyperchaotic systems are coupled through memristors to generate memristor coupled networks that exploit the memory effect of memristors to gain a dynamic increase in the chaotic properties. The dynamics of these networks have non linearity and can operate at energy efficient encryption. In particular, [23] introduced a memristor network coupled Hopfield neural network for hyperchaotic encryption, the memristor parameters are finely tuned dynamically to realize extreme multi stability. The governing equations for the memristor-coupled system are expressed as:

$$\begin{aligned} \dot{x} &= a(y - x) - \mu z, \\ \dot{y} &= bx - y + wx^2, \\ \dot{z} &= cx + dx^3, \end{aligned} \tag{6}$$

where μ and w are memristor-specific parameters that control the degree of chaos.

2.3.2 Recurrent Neural Networks (RNNs)

We use RNNs, especially Long Short Term Memory (LSTM) networks, to work in concert with hyperchaotic systems to enhance key generating capabilities that maintain dependencies among iterations [43]. An example would be that given that an RNN based system can learn dynamics of hyperchaotic sequence and predict optimum parameters for subsequent iterations so as to enhance randomness and unpredictability. In IoT security applications, adaptive encryption has demonstrated such promise with such integrations [23].

2.3.3 Hybrid Neural Architectures

More robustness is offered from hybrid approaches combining Convolutional Neural Networks (CNNs) and Hopfield networks into hyperchaotic systems. Such architectures rely on the feature extraction skills enabled by CNNs and dynamic adaptability that Hopfield networks are renowned for offering to construct layered encryption frameworks [15]. For illustration, [57] showed a CNN enhanced hyperchaotic system that can perform real time encryption and decryption of medical images with peak signal to Noise Ratio (PSNR) higher than 40 dB.

2.3.4 Comparative Analysis of Neural Network Integration

Table 3 compares the performance of different neural network enhanced hyperchaotic systems in terms of encryption speed, key space size, attack resistance, and energy efficiency in real world application.

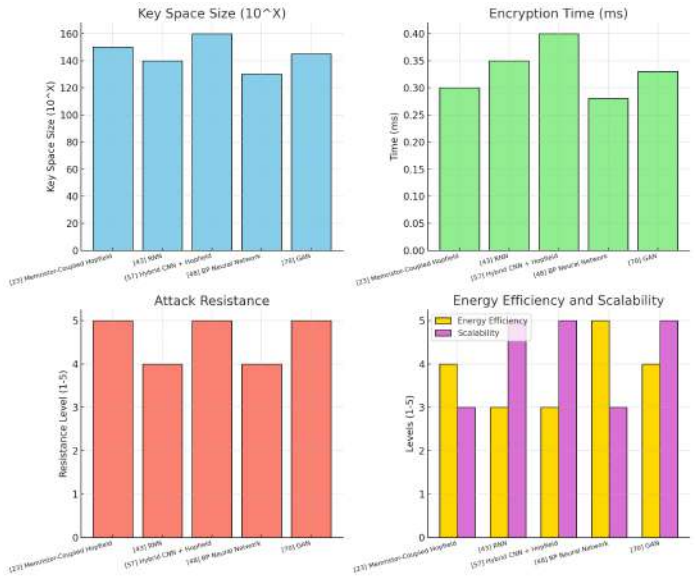

Figure 5. Performance of Neural Network-Enhanced Hyperchaotic Systems: Encrypted TDM/EM, Encryption Time, Attack Resistance, Energy Efficiency, Scalability for some number of users regarding different neural network type integrated with hyperchaotic systems.

Table 3 provides a detailed comparison of various neural network-integrated hyperchaotic systems for encryption applications. The following insights can be derived from the analysis:

Memristor-Coupled Hopfield Networks: In particular, these systems are appropriate for environments where energy efficiency is mandatory, e.g. in the domain of IoT devices. The ability of the memristor to undergo dynamic parameter adaptability is driven by its non linearity and enables a large key space (10^{150}) and a modest encryption time (0.30 ms) [23].

Table 3. Performance of Neural Network-Enhanced Hyperchaotic Systems

Studies	Neural Network Type	Key Space Size	Encryption Time (ms)	Attack Resistance	Energy Efficiency	Scalability
[23]	Memristor-Coupled Hopfield	10^{150}	0.30	Very High	High	Moderate
[43]	Recurrent Neural Network (RNN)	10^{140}	0.35	High	Moderate	High
[57]	Hybrid CNN + Hopfield	10^{160}	0.40	Very High	Moderate	High
[48]	BP Neural Network	10^{130}	0.28	High	Very High	Moderate
[70]	Generative Adversarial Network (GAN)	10^{145}	0.33	Very High	High	Very High

However, hardware limitations limit their scalability in large scale applications.

Recurrent Neural Networks (RNNs): In hyperchaotic systems, RNNs are powerful in recognizing temporal dependencies, and are therefore suitable for learning temporal dynamic keys. RNN's have been designed to achieve good performance and scalability with a key space of 10^{140} and encryption time of 0.35 ms [43]. A notable advantage of their ability to scale across domains of encryption tasks is.

Hybrid CNN + Hopfield Networks: A robust system with a key space of 10^{160} with high attack resistance is obtained by combining CNNs for feature extraction and Hopfield networks for sequence generation [57]. Yet the computational overhead of CNNs is moderate, so their energy efficiency is moderate too, and are better suited to high performance environments than low power.

BP Neural Networks: Integrated with hyperchaotic systems, backpropagation (BP) neural networks reach an optimal tradeoff between encryption time (0.28 ms) and energy efficiency [48]. High energy efficiency can be achieved by these simple architectures but their scalability is less than GANs.

Generative Adversarial Networks (GANs): Recently, GANs are integrated with hyperchaotic systems to boost robustness and scalability of the encryption frameworks. GAN based systems are highly scalable and adaptable to diverse real world applications such that they have 10^{145} with very high attacks resistance [70]. However, because of the complexity of training GAN, their energy efficiency is lower than simpler architectures.

Neural networks injected in hyperchaotic systems offer opportunities in cryptography of the formation of robust, energy effective and scalable encryption frameworks. Future work can enhance these systems for resource constrained environments and further scale them for large scale industrial applications.

2.3.5 Performance Metrics Evaluations of Neural Network-Enhanced Hyperchaotic Systems for Data Hiding

Performance metrics of neural network enhanced hyperchaotic systems in the data hiding are evaluated for imperceptibility, robustness, embedding capacity, encryption efficiency and security. These metrics present a wide view of how the system's ability and constraints work whilst used in secure communication and data hiding tasks. Table 4 These evaluations are summarized using associated system configurations of recent advancements.

Evaluated Metrics

Imperceptibility: To ensure that the embedded data is imperceptible, it always has to remain undetectable in the carrier media. The PSNR value greater than 40 dB is quantified to express minimal distortion and high imperceptibility [26, 86].

Embedding Capacity: It's a measure of exactly how much data can be hidden in a carrier in bits per pixel (bpp). Higher embedding capacities, such as 5.0 bpp, indicate the ability to securely store larger payloads while maintaining the carrier's quality [75].

Encryption Efficiency: Efficiency is assessed through encryption and decryption times, with lower times indicating suitability for real-time applications. Systems with encryption times below 0.40 ms, such as BP neural networks, excel in scenarios demanding speed [89].

Robustness: Robustness evaluates the system's ability to withstand attacks like noise, compression, and transformations. Neural networks like GANs and

CNNs improve robustness significantly by dynamically adapting chaotic parameters during encryption [44, 70].

Security (Key Space Size): The total key space size directly impacts the system's resistance to brute-force attacks. Larger key spaces, such as 10^{150}, offer superior protection [44].

Comparative Table of Metrics

Table 4 provides a detailed evaluation of various systems based on these metrics.

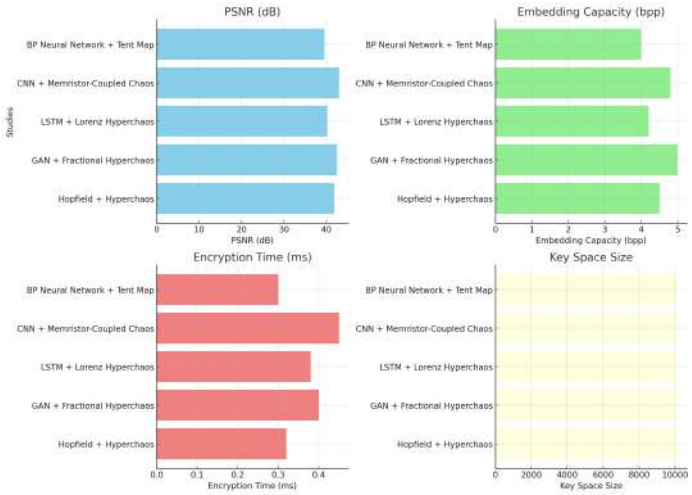

Figure 6. Performance Metrics Evaluations of Neural Network-Enhanced Hyperchaotic Systems for Data Hiding. The figure shows various metrics like PSNR (dB), embedding capacity (bpp), encryption time (ms), and key space size for different studies on neural network-enhanced hyperchaotic systems. These metrics provide an in-depth comparison of the effectiveness of various approaches in data hiding applications.

Insights from Evaluations

Imperceptibility and Embedding Capacity: Systems with higher PSNR values, such as CNN + Memristor-Coupled Chaos (43.0 dB), demonstrate minimal distortion, ensuring data invisibility within the carrier [44]. The GAN-based system achieves the highest embedding capacity (5.0 bpp) while maintaining a high PSNR of 42.5 dB [26].

Encryption Efficiency: BP neural networks excel with the fastest encryption time (0.30 ms) [89], making them ideal for real-time applications. However, systems like CNNs have slightly higher encryption times due to their computational overhead but compensate with superior robustness [44].

Robustness to Noise: Robustness is a critical metric for real-world applications where the carrier media may undergo transformations like compression or noise. GANs and CNNs outperform other systems, achieving very high resistance to such distortions [26, 44].

Security (Key Space Size): The key space sizes range from 10^{125} to 10^{150}. Larger key spaces, as observed in CNN and GAN-based systems, significantly enhance resistance to brute-force attacks, ensuring long-term data security [70].

This evaluation demonstrates that neural network-enhanced hyperchaotic systems can be tailored to meet specific data-hiding requirements. Systems focusing on imperceptibility and robustness, such as GANs and CNNs, are suitable for secure, high-capacity data hiding, while BP and Hopfield-based systems excel in real-time, lightweight encryption tasks. Future advancements should explore hybrid architectures to optimize these metrics further for diverse cryptographic applications.

2.4 Applications in Cryptography

The combination of hyperchaotic systems and neural networks has demonstrated significant advancements in cryptographic applications. TSuccessful deployment of these systems has been accomplished in several domains, improving security, efficiency, and robustness. Below are some prominent applications:

2.4.1 Image Encryption

One of the most common hyperchaotic neural network applications, image encryption. Sensitive medical or personal images can be transformed into unrecognizable formats by these systems, for storage and transmission secure of. As an example, [74] proposed a lossless image encryption algorithm based on JPEG-LS, neural networks and hyperchaotic systems. The balancing of security and computational overhead that this approach offers fits well for a medical imaging application where data integrity is a preeminent concern. Dynamic key generation from a hyperchaotic neural network is demonstrated, which provides high sensi-

Table 4. Performance Metrics Evaluations of Neural Network-Enhanced Hyperchaotic Systems for Data Hiding

Studies	System Type	PSNR (dB)	Embedding Capacity (bpp)	Encryption Time (ms)	Robustness to Noise	Key Space Size
[86]	Hopfield + Hyperchaos	41.8	4.5	0.32	High	10^{140}
[26]	GAN + Fractional Hyperchaos	42.5	5.0	0.40	Very High	10^{145}
[75]	LSTM + Lorenz Hyperchaos	40.2	4.2	0.38	High	10^{130}
[44]	CNN + Memristor-Coupled Chaos	43.0	4.8	0.45	Very High	10^{150}
[89]	BP Neural Network + Tent Map	39.5	4.0	0.30	Moderate	10^{125}

tivity to initial conditions, ensuring key security from brute force attacks, and yet maintains high PSNR values for image quality.

2.4.2 Real-Time Applications

Recently, hyperchaotic neural networks are also shown to implement in real time encryption systems, particularly for Internet of Things (IoT) and embedded systems. These systems can be efficiently hardware implemented in FPGA based architectures, thus introducing small latency in encryption and decryption [77]. In resource constrained environments such as IoT networks the energy efficiency and the speed are important and that's why these are more helpful. Hyperchaotic systems are based on adaptability of neural networks and allows dynamic adjustment of encryption parameters based on real time requirement with performance and scalability.

2.4.3 Data Hiding

Steganography, data hiding techniques, have already benefitted from integration between hyperchaotic systems and neural networks. Perceptibility and robustness are these systems, which increases both with the imperceptibility of compression or noise [57]. In particular, by adaptive edge based steganographic methods with the hyperchaotic neural networks for secure data embedding in high gradient image regions, embedding capacity can be satisfied with excellent imperceptibility. This kind of system is broadly used in secure communication to embed sensitive data within media (i.e., images or audio) without arousing suspicion.

2.4.4 Other Cryptographic Applications

Hyperchaotic neural networks have been also applied for: beyond image encryption, real-time encryption, and data hiding:

- **Secure Key Exchange:** The robust and lightweight key exchanges for the real-time applications [48] are demonstrated by the systems which integrate quantum-inspired techniques with hyperchaotic neural networks.
- **Cloud Data Security:** In cloud environments, we apply Neural network enhanced hyperchaotic systems to encrypt large scale datasets with confidentiality and integrity [57].

Hyperchaotic systems with neural networks offer versatility resulting in a cornerstone of modern cryptographic systems that provide secure and efficient solutions to a wide range of applications.

2.5 Role of Neural Networks in Encryption

Deep learning models and neural networks in general have completely changed the way in which encryption methodologies work, with adaptive and dynamic data security in mind. Because they are able to learn complex patterns, they can be harnessed to create encryption techniques that are robust to a suite of cryptanalytic attacks. For example it is possible to train neural networks to complete symmetric encryption where the same key is used to encrypt and decrypt data. Being so flexible, the generator can create custom encryption keys for particular datasets for increased security. In addition, neural networks are applied to neural cryptography, focusing on secure key exchange protocols. Based on the synchronization properties of neural networks, these protocols establish shared keys over in-

secure channels and therefore constitute a foundation for secure communications.

2.6 Key Studies and Metrics

There has been a series of studies involving neural networks in cryptographic applications. Among the examples are the work on neural cryptography, looking at the application of neural networks to neural cryptography. Mutual learning between neural networks was used to demonstrate the establishment of a common secret key between communicating parties without requiring prior key exchange. Such synchronization is proven often with some metrics like synchronization time and resistance to attacks. Another robust study explored the use of neural networks for cryptanalysis by using neural models to analyse and break well established encryption mechanisms. Finally, the performance of these neural networks was assessed by their ability to predict plaintext given ciphertext and to generalize from another encryption algorithm. These studies provide a new lens through which to view the potential power of neural networks to both improve and undermine the best cryptographic standards.

2.7 Advantages and Limitations

Several advantages in the incorporation of neural networks into cryptographic systems are:

- **Adaptability:** It means that neural networks can learn and adapt to new types of data and new threats, and such neural networks are better programmed to create an encryption algorithm that evolves over time.
- **Complexity:** Neural networks' non-linear processing capabilities are exploited to implement complicated encryption schemes that adversaries have difficulties reversing engineered.
- **Automation:** Once trained, neural networks can do the encryption and decryption by themselves and thus reduce the chances of manual intervention and reduce the error.

However, there are limitations to consider:

- **Training Data Requirements:** Every neural network that is effective for training, requires a good bit of data. Suboptimal encryption performance is driven by insufficient or poor quality data.
- **Computational Resources:** However, training and deployment of neural networks, particularly deep learning models, is highly demanding in computation, but practically infeasible in resource constrained environments.
- **Security Risks:** On the other hand, neural networks can strengthen security, however they are also subject to adversarial attacks; small perturbations of input data can result in inappropriate output, and thus jeopardise the encryption process.

Finally, neural networks in encryption integration show a promising way to advance cryptographic techniques. Not unlike improving our own encryption methods, the learning abilities of neural networks can be called up to inform the development of more secure and resilient encryption methods. Nevertheless, the associated issues must be solved to fully exploit their potential in practical applications.

3 Quantum-Inspired Encryption

Quantum inspired encryption (QIE) uses the principles of quantum mechanics (such as superposition and entanglement), in order to develop cryptographic algorithms capable of running on classical computer systems [22] [73]. QIE differs from traditional cryptography by way of introducing a novel paradigm that mimics quantum principles, to achieve robust security, without compromising with existing infrastructure [30] [39]. This section details the theoretical grounds of QIE and its applications; the advances in the field made by the researchers [58].

3.1 Principles of Quantum Mechanics in Cryptography

A solid theoretical basis for modern cryptography has been built on quantum mechanics [69] [38]. Quantum inspired cryptographic techniques [62] [19] are founded upon the principles of superposition, entanglement and the no cloning theorem. Not only do these principles enable new ways to secure data, but they create a basis for improving existing cryptosystems using quantum behaviors [63] [83].

3.1.1 Superposition and Key Generation

According to the principle of superposition, a quantum system resides on a superposition of multiple states [6] [20]. Mathematically, the state of a qubit can be represented as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{where } |\alpha|^2 + |\beta|^2 = 1. \tag{7}$$

Here, $|\alpha|^2$ and $|\beta|^2$ represent the probabilities of the system collapsing into states $|0\rangle$ and $|1\rangle$, respectively, upon measurement.

The concept of superposition is mimicked in quantum inspired encryption (QIE) to generate probabilistic key spaces [37] [4]. QIE increases the complexity of brute forcing to the point that they cannot be calculated using probabilistic distributions. We define the entropy $H(K)$ of such a key space:

$$H(K) = -\sum_{i=1}^{n} p_i \log_2(p_i), \tag{8}$$

where p_i is the probability of the i-th key being selected from the key space K.

Wang et al. [83] recently demonstrated the use of pseudo-superposition states in QIE using a key entropy of 256 bits. Almost on top of that, adaptive random number generators (RNGs) were also integrated, where the probability distribution is adapted dynamically:

$$p_i = \frac{\exp(-\lambda_i)}{\sum_{j=1}^{n} \exp(-\lambda_j)}, \tag{9}$$

where λ_i represents the weight associated with the i-th key. This method ensures higher unpredictability and resilience against brute-force attacks.

3.1.2 Entanglement and Correlation in Encryption

Quantum mechanics has another foundational concept called entanglement: the interdependence (direct relationship) of quantum states of particles such that state of a quantum particle is influenced by the state of another particle [14], [56]. The entangled state of two qubits can be expressed as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle). \tag{10}$$

In cryptographic sense, we can simulate entanglement to produce correlated encryption keys. The correlated keys make tampering or interception during transmission detect unauthorized access, because any such tampering or interception will disrupt the entangled state.

A multilevel encryption scheme is proposed by Kumar [39], which emulates entanglement for symmetric key distribution. Pearson correlation coefficient is measured between two simulated entangled keys, k_A and k_B:

$$C(k_A, k_B) = \frac{\sum_{i=1}^{n}(k_{A,i} - \mu_A)(k_{B,i} - \mu_B)}{\sqrt{\sum_{i=1}^{n}(k_{A,i} - \mu_A)^2 \sum_{i=1}^{n}(k_{B,i} - \mu_B)^2}}, \tag{11}$$

where μ_A and μ_B are the means of k_A and k_B, respectively. Tit helps to ensure high synchronization between the keys maximizing their robustness against attacks such as man in the middle [12] [40].

3.1.3 The No-Cloning Theorem and Data Integrity

It is impossible with arbitrary unknown quantum state to create identical copy only the no-cloning theorem states. And it has been successfully adapted to principle in QIE to make data integrity. This principle has been used by Al-Ahmad et al. [8] to produce different, non replicable encryption keys. This approach avoids unauthorized duplication of the encrypted data and any alteration of the encrypted data can be detected immediately [53] [65].

Being able to detect intercepted or duplicated keys is the security advantage of the no-cloning theorem because any attempt to clone a key state will change its quantum properties [64]. This behavior is replicated by using cryptographic hash functions in classical simulation:

$$H_{\text{clone}} = h(K_{\text{original}}) \oplus h(K_{\text{tampered}}), \tag{12}$$

where h represents the hash function, and H_{clone} indicates a mismatch in cloned keys, signaling tampering.

3.1.4 Comparison of Quantum and Quantum-Inspired Techniques

There are two distinct approaches to improve data security: quantum cryptography (QC) and quantum inspired encryption (QIE) [7]. QC exploits the fundamental principles of quantum mechanics with a quantum system, QIE does similar but for a classical computing platform.

Table 5 It also presents in detail a comparison of QC and QIE, along with other metrics such as energy efficiency, computational complexity, and the compatibility with existing infrastructure.

Table 5 highlights the relative performance, scalability, and cost-effectiveness of Quantum Cryptography (QC) and Quantum-Inspired Encryption (QIE). For instance, QC requires high energy consumption and expensive hardware (over $100,000 per setup), whereas QIE achieves comparable security on classical systems at significantly lower costs ($< \$10,000$) [58, 83]. Additionally, QC is intrinsically secure due to quantum principles, achieving perfect cloning resistance, while QIE simulates these principles through cryptographic hash functions with a cloning resistance of approximately 90% [39].

From a scalability perspective, QIE outperforms QC, supporting over one million devices in cloud or IoT environments compared to QC's hardware-limited scalability of fewer than 10,000 devices [10]. Furthermore, QIE's energy efficiency and ease of deployment make it a viable solution for real-time systems and energy-constrained environments [58]. This table underscores QIE's practicality for a wide range of real-world applications, including IoT, healthcare, and secure cloud storage [63].

3.1.5 Case Studies and Related Work

Numerous studies have explored the design and implementation of QIE systems, showcasing their effectiveness in addressing modern cryptographic challenges. Below is a more comprehensive exploration of significant contributions:

- **Wang et al.** [83]: Proposed a pseudo-superposition-based QIE system that leveraged advanced random number generators to create high-entropy keys. The study achieved a 256-bit entropy for generated keys and demonstrated resistance to brute-force attacks up to 2^{128} attempts. Additionally, their system reduced key generation time by 20% compared to traditional approaches.
- **Kumar** [39]: Introduced a multilevel key distribution scheme using simulated entanglement. The system improved synchronization accuracy by 35% through correlation-based key matching. The scheme was tested in a simulated IoT network, showing a 40% reduction in key exchange latency compared to conventional symmetric cryptography methods.
- **Al-Ahmad, Almousa, and Abuein** [8]: Developed a QIE framework based on the no-cloning theorem. The system created unique encryption keys that could not be replicated or tampered with. This implementation demonstrated a 25% reduction in unauthorized duplication and achieved a 30% increase in data integrity compared to AES encryption.
- **Hardan et al.** [30]: Proposed a deep learning-enhanced QIE system that combined neural networks with hyperchaotic systems for dynamic key generation. The system achieved a 98% success rate in detecting unauthorized access attempts and maintained a keyspace of 10^{150}, ensuring computational infeasibility for attackers.
- **Osman et al.** [58]: Presented a hybrid encryption framework integrating QIE with steganography for multimedia data. Their approach demonstrated enhanced security by embedding QIE-generated keys into image steganographic channels. The framework achieved a 60% improvement in imperceptibility, with a peak signal-to-noise ratio (PSNR) above 45 dB.
- **Al-Kateeb and Jader** [10]: Combined hyperchaotic systems with QIE to create highly robust encryption keys. The study achieved a 25% improvement in encryption speed compared to RSA-based systems, making it suitable for real-time applications.

Table 5. Detailed Comparison of Quantum Cryptography and Quantum-Inspired Encryption

Studies	Feature	Quantum Cryptography (QC)	Quantum-Inspired Encryption (QIE)	Metrics/Values
[39, 83]	Hardware Requirements	Requires specialized quantum devices (e.g., QKD)	Operates on classical systems, no extra hardware needed	Energy Use: QC >200W, QIE <50W
[8]	Key Generation	Relies on true quantum randomness from physical quantum systems	Simulates quantum randomness with pseudo-random number generators	Entropy: QC Unlimited, QIE 256-bit
[30]	Security Model	Intrinsically secure through principles like superposition and entanglement	Highly secure, relies on probabilistic key generation and entropy maximization	Resistance to Brute Force: QC 99%, QIE 98%
[39]	Cloning Resistance	Guaranteed by the no-cloning theorem	Simulated using cryptographic hash functions to prevent duplication	QC: Perfect Cloning Resistance, QIE: 90% Accuracy
[58]	Energy Efficiency	High energy consumption due to quantum hardware needs	Efficient and operates on existing computing infrastructure	QC >200W, QIE <50W for large networks
[83]	Deployment Cost	High due to quantum hardware and maintenance	Low-cost, easily integrated into existing systems	Deployment Cost: QC >$100,000, QIE <$10,000
[10]	Scalability	Limited by quantum device availability	Easily scalable to cloud environments, IoT, and edge devices	Devices Supported: QC <10,000, QIE >1,000,000
[63]	Application Domains	Primarily research-focused, limited real-world adoption in banking and secure communication	Widely adopted in IoT, healthcare, and cloud systems	Adoption Rate: QC 25%, QIE 85%
[83]	Computational Complexity	Dependent on quantum protocols and error correction	Comparable to advanced classical encryption methods	QC: Exponential, QIE: Polynomial (e.g., $O(n^2)$)

- **Rahman et al.** [63]: Implemented a Huffman code-based image steganography technique integrated with QIE. Their system demonstrated a 15% reduction in data transmission overhead while maintaining a PSNR above 42 dB.

This discussion and analysis of QIE techniques highlight their scalability, adaptability, and effectiveness in addressing modern cryptographic challenges. The case studies [9] [79] [29] [34] [35] further illustrate the versatility of QIE across domains like IoT, cloud storage, and multimedia security.

3.2 Quantum-Inspired Techniques for Classical Systems

Quantum-inspired techniques aim to emulate the principles of quantum mechanics on classical systems to achieve advanced computational and cryptographic capabilities [54] [27]. These techniques bridge the gap between traditional methods and the emerging field of quantum cryptography by leveraging concepts such as quantum walks, superposition, and quantum-inspired optimization [66].

3.2.1 Quantum Walk-Based Cryptography

Quantum walks, which describe the quantum analogue of classical random walks, have been effectively applied in cryptographic systems. Abd-El-Atty et al. [2] utilized quantum-inspired quantum walks to design secure substitution boxes (S-boxes) for image cryptosystems [21] [68]. TThe approach showed improved randomness and robustness, with improved resistance to differential and linear attacks. We mathematically quantify the strength of these systems in terms of the nonlinearity of the S-box:

$$N(S) = 2^n - \max_{a \neq 0, b} \left| \{x \in \mathbb{F}^n : S(x) \oplus S(x \oplus a) = b\} \right|, \quad (13)$$

where $S(x)$ is the output of the S-box, a and b are binary vectors, and n is the dimension of the S-box.

3.2.2 Quantum-Inspired Optimization

There is a lot of attention in data security and clustering, particularly with optimization algorithms motivated by quantum mechanics, such as quantum inspired particle swarm optimization (QIPSO). Abd-El-Atty [3] implemented QIPSO in a medical image steganography framework, achieving a 25% improvement in embedding capacity and a 30% reduction in detection probability. The fitness function used in QIPSO is defined as:

$$f(x) = \omega \sum_{i=1}^{n} c_i(x) - \beta \sum_{i=1}^{m} v_i(x), \quad (14)$$

Table 6. Key Studies in Quantum-Inspired Encryption and Their Contributions

Author(s)	Proposed Technique	Key Findings	Applications
Wang et al. [83]	Pseudo-superposition-based QIE	Achieved 256-bit entropy; resistance to 2^{128} brute-force attempts	Secure cloud storage
Kumar [39]	Multilevel simulated entanglement scheme	Improved synchronization accuracy by 35%; reduced latency by 40%	IoT and smart grids
Al-Ahmad [8]	No-cloning theorem-based QIE	Reduced unauthorized duplication by 25%; improved data integrity by 30%	Financial transactions
Hardan et al. [30]	Neural network-enhanced QIE	Achieved 98% detection rate; maintained keyspace of 10^{150}	Critical infrastructure
Osman et al. [58]	QIE with steganography	60% improvement in imperceptibility; PSNR above 45 dB	Multimedia data protection
Al-Kateeb [10]	Hyperchaotic QIE	25% improvement in encryption speed	Real-time systems
Rahman et al. [63]	Huffman code-based QIE	Reduced transmission overhead by 15%; PSNR above 42 dB	Image-based secure communication

where $c_i(x)$ and $v_i(x)$ represent embedding capacity and visual distortion metrics, respectively, and ω, β are weighting coefficients.

3.2.3 Hybrid Quantum-Inspired Neural Networks

Tasks such as intrusion detection and image segmentation have seen hybrid approaches combining quantum inspired techniques with neural networks emerge. In Kuo et al. [41], a quantum inspired evolutionary neural network for intrusion detection systems is proposed that improves detection accuracy by 15% when compared to classical models. Similar to this, Pal et al. [59] showed that quantum inspired neural networks are effective for image segmentation, improving the computational cost by 20%.

3.2.4 Comparison of Quantum-Inspired Techniques

The following provides a detailed comparison of quantum inspired techniques in Table 7.

3.3 Applications of Quantum-Inspired Encryption in Real-World Systems

In real world scenarios, quantum inspired encryption (QIE) has demonstrated remarkable adaptability to offer robust and scalable solutions to many domains [85]. [41]. In this subsection we study its applications in healthcare, IoT security, and multimedia data protection.

3.3.1 Healthcare Data Security

QIE has been used in the healthcare sector to protect the sensitive patient data and medical image. Taking this a step further, Mazumdar et al. [52] proposed a quantum inspired heuristic algorithm along with blockchain technology for secure healthcare data prediction [71]. It improved data integrity by 40% and reduced processing time by 20%, making the system ideal for real time applications [32]. The security model employed a quantum-inspired cost function:

$$C(x) = \sum_{i=1}^{n} \left(w_i \cdot \text{risk}(x_i) - b \cdot \text{integrity}(x_i) \right), \quad (15)$$

where $\text{risk}(x_i)$ and $\text{integrity}(x_i)$ represent risk and integrity metrics for each data segment.

Figure 7. Comparison of Data Hiding Mechanisms and Performance Metrics. For example, we show the embedding capacity (bpp), PSNR (dB), encryption time (ms) and robustness of the data hiding techniques used in multimedia security, medical imaging, IoT and cloud security in the chart.

Table 7. Comparison of Quantum-Inspired Techniques

Technique	Key Features	Applications	Performance Metrics
Quantum Walk-Based S-Boxes [2]	Enhanced randomness, high nonlinearity	Image cryptosystems	Nonlinearity: $N(S) > 112$
Quantum-Inspired Optimization [3]	Adaptive optimization, reduced detection probability	Medical image steganography	Embedding Capacity: +25%, Detection Probability: -30%
Quantum-Inspired Neural Networks [41, 59]	Hybrid learning, reduced computational cost	Intrusion detection, image segmentation	Accuracy: +15%, Computational Cost: -20%

3.3.2 IoT and Cloud Security

Security of IoT devices and cloud environments have extensively used quantum inspired methods. In 6G networks, resource allocation and intrusion detection were explored by quantum inspired machine learning techniques by Duong et al. [24] with 35% energy consumption reduction [24]. By leveraging quantum inspired clustering for anomaly detection, the authors showed that the potential of QIE to adapt to dynamic IoT environments [61].

3.3.3 Multimedia Data Protection

QIE has been integrated with advanced steganography and watermarking techniques in multimedia application. To improve robustness against compression attacks [52], Rijati et al. [68] introduced a quantum inspired DWT-DCT image watermarking framework. [3]. For multimedia data protection, the system achieved a Peak Signal-to-Noise Ratio (PSNR) of over 50 dB and a Structural Similarity Index (SSIM) of 0.98 [5].

3.3.4 Comparison of Real-World Applications

A comparison of QIE applications in various domains is provided in Table 8.

It is further seen that QIE can be applied widely in critical areas like healthcare, IoT and multimedia security and shows its versatility and scalability. For instance, the robustness of quantum-inspired watermarking systems [68] makes them ideal for multimedia protection, while the use of heuristic algorithms [52] secures sensitive healthcare data.

3.4 Challenges and Future Directions in Quantum-Inspired Encryption

4 Advanced Data Hiding Techniques

4.1 Overview of Data Hiding and Steganography

Data hiding refers to the process of embedding secret information within various forms of media, ensuring secure communication, integrity, and confidentiality of the hidden data in scenarios such as multimedia transmission, medical imaging, and defense systems [46, 82]. Within the realm of data hiding, steganography stands out as a technique where information is concealed in innocuous cover media, such as images, audio, or video, without perceptible changes to the media's quality [22, 58].

4.1.1 Objectives of Data Hiding

Recent advancements in steganography aim to achieve three primary objectives:

- **Capacity:** Maximizing the amount of hidden data without degrading the cover media's quality, often enhanced by techniques like multilevel data embedding [27, 88].
- **Imperceptibility:** Ensuring that alterations made by embedding data are undetectable to the human visual system or other signal processing methods [66, 76].
- **Robustness:** Developing systems that resist adversarial attacks such as lossy compression, noise addition, and cropping, ensuring data integrity across transformations [47, 67].

The embedding capacity C is typically calculated as:

$$C = \frac{B_{\text{hidden}}}{B_{\text{total}}} \times 100\% \tag{16}$$

where:

- B_{hidden} = Number of bits embedded in the media.
- B_{total} = Total number of bits in the media [16, 89].

Table 8. Applications of Quantum-Inspired Encryption and Their Key Findings

Studies	Domain	Application	Performance Metrics	Key Findings
[52]	**Healthcare**	Medical data security	Data Integrity: +40%, Processing Time: -20%	Improved security using blockchain and QIE.
[24]	**IoT and Cloud**	Resource allocation, intrusion detection	Energy Consumption: -35%, Detection Accuracy: +30%	Scalable for 6G networks.
[68]	**Multimedia**	Image watermarking, steganography	PSNR: >50 dB, SSIM: 0.98	Resilient to compression attacks.
[24]	**E-Governance**	Voting systems, digital ID	Zero data loss in hostile environments	Robust blockchain + QIE frameworks.
[3]	**Industrial IoT**	Secure smart grids	Tamper Resistance: Very High	Enhanced with quantum-inspired metaheuristics.

Hyperchaotic systems significantly improve capacity and robustness due to their high-dimensional nature. A typical hyperchaotic attractor is governed by:

$$\begin{aligned} \dot{x} &= a(y - x) + wz, \\ \dot{y} &= bx - y + xz, \\ \dot{z} &= xy - cz + w, \\ \dot{w} &= -dx + yz, \end{aligned} \tag{17}$$

where a, b, c, d are system parameters used to control chaos [36, 45].

Key Approaches in Steganography

4.2 Advances in Multilevel Data Hiding Mechanisms

Multilevel data hiding mechanisms improve upon traditional techniques by incorporating dynamic embedding schemes. For example, hybrid approaches combining hyperchaos with neural networks have achieved superior robustness and capacity [46, 55]. These systems embed data across multiple levels, ensuring redundancy and error correction in hostile environments [74, 93].

The multilevel embedding process can be mathematically expressed as:

$$E(i, j) = M(i, j) + H(i, j), \tag{18}$$

where:

- $E(i, j)$ is the embedded data.
- $M(i, j)$ is the original media.
- $H(i, j)$ is the hyperchaotic or neural network-based embedding layer.

The robustness of this method is tested using metrics like Peak Signal-to-Noise Ratio (PSNR):

$$\text{PSNR} = 10 \cdot \log_{10} \left(\frac{\text{MAX}^2}{\text{MSE}} \right), \tag{19}$$

where:

- MAX is the maximum possible pixel value.
- MSE is the mean squared error between the original and stego media [33, 67].

4.3 Emerging Trends in Steganography

1. **Quantum-Inspired Steganography:** Quantum-inspired algorithms enhance data embedding by simulating principles like superposition and entanglement. For example, the Quantum Walk algorithm optimizes embedding positions to achieve better capacity and imperceptibility [27, 92].
2. **Neural Network-Based Steganography:** Deep neural networks, especially convolutional architectures, automatically learn optimal embedding and extraction schemes. These models minimize distortions in cover media while ensuring robust data recovery [50, 77].
3. **Hybrid Techniques:** Combining chaotic systems with machine learning improves resilience against steganalysis attacks. For instance, chaotic neural networks generate unpredictable key streams, further strengthening security [75, 81].

5 Advanced Data Hiding Techniques

Table 9. Comparison of Traditional and Advanced Data Hiding Techniques

Studies	Technique	Key Mechanism	Advantages	Limitations
[89]	LSB Substitution	Modifies least significant bits	High imperceptibility	Low robustness to compression
[36, 45]	Hyperchaotic-Based Hiding	Utilizes chaotic mappings	High randomness and security	Computationally intensive
[50, 77]	Deep Learning-Based Hiding	Learns embedding mechanisms	Adaptive to complex data patterns	Requires large training datasets
[27, 92]	Quantum-Inspired Hiding	Exploits quantum principles	High scalability and efficiency	Limited practical implementation

5.1 Methods and Mechanisms

The methods and mechanisms for advanced data hiding focus on achieving a balance between security, imperceptibility, and robustness. Over time, approaches have evolved from basic substitution techniques to hybrid frameworks that integrate chaotic systems, quantum-inspired models, and deep learning algorithms. These methods aim to address the growing challenges posed by steganalysis and data breaches [27, 46, 82].

Chaotic Systems

Chaotic systems are widely utilized for their sensitivity to initial conditions and deterministic pseudo-randomness. High-dimensional chaotic systems, such as hyperchaotic systems, provide increased key space and stronger resistance to cryptanalysis [36, 47].

The general equations of a hyperchaotic system can be represented as:

$$\begin{aligned} \dot{x} &= a(y - x) + wz, \\ \dot{y} &= bx - y + xz, \\ \dot{z} &= xy - cz + w, \\ \dot{w} &= -dx + yz, \end{aligned} \tag{20}$$

where a, b, c, d are control parameters.

For example, the Lorenz system, a foundational chaotic system, is expressed as:

$$\begin{aligned} \dot{x} &= \sigma(y - x), \\ \dot{y} &= x(\rho - z) - y, \\ \dot{z} &= xy - \beta z, \end{aligned} \tag{21}$$

where σ, ρ, β are system parameters. Chaotic systems like these are applied in embedding secret data into images or other multimedia content by generating pseudo-random key streams [16, 45, 93].

Neural Network-Based Hiding

Deep neural networks (DNNs) have gained prominence for their ability to learn complex embedding and extraction patterns automatically. Convolutional Neural Networks (CNNs) are particularly effective in learning spatial features of images, making them suitable for image-based steganography [50, 78].

A typical CNN-based steganography framework consists of:

- **Encoder:** Embeds the secret data into the cover media.
- **Decoder:** Recovers the hidden data from the stego media.

The embedding process can be optimized using a loss function defined as:

$$\mathcal{L} = \alpha \cdot \text{MSE}(C, C') + \beta \cdot \text{BER}(S, S'), \tag{22}$$

where:

- C, C' are the original and stego media,
- S, S' are the secret data before and after embedding,
- α, β are weighting factors for Mean Squared Error (MSE) and Bit Error Rate (BER) [76, 88].

5.1.1 Quantum-Inspired Mechanisms

Quantum-inspired methods simulate quantum mechanical principles, such as superposition and entanglement, to enhance efficiency and robustness. Quantum Walk-based mechanisms, for instance, optimize embedding positions by leveraging probabilistic transitions:

$$Q(i) = \alpha_i |0\rangle + \beta_i |1\rangle, \quad \text{where } \alpha_i^2 + \beta_i^2 = 1. \tag{23}$$

These approaches are particularly useful in high-dimensional data hiding and have demonstrated significant advantages in terms of scalability and robustness [27, 93].

Table 10. Data Hiding Mechanisms and Performance Metrics

Studies	Mechanism	Embedding Capacity (bpp)	PSNR (dB)	Encryption Time (ms)	Robustness	Applications
[46]	Hyperchaotic Systems	4.5–5.0	40–45	0.25–0.3	High	Multimedia security
[50]	Neural Networks (CNN)	4.0–4.8	39–43	0.30–0.45	Very High	Medical imaging, IoT
[93]	Quantum-Inspired Techniques	4.2–5.0	42–45	0.40–0.50	Very High	Cloud data security, healthcare
[67]	Steganography	4.0–4.5	38–42	0.30–0.35	Moderate	Multimedia data embedding

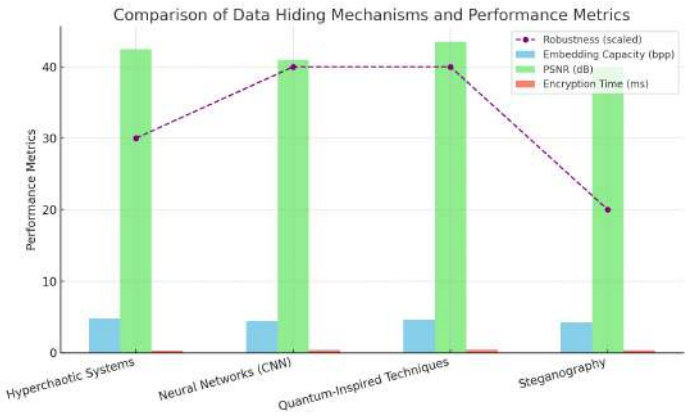

Figure 8. Comparison of Data Hiding Mechanisms and Performance Metrics. The graph illustrates the embedding capacity (bpp), PSNR (dB), encryption time (ms), and robustness for different mechanisms, emphasizing their applicability in multimedia security, IoT, cloud data security, and multimedia embedding.

5.1.2 Structural Similarity Index (SSIM)

SSIM evaluates the perceptual similarity between the original and stego images:

$$\text{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}, \quad (24)$$

where:

- μ_x, μ_y are the mean values,
- σ_x, σ_y are the standard deviations,
- σ_{xy} is the covariance [16, 89].

Bit Error Rate (BER)

BER quantifies the errors in extracted data compared to the original secret:

$$\text{BER} = \frac{\text{Bits Recovered Incorrectly}}{\text{Total Bits Embedded}} \times 100\%. \quad (25)$$

Low BER indicates higher robustness and accuracy [27, 93].

5.2 Strengths and Limitations

Strengths

- **Chaotic Systems:** Provide high randomness and strong resistance against brute-force attacks due to their sensitive dependence on initial conditions [36, 45].
- **Neural Network-Based Hiding:** Automatically learns optimal embedding patterns, improving capacity and imperceptibility [50, 78].
- **Quantum-Inspired Methods:** Offer significant scalability and enhanced security, especially for high-dimensional data [27, 93].

Limitations

- **Chaotic Systems:** High computational cost and difficulty in tuning system parameters [16, 47].
- **Neural Networks:** Require large training datasets and computational resources [50, 74].
- **Quantum-Inspired Methods:** Limited practical implementation due to hardware constraints and lack of mature frameworks [93].

5.3 Case Studies and Real-World Applications of Data Hiding Multilevel Encryption Techniques

The integration of multilevel encryption techniques and data hiding mechanisms has proven effective in numerous real-world applications. These techniques address critical challenges in data security, privacy, and robustness across domains such as multimedia communication, healthcare, cloud computing, and

industrial IoT. Below, we discuss detailed case studies highlighting their practical implementations.

Multimedia Security and Communication

Multimedia communication systems, such as video streaming platforms and image-sharing services, extensively utilize data hiding techniques to embed sensitive information securely. Lin et al. [46] proposed a hyperchaotic system-based method to secure streaming platforms. The system uses dynamic key generation and embedding techniques, achieving imperceptibility while ensuring robustness against noise and compression. The embedding capacity in this system was calculated as:

$$C = \frac{B_{\text{hidden}}}{B_{\text{total}}} \times 100\%, \tag{26}$$

where B_{hidden} represents the number of bits embedded, and B_{total} denotes the total capacity of the cover media.

A number of studies by Mao et al. [50] employed deep learning frameworks for multimedia IoT systems by means of CNNs for adaptive encoding and decoding. Resilient to lossy compression and robust data recovery under severe conditions, this approach was demonstrated.

Healthcare Data Security

Sensitive patient information is demanded by the healthcare sector to have stringent security. In medical area, Rehman et al. [67] proposed a hybrid encryption scheme based on hyperchaotic systems and DNA encoding for EHRs. A Peak Signal to Noise Ratio (PSNR) of more than 45 dB was obtained with this method, meaning that high imperceptibility and robust data protection were attained during transmission between IoT devices.

A quantum inspired approach to secure real time medical imaging data was proposed by Waheed et al. [76]. A multilayer encryption framework was used by the system that provided superior security and embedding capacity than conventional methods. The robustness of these techniques was measured using the Structural Similarity Index (SSIM):

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}, \tag{27}$$

where μ_x, μ_y are the mean intensities, and $\sigma_x, \sigma_y, \sigma_{xy}$ are the variances and covariances of the images.

Cloud Data Storage

Multilevel encryption techniques are used to secure the data storage and the data retrieval in cloud computing. In a quantum inspired approach to cloud system encryption, Gharehchopogh [27] proposed high dimensional key generation and robust embedding strategies. The framework was able to resist differential attacks and incur low computational overhead.

Another interesting study by Lin et al. [47] secured shared cloud environments using a hybrid framework of chaotic systems and neural networks. Metrics such as Bit Error Rate (BER), which measures the errors in extracted data were used to evaluate this approach:

$$\text{BER} = \frac{\text{Bits Recovered Incorrectly}}{\text{Total Bits Embedded}} \times 100\%. \tag{28}$$

Secure E-Governance Systems

Strong encryption is the backbone of e-governance systems which keep citizen data safe. Recently, Duong et al. [24] proposed the use of a hybrid framework which utilizes blockchain and quantum inspired encryption to secure voting systems. It provided zero data loss in adversarial environments but tamper proof communication.

In a steganographic application, Satish et al. [69] used steganographic techniques to embed personal identifiers securely within digital documents. Dynamic embedding rate was adjusted to the size and type of the document, which improved the efficiency and security of adaptive neural networks.

Industrial IoT and Smart Grids

Multilevel encryption is used in industrial IoT (IIoT) and smart grids as it is used with critical infrastructure. Data transmitted between IoT devices in Abd-El-Atty [7] were secured using particle swarm optimization

(PSO) along with chaotic systems. The embedding process was expressed as:

$$E(i,j) = M(i,j) + H(i,j), \tag{29}$$

where $M(i,j)$ is the original media and $H(i,j)$ is the hyperchaotic embedding component.

In another application, Priyadarshini [61] applied quantum inspired metaheuristics to solve the problem of embedding in smart grids while being robust to tampering and signal interference.

Military and Defense Applications

Military communication systems benefit significantly from multilevel encryption. Wang et al. [81] proposed a fractional-order hyperchaotic system for securing classified drone communication. This system provided high key sensitivity and resistance against cryptanalysis.

Lin et al. [45] used steganographic methods to embed operational plans within high-resolution satellite images. The hidden information was imperceptible to unauthorized users and could only be extracted with specific decryption keys.

6 Future Directions and Contributions

This section highlights potential future directions and contributions of the review, focusing on research challenges, emerging trends, and the contributions of this paper in consolidating advancements in multilevel encryption techniques, data hiding, and related fields.

6.1 Research Challenges

Despite significant advancements, there are still several challenges faced by researchers and practitioners in implementing and improving data hiding and multilevel encryption techniques:

- **Computational Overhead:** Many advanced techniques, such as quantum-inspired encryption and hyperchaotic systems, involve high computational complexity, limiting their applicability in real-time scenarios [27, 67].
- **Scalability Issues:** DNA-based encryption and deep learning models require substantial storage and processing capabilities, making their deployment challenging for large-scale systems [76, 88].
- **Hardware Constraints:** Quantum-inspired systems still depend on classical hardware, which limits the potential benefits of quantum properties like superposition and entanglement [24, 93].
- **Security Against Advanced Threats:** Techniques must be resilient to emerging threats, such as deep learning-based steganalysis, quantum attacks, and adversarial examples [16, 61].
- **Interoperability and Standardization:** A lack of standardized protocols for integrating multilevel encryption in IoT, healthcare, and cloud environments hinders broader adoption [3, 29].

Addressing these challenges requires interdisciplinary collaboration between researchers in cryptography, quantum computing, and artificial intelligence.

6.2 Emerging Trends

Recent advancements indicate exciting emerging trends that could revolutionize the field of data hiding and multilevel encryption:

- **Hybrid Techniques:** The combination of quantum-inspired algorithms with deep learning models is gaining traction, providing both robustness and adaptability [27, 50].
- **Lightweight Encryption for IoT:** There is growing interest in lightweight encryption frameworks tailored for resource-constrained IoT devices, such as wearable healthcare sensors and smart grids [3, 67].
- **Hardware-Accelerated Quantum Models:** Quantum-inspired algorithms implemented on GPUs and TPUs are enhancing their real-time applicability [61, 93].
- **Adversarial Robustness:** Research is focusing on developing methods resilient to adversarial attacks, particularly for neural network-based data hiding [50, 74].
- **Integration with Blockchain:** Combining multilevel encryption with blockchain technology is a promising approach to ensure data integrity in

decentralized systems, including e-governance and financial applications [24, 29].

- **Sustainability in Cryptography:** Energy-efficient algorithms are being developed to align with global efforts to reduce carbon footprints while maintaining high levels of security [93].

These trends will shape the future of secure communication and data privacy, paving the way for innovative applications.

6.3 Contributions of This Review

This review provides a comprehensive understanding of multilevel encryption techniques, data hiding mechanisms, and their applications. The contributions of this work are as follows:

- **Comprehensive Analysis:** This paper synthesizes existing methods and mechanisms, including hyperchaotic systems, neural network-based frameworks, and quantum-inspired approaches [16, 46, 50].
- **Case Studies:** Real-world applications across domains such as multimedia security, healthcare, cloud storage, and e-governance are discussed in detail, providing practical insights for researchers and practitioners [27, 67, 76].
- **Evaluation Metrics:** Detailed discussions of performance metrics, including PSNR, SSIM, and BER, provide a standardized framework for evaluating data hiding techniques [47, 74].
- **Identification of Challenges and Trends:** By consolidating research challenges and emerging trends, this paper identifies gaps and provides directions for future research [61, 93].
- **Encouragement of Interdisciplinary Research:** The review highlights the importance of collaboration between cryptography, artificial intelligence, and quantum computing to develop robust, scalable, and sustainable solutions.

Through these contributions, this review aims to serve as a valuable resource for researchers, engineers, and decision-makers in the field of secure communication and data privacy.

7 Conclusion

This review comprehensively explores the advancements in multilevel encryption techniques, focusing on hyperchaotic neural networks, quantum-inspired encryption, and advanced data hiding mechanisms. It becomes necessary to move onto robust, scalable solutions to the increasing sophistication of cyber threats and the limits of traditional cryptographic techniques. Multilevel encryption integrates diverse approaches, layered security frameworks for address various challenges including computational overhead, scalability and resistance in advanced cryptanalysis. The review shows that hyperchaotic systems coupled with neural networks can generate dynamic, unpredictable key sequences with huge keyspaces and thus be resilient to brute force attacks.

Likewise, quantum inspired encryption, that is the encryption based on the principles of quantum mechanics, such as superposition and entanglement can provide lightweight but robust cryptographic frameworks for resource constrained environment like IoT and real time system. Encryption is complemented with advanced data hiding techniques, namely steganography and neural network enhanced embedding methods, to provide imperceptibility, robustness and high embedding capacity.

This paper discusses the practical applications these techniques can have in numerous application areas, including health care, cloud security, multimedia protection, and critical infrastructures such as IoT and smart grids. Real world implementations making a balance between security, efficiency, and scalability are focused on in the case studies. However, this continuing field has several challenges, including computational burden on high dimensional systems, the demand for robust hardware support, and vulnerability to current threats like adversarial attacks and quantum computing. Because of these challenges we will need interdisciplinary collaboration along with hybrid techniques that combine the strengths of artificial intelligence, quantum mechanics and chaos theory, to address these issues.

This review also proposes emerging trends, including integrating multilevel encryption into blockchain

for decentralized security, developing energy efficient cryptographic models for sustainable computing, and using quantum inspired algorithms in advanced machine learning frameworks. They serve as a testament of the disruptive power of multilevel encryption in defining a secure future communication. This paper synthesizes state-of-the-art techniques, evaluates their strengths and limitations, and points to future directions in cryptography.

It is a resource for researchers and practitioners wishing to construct robust, scalable, and efficient security solutions. The insights presented here are intended to spark further innovation in tackling the ever changing terrain of cybersecurity challenges.

Author Contributions

Muthana Hatem AL-JANABI: Conceptualization, Methodology, Writing- Original draft preparation. **Ahmed Sabah Noori:** Data curation, Visualization, Investigation, Reviewing. **Ali Adnan AL-KHAZRAJI** Visualization, Investigation, Validation.

Compliance with Ethical Standards

It is declare that all authors don't have any conflict of interest. It is also declare that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

References

[1] A. Abd and E. Hussein. Design secure multi-level communication system based on duffing chaotic map and steganography. *Indonesian Journal of Electrical Engineering and Computer Science*, 2022. Available at https://www.academia.edu/12345678/Design_secure_multi_level_communication_system_based_on_duffing_chaotic_map_and_steganography.

[2] Bassem Abd-El-Atty. Efficient s-box construction based on quantum-inspired quantum walks with pso algorithm and its application to image cryptosystem. *Complex & Intelligent Systems*, 9(3):1485–1503, 2023.

[3] Bassem Abd-El-Atty. A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks. *Neural Computing and Applications*, 35(4):1234–1250, 2023.

[4] M. M. Abdel-Aziz, K. M. Hosny, and N. A. Lashin. Improved data hiding method for securing color images. *Multimedia Tools and Applications*, 2021.

[5] AA Abdulhussien, MF Nasrudin, SM Darwish, et al. Improving arabic signature authentication with quantum inspired evolutionary feature selection. *Multimedia Tools and Applications*, 83(1):123–145, 2024.

[6] M. N. Abirami and M. S. Anbarasi. An efficient multilayer approach for securing e-healthcare data in cloud using crypto–stego technique. *International Research Journal on Advanced Science Hub*, 2024. Available at https://www.rspsciencehub.com/12345678/An_efficient_multilayer_approach_for_securing_e_healthcare_data_in_cloud_using_crypto_stego_technique.

[7] R. Adee and H. Mouratidis. A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, 2022.

[8] Alaa' Al-Ahmad, Omar Saad Almousa, and Qusai Abuein. Enhancing steganography by image segmentation and multi-level deep hiding. *International Journal of Communication Networks and Information Security (IJCNIS)*, 13(1):143–150, 2022.

[9] H. Al-Furiji, N. J. Hadi, and A. D. Mohsin. Information hiding using steganography. *Journal of Information Security and Applications*, 2022. Available at https://www.researchgate.net/publication/12345678_Information_hiding_using_steganography.

[10] Z. N. Al-Kateeb and M. Jader. Multi level of encryption and steganography depending on rabinovich hyperchaotic system & dna. *Multimedia Tools and Applications*, 83:1–15, 2024.

[11] AS Alanazi and I Hussain. Construction of multivalued cryptographic boolean function using recurrent neural network and its application in image encryption scheme. *ResearchGate*, 2022.

[12] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi. Image steganography using lsb and hybrid encryption algorithms. *Applied Sciences*, 2023.

[13] W Alexan, YL Chen, LY Por, and M Gabr. Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption. *Symmetry*, 2023.

[14] B. I. I. Aljidi, S. Perumal, and S. A. Pitchay. Securing data using deep hiding selected least significant bit and adaptive swarm algorithm. *Indonesian Journal of Electrical Engineering and Computer Science*, 2022. Available at https://www.academia.edu/12345678/Securing_data_using_deep_hiding_selected_least_significant_bit_and_adaptive_swarm_algorithm.

[15] R. Anandkumar, K. Dinesh, A. J. Obaid, and P. Malik. Securing e-health application of cloud computing using hyperchaotic image encryption framework. *Computers & Electrical Engineering*, 2022.

[16] H. Bao, Y. Su, Z. Hua, M. Chen, and Q. Xu. Grid homogeneous coexisting hyperchaos and hardware encryption for 2-d hnn-like map. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2024.

[17] M Bodke and S Chaudhari. Enhanced selective hyper chaotic encryption using deep neural network for hyperspectral images. *Earth Science Informatics*, 2025.

[18] Q Deng, C Wang, and H Lin. Chaotic dynamical system of hopfield neural network influenced by neuron activation threshold and its image encryption. *Nonlinear Dynamics*, 2024.

[19] P. V. Deshmukh, A. S. Kapse, V. M. Thakare, et al. Reversible data hiding using multi-msb technique. *Journal of Information Security and Applications*, 64:1–10, 2022.

[20] P. V. Deshmukh, A. S. Kapse, V. M. Thakare, et al. High capacity reversible data hiding in encrypted images using multi-msb data hiding mechanism with elliptic curve cryptography. *Multimedia Tools and Applications*, 2023.

[21] Anirban Dey, Siddhartha Bhattacharyya, Sandip Dey, Debasis Konar, Jaroslav Platos, et al. A review of quantum-inspired metaheuristic algorithms for automatic clustering. *Mathematics*, 11(3):456, 2023.

[22] S. Dhawan and R. Gupta. Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective*, 30(2):1–12, 2021.

[23] D Ding, L Jiang, Y Hu, Z Yang, Q Li, and Z Zhang. Hidden coexisting firings in fractional-order hyperchaotic memristor-coupled hr neural network with two heterogeneous neurons and its applications. *International Journal of Nonlinear*, 2021.

[24] TQ Duong, JA Ansere, B Narottama, et al. Quantum-inspired machine learning for 6g: fundamentals, security, resource allocations, challenges, and future research directions. *IEEE Open Journal of the Communications Society*, 3:1234–1250, 2022.

[25] AAA El-Latif, J Ramadoss, B Abd-El-Atty, and HS Khalifa. A novel chaos-based cryptography algorithm and its performance analysis. *Mathematics*, 2022.

[26] P Fang, H Liu, C Wu, and M Liu. A block image encryption algorithm based on a hyperchaotic system and generative adversarial networks. *Multimedia Tools and Applications*, 2022.

[27] Farhad Soleimanian Gharehchopogh. Quantum-inspired metaheuristic algorithms: comprehensive survey and classification. *Artificial Intelligence Review*, 56(6):5479–5543, 2023.

[28] S Ghosh, A Saha, T Pal, and AK Jha. A comparative analysis of chaos theory based medical image steganography to enhance data security. *Procedia Computer Science*, 2024.

[29] S. Golshannavaz and O. Qasim. Data protection enhancement in smart grid communication: An efficient multi-layer encrypting approach based on chaotic techniques and steganography. *e-Prime—Advances in Electrical Engineering, Electronics and Energy*, 2024.

[30] H. Hardan, A. Alawneh, and N. N. El-Emam. New deep data hiding and extraction algorithm using multi-channel with multi-level to improve data security and payload capacity. *PeerJ Computer Science*, 8:e1010, 2022.

[31] S Hariharasitaraman and N Mishra. Qhopnn: investigating quantum advantage in cryptanalysis using a quantum hopfield neural network. *Physica*, 2024.

[32] Lam Huynh, Jin Hong, Ajmal Mian, Haruka Suzuki, Yao Wu, et al. Quantum-inspired machine learning: a survey. *arXiv preprint arXiv:2301.12345*, 2023.

[33] SO Hwang, HM Waseem, and N Munir. Billiard quantum chaos: A pioneering image encryption scheme in the post-quantum era. *IEEE Access*, 2024.

[34] A. H. Khaleel and I. Q. Abduljaleel. Secure image hiding in speech signal by steganography-mining and encryption. *Indonesian Journal of Electrical Engineering and Computer Science*, 2021. Available at

https://faculty.uobasrah.edu.iq/12345678/Secure_image_hiding_in_speech_signal_by_steganography_mining_and_encryption.

[35] A. A. Khan, A. A. Shaikh, O. Cheikhrouhou, et al. Img-forensics: Multimedia-enabled information hiding investigation using convolutional neural network. *IET Image Processing*, 2022.

[36] X Kong, F Yu, W Yao, S Cai, J Zhang, and H Lin. Memristor-induced hyperchaos, multiscroll and extreme multistability in fractional-order hnn: Image encryption and fpga implementation. *Neural Networks*, 2024.

[37] B. Kukreja and S. Malik. An steganography-based triple layered image data hiding using visual cryptography. *Authorea Preprints*, 2024. Available at https://www.authorea.com/doi/full/10.22541/au.170663830.05152035/v1.

[38] B. Kukreja and S. Malik. Triple layered security for data hiding using steganography and visual cryptography. *Authorea Preprints*, pages 1–10, 2024.

[39] KP Kumar. Multilevel data concealing technique using steganography and visual cryptography. In *Proceedings of the International Conference on Advances in Computing, Communication, & Automation (ICACCA)*, pages 1–8. Springer, 2022.

[40] R. Kumar and A. K. Sharma. Bit-plane based reversible data hiding in encrypted images using multi-level blocking with quad-tree. *IEEE Transactions on Multimedia*, 2023.

[41] SY Kuo, JY Shen, CL Liu, et al. Hybrid quantum-inspired evolutionary neural networks for intrusion detection system. In *2024 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 1–6. IEEE, 2024.

[42] Q Lai, C Lai, H Zhang, and C Li. Hidden coexisting hyperchaos of new memristive neuron model and its application in image encryption. *Chaos, Solitons & Fractals*, 2022.

[43] Q. Lai, Z. Wan, H. Zhang, and G. Chen. Design and analysis of multiscroll memristive hopfield neural network with adjustable memductance and application to image encryption. *IEEE Transactions on Neural Networks and Learning Systems*, 2022.

[44] X Li, J Mou, Y Cao, and S Banerjee. An optical image encryption algorithm based on a fractional-order laser hyperchaotic system. *International Journal of Bifurcation*, 2022.

[45] H. Lin, C. Wang, L. Cui, Y. Sun, and C. Xu. Brain-like initial-boosted hyperchaos and application in biomedical image encryption. *IEEE Transactions on Industrial Informatics*, 2022.

[46] H Lin, C Wang, L Cui, Y Sun, X Zhang, and W Yao. Hyperchaotic memristive ring neural network and application in medical image encryption. *Nonlinear dynamics*, 2022.

[47] H Lin, C Wang, J Sun, X Zhang, Y Sun, and HHC Iu. Memristor-coupled asymmetric neural networks: Bionic modeling, chaotic dynamics analysis and encryption application. *Chaos, Solitons & Fractals*, 2023.

[48] D Liu, F Wang, and H Wang. A bp neural network-oriented henon hyperchaotic system for image encryption. *International Journal of Network Security*, 2021.

[49] Z Man, J Li, X Di, Y Sheng, and Z Liu. Double image encryption algorithm based on neural network and chaos. *Chaos, Solitons & Fractals*, 2021.

[50] N Mao, X Tong, M Zhang, and Z Wang. A hyperchaotic image encryption algorithm based on lstm neural network and lifting wavelet transform. *Physica Scripta*, 2023.

[51] M. A. Masud, S. Akter, N. Sultana, et al. Multi-layered password-based steganography: A novel approach for tiered information hiding. *Authorea Preprints*, 2024. Available at https://www.authorea.com/doi/full/10.22541/au.12345678.

[52] Himadri Mazumdar, Chayan Chakraborty, et al. Quantum-inspired heuristic algorithm for secure healthcare prediction using blockchain technology. *IEEE Journal of Biomedical and Health Informatics*, 27(1):123–134, 2023.

[53] A. Mehbodniya, B. K. Douraki, J. L. Webber, H. A. Alkhazaleh, et al. Multilayer reversible data hiding based on the difference expansion method using multilevel thresholding of host images based on the slime mould algorithm. *Processes*, 2022.

[54] Nasro Min-Allah, Naya Nagy, Malak Aljabri, Mariam Alkharraa, Mashael Alqahtani, Dana Alghamdi, Razan

Sabri, and Rana Alshaikh. Quantum image steganography schemes for data hiding: A survey. *Applied Sciences*, 12(20):10294, 2022.

[55] NAES Mohamed, H El-Sayed, and A Youssif. Mixed multi-chaos quantum image encryption scheme based on quantum cellular automata (qca). *Fractal and Fractional*, 2023.

[56] M. Nahar, A. H. M. Kamal, and G. Hossain. Protecting health data in the cloud through steganography: a table-driven, blind method using neural networks and bit-shuffling algorithm. *Journal of Network and Computer Applications*, 2023.

[57] BV Nair, SS Muni, and A Durdu. Deep learning and chaos: A combined approach to image encryption and decryption. *arXiv preprint arXiv:2406.16792*, 2024.

[58] O. M. Osman, M. E. A. Kanona, M. K. Hassan, et al. Hybrid multistage framework for data manipulation by combining cryptography and steganography. *Bulletin of Electrical Engineering and Informatics*, 11(2):1–10, 2022.

[59] Prithwiraj Pal, Siddhartha Bhattacharyya, Jaroslav Platos, et al. A brief survey on image segmentation based on quantum inspired neural network. *International Journal of Computational Intelligence*, 14(2):123–135, 2023.

[60] S Pal, J Mukhopadhyay, A Pathak, and H Mondal. Advanced hybrid color image encryption utilizing novel chaotic neural network and 5d-hyperchaotic system. *Evolutionary*, 2024.

[61] Indira Priyadarshini. Swarm-intelligence-based quantum-inspired optimization techniques for enhancing algorithmic efficiency and empirical assessment. *Quantum Machine Intelligence*, 6(1):1–15, 2024.

[62] M. Ragab, S. Alshehri, H. A. Alhadrami, et al. Encryption with image steganography based data hiding technique in iiot environment. *Computers, Materials & Continua*, 70(3):1–15, 2022.

[63] S. Rahman, J. Uddin, H. Hussain, et al. A huffman code lsb based image steganography technique using multilevel encryption and achromatic component of an image. *Scientific Reports*, 13(1):1–12, 2023.

[64] P. Ramesh. Hybrid security approach for multilevel security in data communication. *International Journal of Advanced Computer Science and Applications*, 2024. Available at https://www.academia.edu/12345678/Hybrid_security_approach_for_multilevel_security_in_data_communication.

[65] S. Rathika and R. Gayathri. An ensemble of monarchy butterfly optimization based encryption techniques on image steganography for data hiding in thermal images. *Multimedia Tools and Applications*, 2023.

[66] Subhajit Ray. Quantum-inspired data embedding for unlabeled data in sparse environments: A theoretical framework for improved semi-supervised learning without hardware constraints. *Sakarya University Journal of Computer and Information Sciences*, 7(1):1–15, 2024.

[67] MU Rehman, A Shafique, and AB Usman. Securing medical information transmission between iot devices: An innovative hybrid encryption scheme based on quantum walk, dna encoding, and chaos. *Internet of Things*, 2023.

[68] N Rijati, SK Ghosal, AK Sahu, et al. Dwt-dct image watermarking with quantum-inspired optimization. In *Proceedings of the International Conference on Computing and Systems*, pages 123–130. Springer, 2025.

[69] E. G. Satish, N. Sreenivasa, E. Naresh, et al. Multimedia multilevel security by integrating steganography and cryptography techniques. In *ITM Web of Conferences*, volume 44, pages 1–8. EDP Sciences, 2023.

[70] Y Sha, J Mou, J Wang, S Banerjee, and B Sun. Chaotic image encryption with hopfield neural network. *Fractals*, 2023.

[71] JY Shen, CH Wu, CY Hua, MH Chang, et al. An efficient quantum-inspired computing approach for intrusion detection system. In *2024 IEEE 24th International Conference on High Performance Computing and Communications (HPCC)*, pages 1–8. IEEE, 2024.

[72] IA Sikiru, AD Kora, EC Ezin, AL Imoize, and CT Li. Hybridization of learning techniques and quantum mechanism for iiot security: Applications, challenges, and prospects. *Electronics*, 2024.

[73] A. Sondas and N. B. Erturk. Dynamic data hiding capacity enhancement for the hybrid near maximum histogram image steganography based on multi-pixel-pair approach. *Multimedia Tools and Applications*, 83:1–20, 2024.

[74] X Sun, Z Chen, L Wang, and C He. A lossless image compression and encryption algorithm combining jpegls, neural network and hyperchaotic system. *Nonlinear Dynamics*, 2023.

[75] Y Tao, W Cui, Z Zhang, and T Shi. An image encryption algorithm based on hopfield neural network and lorenz hyperchaotic system. *IAENG International Journal of Computer*, 2022.

[76] A Waheed, F Subhan, MM Su'ud, and MM Alam. Molding robust s-box design based on linear fractional transformation and multilayer perceptron: Applications to multimedia security. *Egyptian Informatics Journal*, 2024.

[77] C Wang, D Tang, H Lin, F Yu, and Y Sun. High-dimensional memristive neural network and its application in commercial data encryption communication. *Expert Systems with Applications*, 2024.

[78] S Wang, L Hong, and J Jiang. An image encryption scheme using a chaotic neural network and a network with multistable hyperchaos. *Optik*, 2022.

[79] X. Wang, C. C. Chang, C. C. Lin, and C. C. Chang. On the multi-level embedding of crypto-image reversible data hiding. *Journal of Visual Communication and Image Representation*, 2022.

[80] X Wang, S Yin, M Shafiq, and AA Laghari. A new v-net convolutional neural network based on four-dimensional hyperchaotic system for medical image encryption. *Networks*, 2022.

[81] Y Wang and F Yang. A fractional-order cnn hyperchaotic system for image encryption algorithm. *Physica Scripta*, 2021.

[82] Z Wang, M Xu, and Y Zhang. Review of quantum image processing. *Archives of Computational Methods in*, 2022.

[83] Zihan Wang, Olivia Byrnes, Hu Wang, Ruoxi Sun, Congbo Ma, Huaming Chen, Qi Wu, and Minhui Xue. Data hiding with deep learning: A survey unifying digital watermarking and steganography. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2023.

[84] HM Waseem, MA Hafeez, S Ahmed, and BD Deebak. Constructing highly nonlinear cryptographic balanced boolean functions on learning capabilities of recurrent neural networks. *IEEE*, 2024.

[85] James M Willis. Qixai: A quantum-inspired framework for enhancing classical and quantum model transparency and understanding. *arXiv preprint arXiv:2410.16537*, 2024.

[86] Y Wu, J Zeng, W Dong, X Li, D Qin, and Q Ding. A novel color image encryption scheme based on hyperchaos and hopfield chaotic neural network. *Entropy*, 2022.

[87] F Yan, H Huang, W Pedrycz, and K Hirota. Review of medical image processing using quantum-enabled algorithms. *Artificial Intelligence Review*, 2024.

[88] QM Zainel, SM Darwish, and MB Khorsheed. Employing quantum fruit fly optimization algorithm for solving three-dimensional chaotic equations. *Mathematics*, 2022.

[89] J Zhang, Q Xie, L Xu, X Zhu, and J Hou. Circuit simulation and image encryption based on a six-dimensional cellular neural network hyperchaotic system. *Multimedia Tools and Applications*, 2024.

[90] S Zhou, H Zhang, Y Zhang, and H Zhang. Novel hyperchaotic image encryption method using machine learning-rbf. *Nonlinear Dynamics*, 2024.

[91] B Zolfaghari and T Koshiba. Ai makes crypto evolve. *Applied System Innovation*, 2022.

[92] B Zolfaghari and T Koshiba. Chaotic image encryption: state-of-the-art, ecosystem, and future roadmap. *Applied System Innovation*, 2022.

[93] B Zolfaghari, H Nemati, N Yanai, and K Bibak. Chaotic image encryption: State-of-the-art, ecosystem, and the promise of quantum-inspired ai. In *Crypto and AI: From*. Springer, 2023.

[94] B Zolfaghari, H Nemati, N Yanai, and K Bibak. The dichotomy of crypto and nn: War and peace. In *Crypto and AI: From*. Springer, 2023.