IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received 23 January 2024, accepted 15 February 2024, date of publication 19 February 2024, date of current version 26 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3367232

RESEARCH ARTICLE

Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques

ABID MEHMOOD[1], (Member, IEEE), ARSLAN SHAFIQUE[2], MOATSUM ALAWIDA[1], AND ABDUL NASIR KHAN[3]

[1]Department of Computer Sciences, Abu Dhabi University, Khalifa city, Abu Dhabi, United Arab Emirates
[2]School of Biomedical Engineering, University of Glasgow, G12 8QQ Glasgow, U.K.
[3]Department of Computer Science, COMSATS University Islamabad, Abbottabad Campus, Abbottabad 45550, Pakistan

Corresponding author: Abdul Nasir Khan (anasir@cuiatd.edu.pk)

This work was supported by Abu Dhabi University's Office of Sponsored Programs in the United Emirates under Grant 19300752.

ABSTRACT In the contemporary landscape, where a huge amount of data plays a vital role, the importance of strong and robust cybersecurity measures has become increasingly paramount. This research proposes a review and extensively explores cybersecurity techniques within the domain of machine/deep learning and quantum techniques, with a particular focus on cryptographic methods and methodologies applied to image encryption. The proposed survey covers a range of cybersecurity techniques, including quantum random number generation, secure transmission of quantum images, watermarking through quantum methods, and quantum steganography. Moreover, it explores the domain of image encryption, which integrates adversarial neural networks, deep learning and machine learning, transformation techniques, and chaotic neural networks that can be used to secure digital data from cyber attacks. Our focus extends beyond highlighting advances in investigating vulnerabilities in existing cryptographic techniques. By identifying the challenges and weaknesses, the potential solutions are also presented, establishing a foundation for future recommendations. These future suggestions address and overcome the vulnerabilities observed in existing cybersecurity techniques. The aim of the extensive survey and analysis of existing cryptographic techniques is to provide a deep understanding of innovative and diverse approaches within the cybersecurity domain. Simultaneously, it aims to create a roadmap for the future to counter potential cyber threats and challenges.

INDEX TERMS Cybersecurity, machine learning, deep learning, quantum cryptography, cryptographic techniques.

I. INTRODUCTION

In today's fast-paced digital world, cybersecurity is a shield against a growing number of threats that come with technological advancements. Cybersecurity protocols are important in the present era because most digital systems, such as distributed file systems, NoSQL databases, and network-attached storage (NAS), are used to store large amounts of data [1], [2], [3]. Such systems also provide strong connectivity and convenience, but also bring some risks related to the transformation of data over an insecure channel known as the Internet. Sensitive data that is stored in digital systems can face different types of cyberattacks, such as differential attacks and statistical attacks [4], [5]. Furthermore, there is a high risk of data theft by an unauthorized entity where many digital devices, such as smart

The associate editor coordinating the review of this manuscript and approving it for publication was Senthil Kumar.

homes, wearables, and industrial systems, are connected in the Internet of Things (IoT) environment [6], [7], [8]. An IoT environment is a large network where big data is being transferred nowadays. Digital devices can be vulnerable to cyber attacks, which is why there is a serious need for robust cybersecurity techniques [9]. The big data means that there is a bunch of sensitive information, including financial details and important business data.

Modern techniques such as Advanced Persistent Threats (APTs) [10], Ransomware [11], and Phishing [12] can exploit and steal sensitive data. These incidents not only result in significant financial losses for businesses and individuals, but also damage their reputations and undermine consumer trust. In addition to the financial impact, cyber threats can also cause real damage to critical infrastructure. Robust approaches, including encryption protocols [13], segmentation networks [14], and implementation of access controls that incorporate intrusion detection systems [15], can be used to prevent data from being attacked. Dealing with cybersecurity also involves policies, education, and collaboration. It requires a great deal of effort that brings together government initiatives, industry collaborations, and cybersecurity education. This collective approach can improve the understanding of attacks and improve the integrity and confidentiality of digital data [16], [17].

A. CONFIDENTIALITY, INTEGRITY, AUTHENTICATION, AND NON-REPUDIATION THROUGH ENCRYPTION

In the digital world, where most digital devices are interconnected, the use of cryptographic techniques is important to keep conversations, communications, and sensitive data secure [18], [19]. Cryptography is about transforming information into an unreadable message that helps prevent unauthorized access to confidential data and ensures that digital communication and data remain private and intact [20].

Moreover, cryptographic methods play an important role in maintaining confidentiality [21], integrity [22], authentication [23], and nonrepudiation [24] in communication systems where a large amount of data is transferred. Furthermore, a cryptographic tool known as digital signatures [25] can help streamline the signing of electronic documents or transactions to validate the authenticity and integrity of the content. Similarly, the hash function [26] facilitates the verification of data integrity by generating unique hash values for the original data. Cryptographic protocols like SSL/TLS [27] authenticate website identities that provide the guarantee of secure online transactions. Collectively, such cryptographic methodologies strengthen communication systems in terms of cybersecurity and establish a robust framework for secure data exchange [28], [29]. Non-repudiation is another essential cryptographic tool that provides a guarantee that entities in a communication or transaction cannot later repudiate the legitimacy of the messages exchanged. Figure 1 illustrates the various fundamental cryptographic tools that strengthen the robustness of sensitive information against cyberattacks.

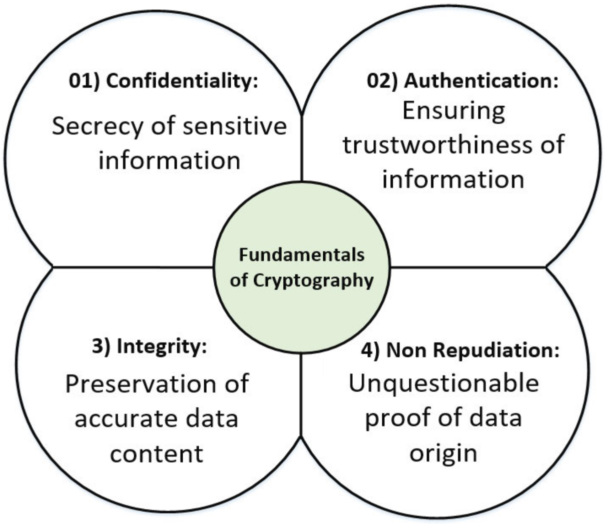
01) Confidentiality:
Secrecy of sensitive information
02) Authentication:
Ensuring trustworthiness of information
Fundamentals of Cryptography
3) Integrity:
Preservation of accurate data content
4) Non Repudiation:
Unquestionable proof of data origin

FIGURE 1. Key cryptographic elements tools are required to enhance the robustness of sensitive information against cyberattacks.

The development of a robust cryptographic scheme for digital data is important for the following several reasons:

- The robust cryptographic scheme guarantees the confidential transmission of sensitive information such as military information and medical records [30].
- Encryption plays an important role in maintaining data integrity specifically in the context of medical information [31]. By mitigating the potential for unauthorized alterations, encryption helps prevent the occurrence of wrong diagnoses.
- A reliable and robust encryption system protects sensitive information against potential breaches or manipulations by malicious entities [32].

B. CONTRIBUTIONS OF THE PAPER

The major contributions of this research are as follows:

- **Comprehensive review of cybersecurity techniques:** The proposed survey provides a comprehensive review of the existing cryptographic technologies in the areas of quantum encryption, machine learning, deep learning, and cryptographic techniques. Moreover, the proposed study also explores a variety of cutting-edge approaches such as quantum random number generation, secure transmission of quantum images, watermarking through quantum methods, and quantum steganography.
- **Focus on cryptographic methods for image encryption:** The proposed research focuses on the cryptographic techniques that are applied for image encryption. Various existing cryptographic techniques are analyzed, such as adversarial neural networks, deep hashing, transformation techniques, and chaotic neural networks.
- **Identification of vulnerabilities and weaknesses:** This research examines and identifies the challenges and weaknesses in the existing cryptographic techniques. By pinpointing the vulnerabilities, the aim of the

research is to enhance awareness of potential attacks and gaps in the existing cryptographic techniques.

- **Presentation of potential solutions:** In response to the weaknesses and vulnerabilities identified in the existing cryptographic techniques, this research proposes potential solutions to strengthen the existing techniques in terms of security. Moreover, the suggested potential solutions offer valuable insights for future cybersecurity enhancements.
- **Establishment of a foundation for future recommendations:** The proposed research establishes a foundation for future research in the field of cybersecurity. By addressing the challenges, weaknesses, and vulnerabilities, this survey establishes the foundation for the advancement of cybersecurity measures.
- **Creation of a roadmap for future cybersecurity:** The proposed survey provides a comprehensive roadmap for future cybersecurity research. It aims to guide researchers in countering potential cyber threats and challenges by leveraging innovative, novel, and diverse cryptographic approaches. Figure 2 shows the stepwise contribution of the proposed survey.

The remaining part of the proposed survey is structured as follows: Section II outlines the essential components that should be incorporated into any cryptographic scheme. Sections III, IV, V, VI, VII, VIII, IX and X are dedicated to the overview of the existing cryptographic techniques. In Section XI, challenges and research gaps in existing cryptographic techniques are discussed, together with the corresponding future directions to address these challenges. Finally, Section XII concludes the proposed survey.

II. ESSENTIAL ELEMENTS OF IMAGE ENCRYPTION

During the development of an algorithm for image encryption, it should be ensured that the cryptographic components used in it can provide robust security to digital data or not [33], [34]. The robust encryption algorithm should contain the following characteristics:

- **Perceptual Security:** Perception security relates to the visualization of the original data. For instance, if the data is encrypted using an encryption algorithm, the original data should not be visible in the encrypted [35]. It must be properly concealed.
- **Keyspace Importance:** Keyspace provides security to the encrypted data from brute force attacks. According to Alvazir [36], the key space must be equal to or greater than 2^{100} in order to resist the brute force attack.
- **Key Sensitivity:** Key sensitivity refers to a minor change in a secret key that can lead to a significant change in a decrypted message [37]. To develop a highly key-sensitive encryption algorithm, most researchers are using chaos theory. Chaotic maps are highly sensitive to initial conditions and control parameters, which can be used as secret keys in an encryption algorithm [38], [39].
- **Defense Against Attacks:** Robust encryption should withstand various attacks, such as ciphertext-only attacks. known-plaintext attack, and differential attacks [40].
- **Computational Complexity:** To implement an encryption scheme in real-time applications, it must be computationally efficient. For example, in drone applications, an encryption algorithm with high computational efficiency is essential where minimal processing is required [41], [42], [43].
- **Compression Ratio Invariance (CRI)**: Maintaining the CRI [44] of encrypted images is necessary to preserve storage space, image quality, and data transfer rates [45].
- **Real-Time Demands:** In real-time scenarios such as image surveillance, the encryption and decryption processes should not cause any delays [46].
- **Multi-Level Security:** To maintain high-level security, it is necessary to implement several encryption methods, such as the bit-plane extraction method [47], chaotic maps [48], and encryption with neural networks [49]. While maintaining multilevel security by implementing multiple encryption methods, it is also important to keep the processing time as low as possible.
- **Transmission Error Tolerance:** Robust encryption systems should possess the capability to accurately decrypt every individual bit of the original data, such as textual data, from the encrypted data [50]. It is not suitable if the original data and the decrypted data differ after transmission through any network. In the case of image data, achieving an exact decryption of the original data is not mandatory; instead, it should be perceptually identical to the original data. Figure 3 illustrates the subcategories associated with each respective characteristic.

A. EVALUATION OF CRYPTOGRAPHIC ALGORITHMS

To gauge the efficacy of encryption schemes, a variety of metrics and criteria have been used in recent decades [51], [52], [53], [54]. The assessment metrics are as follows:

- **Visual Assessment:** Visual assessment refers to whether the content of the original image is present within the encrypted image or not. The absence of visible information in an encrypted message indicates that the image pixels are properly concealed.
- **Statistical Analysis:** Analyzing the security of data using statistical measures such as entropy, correlation, and energy refers to statistical analysis.
- **Differential Analysis:** Understanding the concept of the impact of changing a single bit of secret key on the encrypted image.
- **Security Analysis:** This includes evaluating the robustness of encryption techniques using key sensitivity analysis, perceptual security, and key space analysis. Detailed subcategories of the metrics that can be used for the evaluation of encryption schemes are shown in Figure 4. Additionally, the evaluation metrics are summarized in Table 1.

In recent decades, researchers have proposed numerous cryptographic schemes, some of which have undergone

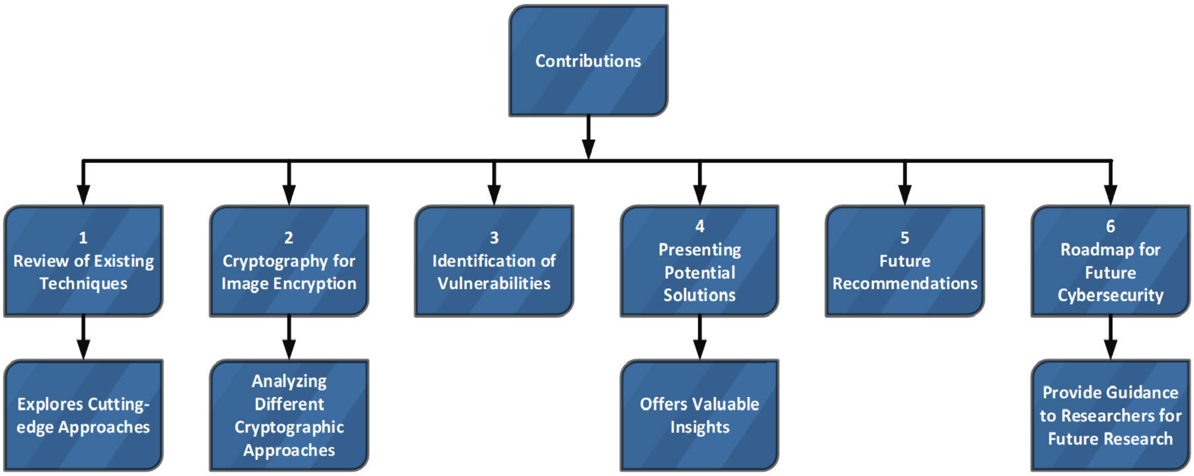
Contributions
1 Review of Existing Techniques
2 Cryptography for Image Encryption
3 Identification of Vulnerabilities
4 Presenting Potential Solutions
5 Future Recommendations
6 Roadmap for Future Cybersecurity
Explores Cutting-edge Approaches
Analyzing Different Cryptographic Approaches
Offers Valuable Insights
Provide Guidance to Researchers for Future Research

FIGURE 2. Stepwise contribution of the proposed survey.

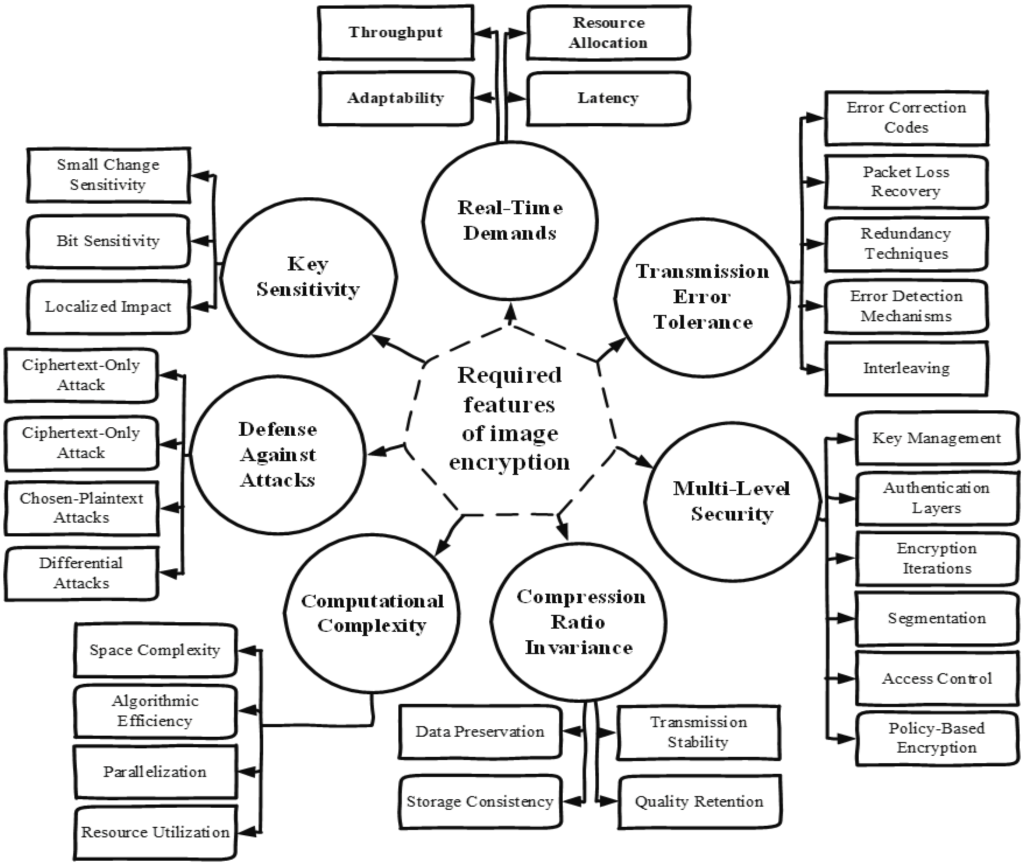

FIGURE 3. Required features of image encryption and their corresponding sub-categories.

cryptanalysis, successfully revealing vulnerabilities in existing techniques [55], [56], [57], [58]. The proposed survey examines several major categories where cryptographic techniques have been introduced. Furthermore, the next sections offer a thorough examination of existing cryptographic techniques and highlight their vulnerabilities. The categories of cryptographic techniques covered in this survey are illustrated in Figure 5. Meanwhile, Table 2 outlines the comparison between the proposed survey and the existing ones. The table suggests that the proposed survey offers a comprehensive review of a wide range of cryptographic schemes in comparison with the existing surveys.

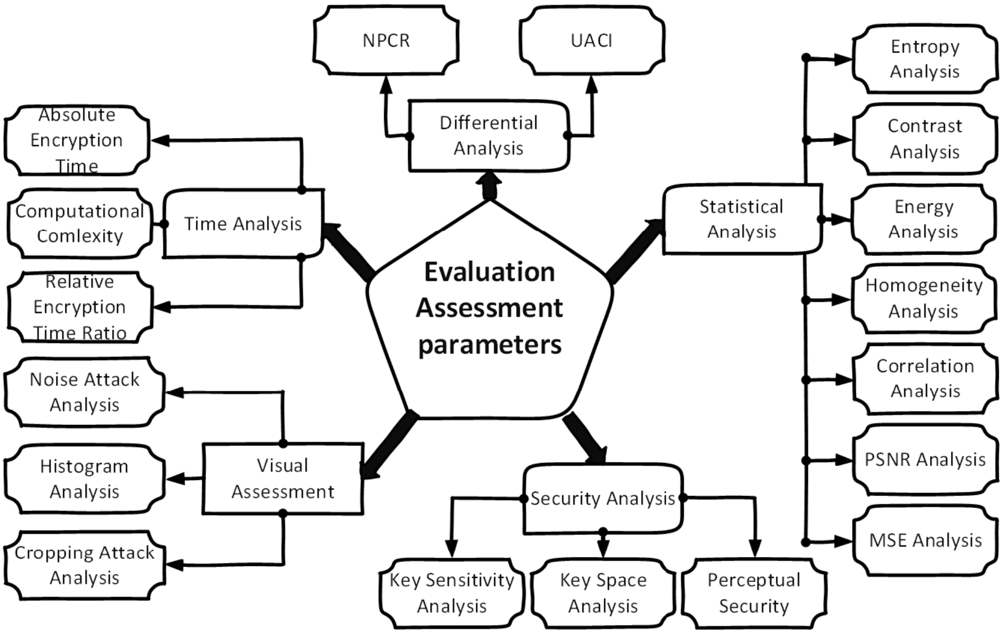

FIGURE 4. Evaluation parameters to gauge the performance of the cryptographic algorithms.

III. HYBRID QUANTUM ENCRYPTION

This section explores existing hybrid quantum encryption techniques, which are the cutting-edge fusion of classical and quantum cryptography. Addressing the growing demand for secure communication, current methodologies are examined to show how hybrid quantum techniques enhance security for digital data. In [63], Abdullah et al. proposed a methodology to share cryptographic secret keys between two parties that employs quantum key distribution (QKD) [64]. Additionally, the authors integrated QKD with public key cryptography [65]. Vulnerabilities in their research include potential weaknesses in the quantum channel and being highly dependent on traditional computational security. Moreover, susceptibility to attacks on the hardware of the QKD system and the implementation process entail significant risks.

In [66], proposed a hybrid quantum-classical method for the classification of digital images by utilizing a variational quantum circuit (VQC) [67] and addressing qubit limitations through multiple amplitude encoding mechanisms. Various operations, such as convolutions [68] and optimized single-qubit rotations, are incorporated to process the digital images. Their cryptographic approach was assessed on multiple datasets, showcasing improved efficiency in quantum cost compared to existing quantum encryption schemes. However, a few vulnerabilities that need to be addressed include the low robustness of VQCs with complex image datasets. Moreover, the fusion of quantum computing and quantum-classical methods might pose challenges when developing a cryptosystem suitable for real-time applications where low computational time is required.

In [69], Song et al. devised a quantum image encryption scheme using restricted geometric and color transformations [70], enhancing security with sensitive chaotic map-generated keys. However, vulnerabilities might arise due to chaotic map predictability, risking security breaches, and reliance on probabilistic models in the measurement step could introduce biases affecting scheme security.

In [71], Hao et al. devised an image encryption system utilizing quantum principles, employing a quantum-based PRNG [72] and NEQR model [73] for encryption. However, potential vulnerabilities lie in the PRNG's quantum entanglement basis, risking the security of the generated code stream, and potential threats targeting quantum algorithms might pose a security risk despite their high performance in experiments. A summary of the existing cryptographic technologies that incorporate hybrid quantum encryption is given in Table 3.

IV. QUANTUM IMAGE WATERMARKING

This section explores quantum image watermarking schemes specifically focused on enhancing their robustness in terms of security. Furthermore, the vulnerabilities in the existing schemes are also highlighted. In [74], Miyake et al. proposed a watermarking technique to secure digital images. The scheme utilizes compact quantum circuits [75] and NEQR representations. Moreover, the method involves controlled SWAP gates and CNOT gates [76] to integrate and extract watermarks, demonstrating robustness in experimental results and analysis. However, the vulnerabilities in the scheme are related to key-dependent operations if the keys are compromised.

In [77], Iranmanesh et al. presented a quantum transmitter and receiver circuit for a Quantum Image Watermarking (QIW) scheme that utilizes the NEQR quantum image

TABLE 1. Summary of the evaluation metrics.

Metrics	Short definitions	Mathematical equations	Variable description	Relationship with robustness
Entropy	Entropy is used to measure the randomness in any message	$Ent = -\sum p(k_i) log_2 p(k_i)$	k_i: probability occurrence in the variable i Ent: Entropy	Robustness $\propto$ Entropy
Correlation	Correlation is used to measure the similarity between the image pixels	CorrCoff = $\frac{Cov(w,t)}{\sigma_w \sigma_t}$ σ_w = $\sqrt{VAR_w}$ σ_t = $\sqrt{VAR_t}$ VAR (n) = $\frac{1}{R} \sum_{u=1}^{R}$(n$_s$ - E(n))^2 Cov(n, m)= $\frac{1}{R} \sum_{u=1}^{R}$(n$_s$ - E(n) (h$_s$ - E(m)	E: Expected value operator, σ: Standard deviation	Robustness $\propto$ $\frac{1}{\text{Correlation}}$
Contrast	It is used to identify the objects in an image	Contrast = $\sum_{q,r=0} \lvert q-r \rvert^2 \gamma(q-r)$	q and r are the 8-bit gray level images, $\gamma(q-r)$ is the gray level occurrence matrix	Robustness $\propto$ Contrast
Energy	It is used to quantify the information present n an image	$Entropy = \sum I(g,m)^2$	$I(g,m)$: plaintext image	Robustness $\propto$ $\frac{1}{En}$
Homogeneity	It is used to analyze the uniformity in image pixels	$Hom = \sum_x \sum_y \frac{p(x,y)}{1+\lvert x\breve{} y \rvert}$	x: Rows y: Columns $P(x,y)$: Plaintext image	Robustness $\propto$ $\frac{1}{H}$
MSE	It is used to measure the difference between two images	$MSE = \frac{1}{LM} \sum_{w=0}^{L-1} \sum_{t=0}^{M-1} (O(w,t) - X(w,t))^2$	$O(w,t)$: Original image, $X(w,t)$: Ciphertext image	Robustness $\propto$ MSE
PSNR	It is used to measure the similarity between two images	$PSNR = 10 \times log_2 \frac{P_{max}^2}{MSE}$	P_{max}: Maximum pixel value in an image	Robustness $\propto$ $\frac{1}{PSNR}$

TABLE 2. Comparison with the existing survey..

Categories	**Sub-Categories**	**Sajitha et al. [59]**	**Harran et al. [60]**	**Ramanathan et al. [61]**	**Salman et al. [62]**	**Proposed survey**
Hybrid Quantum Encryption						✓
Quantum Image Watermarking						✓
Quantum Random Number Generation						✓
Quantum Stegnography	Quantum Secure Image Transmission		✓	✓	✓	✓
Adversal Neural Networks (ANN)	ANN with Chaos	✓	✓	✓		✓
Chaotic Neural Networks		✓	✓	✓		✓
Deep Learning Based Cryyptography	Deep Hashing			✓		✓
Machine Learning Based Cryptography				✓	✓	✓

representation. Their scheme integrated IBM's quantum operations and the MCNOT-R quantum gate. The experimental results and simulations reveal satisfactory visual quality. However, the implementation of the MCNOT-R gate could

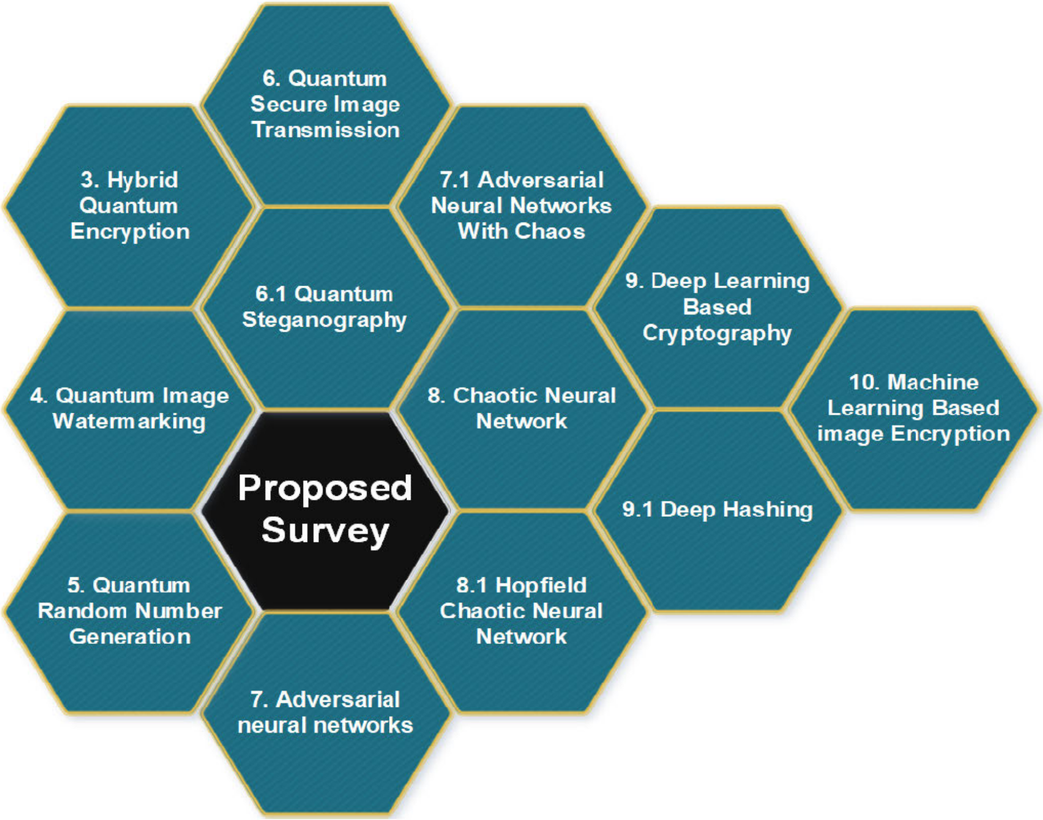
6. Quantum Secure Image Transmission
3. Hybrid Quantum Encryption
7.1 Adversarial Neural Networks With Chaos
6.1 Quantum Steganography
9. Deep Learning Based Cryptography
4. Quantum Image Watermarking
8. Chaotic Neural Network
10. Machine Learning Based image Encryption
Proposed Survey
9.1 Deep Hashing
5. Quantum Random Number Generation
8.1 Hopfield Chaotic Neural Network
7. Adversarial neural networks

FIGURE 5. Topics covered in the proposed survey.

TABLE 3. Summary of existing techniques based on hybrid quantum encryption techniques.

Methodology Name	**Application Domain**	**Real-World Performance**	**Robustness Against Attacks**	**Disadvantages**	**Potential Solutions**
Method ology	**Application domain**	**Real-world performance**	**Robustness against attacks**	**Disadvantages**	**Potential solutions**
Abdullah et al. [63]	Cryptographic Key Sharing	Dependent on QKD	Vulnerabilities in the Quantum Channel	Susceptibility to Attack in QKD Hardware	Continuous Monitoring, Improvement of QKD Systems
Bar et al. [66]	Digital Image Classification	Enhanced Efficiency in Quantum Cost for Encryption Schemes	Low Robustness of VQCs with Complex Datasets	Fusion of Quantum Computing and Quantum Classical Method Challenges	Research on Improving VQC Robustness and Optimizing Quantum Classical Fusion
Song et al. [69]	Quantum Image Encryption	Security Enhancement With Chaotic Map Generated Keys	Chaotic map Predictability and Reliance on Probabilistic Model	Potential Security Breaches	Research on Improving Chaotic MAp Unpredictability and Exploring Alternative Models
Hao et al. [71]	Image Encryption	High Performance in Experiments Using Quantum Principles	Vulnerabilities in the Quantum Entangment Basis of PRNG	Potential Threats Targeting Quantum Algorithms	Exploration of Alternative PRNG Designs

compromise the security of their proposed watermarking scheme. Moreover, this scheme is also susceptible to adversarial attacks because of weak and time-consuming quantum operations.

In [78], Hu et al. explored a quantum watermarking technique that incorporates NEQR for binary images and 3-D color images. Gray code transformation [79] and least significant bits (LSB) steganography are also used in the edge region of a color carrier image using LSBs. Their scheme might face vulnerabilities due to the susceptibility of gray code transformation and LSB embedding techniques, which are ultimately weak against differential attacks.

In [80], Wang et al. presented a watermarking scheme by merging image self-recovery with quantum watermarking. Their approach emphasizes tamper localization and self-recovery in quantum images by using 2 × 2 non-overlapping image pixels blocks for the generation of watermarks, tamper detection, and recovery [81]. However, an attacker or an unauthenticated user might launch an attack to break the security of the system, which could make it difficult for the receiver to recover the original message and fix any damage. Also, this system depends on a specific size, which makes it less able to handle complicated attacks.

In [82], Jiang et al. proposed a quantum watermarking scheme that combines Hilbert scrambling and Moiré fringe steganography. The high reliance on Moiré fringe steganography can make it easy for attackers to decrypt.

In [83], Hai et al. proposed a quantum image watermarking method that combines LSB-based watermarking with NEQR to enhance security via block-based scrambling. However, the LSB-based embedding scheme has proven vulnerable to cyberattacks. Moreover, the emphasis on higher PSNR might limit resilience against quantum attacks due to non-complex operations.

In [84], Zhou et al. proposed a two-bit superposition method for image watermarking that also incorporates encryption steps such as bit-plane encryption and Fibonacci scramble. Such encryption schemes pose risks to the security of the watermark. Moreover, the performance evaluation of their scheme PSNR and image histogram analysis lacks verification against quantum attacks that make them vulnerable in real-time applications.

In [85], Zhou et al. proposed a watermarking scheme to secure 3-D color quantum images. The scheme incorporates the INCQI model and employs a few preprocessing steps, such as color space conversion [86], noise reduction [87], and contrast enhancement [88], before embedding the plaintext image. However, employing basic pre-processing techniques can create vulnerabilities in terms of weak security. The scheme showed improved visual quality, but the resilience of their scheme against advanced quantum attacks such as QKD attacks, post-quantum cryptography (PQC) attacks, and quantum side-channel (QSC) attacks remains unverified, leading to weaknesses in real-time scenarios.

In [89], Ghai et al. introduced a quantum-based image watermarking scheme that incorporates complex steps for embedding such as frequency domain transformation [90], selective embedding in regions of interest (ROIs) [91], and dynamic embedding schemes [92]. However, dependency on quantum techniques poses vulnerabilities, and the use of singular value decomposition (SVD) in embedding can be susceptible to cyberattacks.

In [93], Hu et al. proposed an image watermarking scheme technique that utilizes the flexible representation of quantum images. Operating through a $2^{n1} \times 2^{n1}$ to $2^n \times 2^n$ ratio, they applied a quantum Haar wavelet transform [94]. While simulation results show strong performance in maintaining image similarity, the robustness of the scheme for invertible quantum operations may pose vulnerabilities if the quantum processes are compromised. Table 4 summarized the cryptographic schemes that are based on quantum image watermarking.

V. QUANTUM RANDOM NUMBER GENERATION

In [95], Kuang et al. introduced a pQRNG using the quantum permutation pad (QPP), exploiting the quantum permutation space for high entropy. However, potential vulnerabilities might arise from errors in the QPP algorithm, impacting the reliability of generated numbers. Over time, as with most PRNGs, there's a theoretical risk of predictability emerging, potentially compromising its unpredictability.

In [96], Akhshani et al. introduced a PRNG based on the quantum logistic map, showing strong pseudorandom number generation. The method boasts fast computation using equations from the quantum chaotic map and has passed rigorous tests such as NIST, DIEHARD, and TestU01 [97], [98], proving its reliability. However, potential vulnerabilities in the underlying equations and untested resilience against advanced statistical analyses or quantum attacks pose concerns.

In [99], Iavich et al. explored quantum mechanics for generating genuinely random numbers, crucial for modern cryptographic protocols. The authors discussed the certification methods for evaluating device performance and delve into self-testing and device-independent quantum random number generation, proposing a semi-self-testing certification method that enhances randomness security and speed compared to self-testing. Their scheme uses only quantum mechanics, which can make it vulnerable to differential attacks. Moreover, it can also reduce the accuracy of detecting irregularities when a large dataset is used as input.

In [100], Avesani et al. developed a source-device-independent scheme that is based on positive operator value measurements (POVM) [101], with a major focus on heterodyne measurements. The scheme provided a secure generation rate of 17.42 Gbit/s without needing initial randomness. The robustness of the scheme against several cyberattacks in a finite-key scenario is validated. However, the heterodyne measurements and parameters are not optimized in the scheme, making it suspectable and challenging for security assurances over time.

In [102], Sanguinetti et al. analyzed QRNGs and their potential for strengthening cryptographic security by offering highly random keys. The authors noted current QRNG limitations in terms of cost, size, and power, causing widespread adoption. Highlighting progress in making mobile cameras better, especially in capturing very low light, they used such improved cameras to create random numbers that are based

TABLE 4. Summary of existing techniques based on quantum image watermarking schemes.

Methodology Name	Application Domain	Real-World Performance	Robustness Against Attacks	Disadvantages	Potential Solutions
Miyake et al. [74]	Digital Image Watermarking	Robust Experimental Results	Key-Dependent Vulnerability	Compromised Keys	Improved Key Management
Iranmanesh et al. [77]	Quantum Image Watermarking	Satisfactory Visual Quality	MCNOT-R Gate Vulnerability	Weak Against Adversarial Attacks	Strengthen Quantum Operations
Hu et al. [78]	Quantum Watermarking for Images	NEQR, Gray Code Vulnerability	Gray Code, LSB Susceptibility	Differential Attack Vulnerability	Improved Transformation
Wang et al. [80]	Quantum Image Self Recovery	Tamper Localization, Self Recovery	Security Breach Risk	System Dependence on Size	Enhanced Tamper Detection
Jiang et al. [82]	Quantum Watermarking with Fringe	High Reliance on Moiré Fringe	Increased Vulnerability	Reliance on Fringe Steganography	Explore Alternative Techniques
Hai et al. [83]	Quantum Image Watermarking	NEQR, Higher PSNR Vulnerability	Cyberattacks, Limited Resilience	Cyberattacks PSNR Emphasis Limitation	Enhanced Cybersecurity
Zhou et al. [84]	Superposition Method for Watermarking	Encryption Scheme Risks	Lack of Verification	Encryption Scheme Risks	Verification required
Zhou et al. [85]	Color Image Quantum Watermarking	Preprocessing Risks	Unverified Resilience	Unverified Resilience	Improved Steps
Ghai et al. [89]	Quantum-Based Image Watermarking	Complex Embedding Steps	Quantum Techniques Dependency	Quantum Techniques Dependency, SVD Vulnerability	Dependency Reduction, Improved SVD
Hu et al. [93]	Quantum Image Watermarking	Quantum Haar Wavelet, Similarity	Invertible Operations Risk	Invertible Operations Vulnerability	Improved Operations, Security

on quantum principles. Depending on devices such as mobile cameras can make the system vulnerable due to its lower sensitivity and can also be influenced by external factors, which could ultimately impact how random and reliable the generated numbers are.

In [103], Truong et al. performed a machine learning (ML) analysis to evaluate the impact of deterministic classical noise on an optical continuous variable QRNG. The ML model successfully detected correlations in the data points and demonstrated the resilience of the QRNG after removing and filtering any randomness from the entire data set. Their scheme has shown the robustness of ML approaches by gauging the randomness of the generated numbers from both the QRNG and a congruential RNG (CRNG) [104]. The limitations of ML include adapting to unforeseen noise patterns and different RNG systems because it relies on predefined parameters. Furthermore, encountering new noise types not accounted for in the training data can compromise the effectiveness of the ML approach in terms of evaluating RNG quality.

In [105], Iavich et al. proposed a mathematical model for a fast and cost-effective random number generator that emphasizes its reliance on quantum mechanics for randomness and unpredictability. The authors proposed a semi-self-testing certification method for QRNG that depends on photon arrival time (PAT) [106]. The only dependency on PAT can affect precision, thus impacting randomness. The effectiveness of the method in countering all QRNG vulnerabilities remains a research gap for ensuring robust security. The cryptographic schemes derived from quantum random number generation are summarized in Table 5.

VI. QUANTUM SECURE IMAGE TRANSMISSION

In this section, we delve into quantum random number generation to secure digital data. With an increasing need for random numbers for the security of the digital, several researchers have proposed different techniques to generate random numbers using the concept of quantum theory. In [107], Anitha et al. proposed the Quantum Chaos-based Network-centric Encryption for Data Transmission (Q-CNEST) protocol for secure transmission of digital data. The encryption process involves the creation of secret keys through quantum chaotic logistic maps, which are based on random network parameters [108], [109]. After that, pixel diffusion and permutation are performed between the image pixels using the generated random cipher keys. Experimental results and analysis have shown that Q-CNEST,

TABLE 5. Summary of existing techniques based on quantum Random Number Generation.

Methodology Name	Application Domain	Real-World Performance	Robustness Against Attacks	Disadvantages	Potential Solutions
Kuang et al. [95]	Pseudo-RNG	High entropy	QPP algorithm errors	QPP improvements	Periodic updates
Akhshani et al. [96]	Quantum Logistic Map	Strong generation	Equation vulnerabilities	Rigorous testing	Improved equations
Iavich et al. [99]	Device-Independent	Enhanced speed	Differential attacks	Hybrid approaches	Improved certification
Avesani et al. [100]	Source-Device-Independent	17.42 Gbit/s rate	Robust against cyber-attacks	Non-optimized measurements	Measurement optimization
Sanguinetti et al. [102]	Mobile Camera-based	Improved randomness	Device limitations	Enhanced sensitivity	External factor compensation
Truong et al. [103]	ML Analysis on Optical QRNG	Resilience demonstrated	Limited noise adaptation	Adaptive ML models	Continuous noise analysis
Iavich et al. [105]	Hybrid QRNG	Quantum emphasis	PAT dependency	Diversified sources	Precision management

which utilizes network characteristics as initial conditions, can generate highly complex encrypted data. Moreover, Qiskit packages demonstrated the robust randomness of the encryption scheme, which makes it effective against conventional and differential attacks and allows the secure transmission of medical data. However, the vulnerability of the scheme and its untested resilience against sophisticated cryptographic attacks remain areas of concern.

In [110], Guo et al. proposed a Feistel-based quantum image encryption based on encryption quantum circuits. The authors proposed a modified Feistel structure, continuing a 128-bit block cipher that merges Feistel and substitution-permutation networks [111], [112]. The quantum circuit designs were validated through simulations and experimental results, which showed their resistance against statistical attacks. However, quantum encryption circuits can be vulnerable to future quantum computing.

In [113], Liu et al. proposed a three-level quantum image encryption (3QIE) scheme using the Arnold transform and logistic map, which incorporates block-level permutation [114], bit-level permutation [115], and pixel-level diffusion [116] for robust encryption. The 3QIE employs an enhanced version of the quantum representation model for the conversion of classical images into quantum form using the quantum Arnold transform (QArT) [117]. The encryption process also includes iterative block-level permutations and bit-level rearrangements based on a logistic map-generated sequence [118]. In recent years, the Arnold transform and logistic map have shown non-robust encryption results. Therefore, the 3QIE might be attacked by cipher-text-only or cipher-text-chosen attacks.

In [119], Janani et al. investigated the efficiency of quantum image encryption in telemedicine applications. The investigation process involves quantum block-based spatial transformations [120]. Their proposed cryptosystem aimed to enhance the security of medical images with multiple protection levels and layers [121], [122]. Using plain image-derived seed values and quantum block-based scrambling strengthened the security of the medical data. The system ensured image integrity via dedicated quantum encryption by concealing only the region of interest (ROI) of the plaintext data. Simulations on the Cancer Imaging Archive dataset [123]validated the efficiency in terms of security of the proposed multiple-level and layer-based encryption, ultimately fortifying medical image confidentiality in telemedicine applications. Reliance on plain image-derived seeds that are untested against differential attacks compromises its security.

In [124], Qu et al. proposed a new protocol for secure healthcare information transmission. The protocol employs three layers to implement pixel embedding and encryption simultaneously. The encrypted data are transmitted through a quantum channel as a quantum state that shows high security [125]. This protocol also serves as a quantum image steganography method that enhances security and prevents various cyberattacks during information transmission. The embedding of secret information within quantum states can pose a vulnerability to quantum computing [126].

In [127], Wen et al. proposed a new image encryption scheme that combined a quantum chaotic map with security-enhanced mechanisms to improve security. The system incorporated a plaintext correlation system and a diffusion-permutation-diffusion network that is validated on a secure communication platform to demonstrate its robustness against cryptographic attacks. The reliance on the quantum chaotic map exposes vulnerabilities if patterns in these sequences are exploited, and therefore the resilience of the system against more advanced attacks beyond the analyzed parameters remains unverified.

In [128], Peng et al. proposed a secure data transmission scheme that combines image compression [129], encryption, image fingerprinting [130], and digital image watermarking [131]. Their scheme enhanced transmission efficiency, security, and authenticity in telemedicine applications. The high reliance on perceptual hash algorithms makes them prone to attacks targeting hash functions that undermine image authenticity.

A. QUANTUM STEGANOGRAPHY

Quantum secure image transmission refers to the use of the principles of quantum communication to ensure the secure and confidential transmission of digital images. In recent years, quantum computing has been frequently used for the secure transmission of information. In [132], Jiang et al. proposed a two-blind LSB steganography algorithm based on quantum circuits for quantum images. The plain LSB and block LSB methods involve substituting LSB directly and embedding message bits in image blocks, respectively. Experimental results showed strong invisibility and adaptable capacity that make the encryption scheme strong against advanced cyberattacks, and targeting LSB manipulation or block embedding can also enhance the robustness of the encrypted message.

In [133], Yang et al. investigated a quantum hash function that is derived from modified quantum walks and enhances security and privacy amplification in quantum key distribution. The authors also highlighted the ability of the proposed scheme for the generation of pseudo-random numbers due to the inherent chaotic dynamics [134], [135]. After that, utilizing the quantum hash function, an image encryption scheme is proposed for the secure transmission of digital data. The encryption scheme is validated through simulations and tests, which showed its adaptability across several security tests, but it can be vulnerable in terms of modified quantum walks. Moreover, the unverified resilience against cyberattacks raises concerns about its effectiveness and robustness in highly sophisticated attack scenarios.

In [136], Qu et al. proposed the controlled flexible representation for quantum image Steganography (CFRQIES), which offers enhanced control over information transmission security. Their secure, controlled quantum image steganography algorithm utilizes the controlled access mechanism of CFRQI to enhance imperceptibility and security. The proposed algorithm is not strong enough to defend itself against advanced quantum attacks.

In [137], Qu et al. proposed a QIS-IEMD quantum image steganography protocol with an enhanced Exploiting Modification Direction (EMD) algorithm [138]. Expands modification ranges that employ dynamic subgroup sharing and embeds information across multiple-bit planes, demonstrating its practicality through dedicated quantum circuits. The experimental results and the analysis showed the superior imperceptibility of QIS-IEMD and its efficiency rate. The vulnerabilities in the expanded modification ranges and dynamic subgroup sharing of the QIS-IEMD protocol can compromise embedded information security.

In [139], Zhou et al. introduced a quantum image steganography method using NEQR and LSB, assuming specific image sizes and employing scrambling techniques controlled by operator keys for embedding and extraction. Their validation involved evaluating PSNR, capacity, security, and circuit complexity [140], [141]. However, the vulnerability lies in the scheme's reliance on operator-controlled keys, potentially leading to compromise, while the reliance on scrambling techniques could be undermined by evolving decryption methods.

In [142], Jiang et al. proposed a quantum image steganography scheme using Moiré patterns by embedding and extracting images securely without keys. Their steganography scheme relied on NEQR and recursive quantum circuits, which were evaluated using experimental analysis for effectiveness. The keyless nature poses vulnerability to unauthorized access, and the reliance on Moiré patterns is susceptible to evolving decryption methods that compromise long-term robustness.

In [143], Qu et al. proposed a quantum image steganography algorithm using the EMD technique, in which $(2N + 1)$ modifications are made within the groups of carriers of pixels to represent secret digits. In their proposed encryption scheme, a quantum circuit for EMD is incorporated to show robust performance in MATLAB simulations across various security metrics. Several vulnerabilities related to security and computational time complexity can arise from the $(2N + 1)$ notation system. Furthermore, its real-world resilience against advanced decryption methods remains unverified. This shows the challenging nature of the proposed scheme in terms of robustness outside controlled settings.

In [144], Sharma et al. proposed an image steganography scheme that uses graph signal processing. Their proposed technique involved quantum scrambling to create a scrambled image, followed by graph wavelet transformations [145] and α blending of signals from the cover and encrypted images. The method demonstrated exceptional visual quality for both the stego and extracted encrypted images because of the improved interpixel correlation. The vulnerabilities lie in the highly reliance on quantum scrambling of the technique against advanced structural analysis methods that impact the overall security and recovery of the encrypted and hidden information.

In [146], Atty et al. proposed a quantum image steganography method in which Hadamard transformation and NEQR are used to embed quantum text messages into quantum images. This allows the message to be recovered only from the stego image. Their proposed approach filled a prior gap in quantum image steganography. The results of the simulation highlighted its strong capacity, invisibility, and security. Potential vulnerabilities as weaknesses are found in Hadamard transformation and NEQR [147] that compromise the security of the embedded quantum text. In addition, real-world testing against advanced quantum decryption techniques is crucial to assess its practical resilience.

In [148], Hu et al. proposed a quantum steganography scheme in which binary images are embedded into a color carrier image using a modified exploiting modification direction algorithm. The security of the stego image is enhanced by generating a secret key through an exclusive OR (XOR) operation on two secret images. Detailed quantum circuit analysis and MATLAB simulations showed the strong imperceptibility and security of the algorithm. The utilization of XOR operations in the generation of secret keys can comprise security. The real-time applications and performance of the algorithm against advanced quantum decryption techniques pose challenges for uncontrolled environments. Table 6 provides a summary of cryptographic schemes based on quantum encryption and quantum stegnography.

VII. ADVERSARIAL NEURAL NETWORKS IN IMAGE ENCRYPTION

Adversarial neural networks in image encryption use generative adversarial networks (GANs) to create enciphered images [149], [150], [151]. The generator network produces encrypted images, while the discriminator network learns to differentiate between enciphered and plaintext images. In [152], Maung et al. presented an image encryption scheme using adversarial defense to draw inspiration from traditional perceptual encryption schemes. Their method employs block-wise pixel shuffling with a secret key for both training and test images. Evaluation against various attacks showed its effectiveness in terms of high accuracy. having superior performance against existing defenses, the reliance on pixel shuffling with a secret key creates the vulnerability. Also, its resilience against a broader range of evolving attacks requires further verification.

In [153], Meraouche et al. proposed a multi-agent adversarial neural network model for securing communication between Alice and Bob against cyber-attacks. Unlike existing methods such as [154], [155], [156], and [157] that require shared symmetric information, this model allows Alice and Bob to train themselves using asymmetric information. The five-agent setup includes Alice, Bob, Eve (the eavesdropper), and neural networks generating public and private keys from secret random noise provided by Bob. This key generation process allows encryption by Alice using the public key and decryption by Bob with the private key, which prevents Eve from recovering the message with the public key. The model faces vulnerabilities in potential adversarial attacks on key generation that compromise message integrity.

In [158], Li et al. proposed the Adversarial Network Encryption System (ANES) by incorporating adversarial networks with senders, receivers, and various attackers. The authors devised three ANES variations that simulate various password attacks that employ a general loss function. ANES autonomously learned one-time-pad (OTP) algorithms through one-to-one adversarial training, showing higher proficiency against robust opponents and showcasing potential even when subjected to Chosen Ciphertext Attacks. The ANES can struggle to adapt to evolving attacks, potentially limiting its effectiveness against emerging threats. Furthermore, its reliance on adversarial training renders it vulnerable to adversarial examples or perturbations.

In [159], Coutinho et al. analyzed the security of cryptographic algorithms that are generated via adversarial neural cryptography (ANC). The authors used an artificial neural network (ANN) [160] to train an advanced security system known as the ANC model, which is how to independently learn the OTP algorithm. This algorithm is extremely secure for communication. The AI agents demonstrated the capability to secure messages automatically without the need for human involvement. The reliance of ANC on neural networks exposes it to potential adversarial attacks targeting the learning process, which poses a threat to its cryptographic algorithm generation. Furthermore, with evolving AI capabilities, ANC could face increased susceptibility to advances in AI-generated attacks.

A. ADVERSARIAL NEURAL NETWORKS WITH CHAOS

In [161], Fang et al. highlighted a few flaws, such as instability of the chaotic system [162] and limited key space [163] in existing image encryption schemes that employ chaotic systems. To overcome such challenges, the authors proposed a new block-based encryption scheme. In their encryption process, an enhanced version of the hyperchaotic system [164] and the secret keys having a large key space are integrated with neural networks, GANs, and an improved Feistel structure to encrypt images at a pixel level to enhance the security and efficiency of the encrypted images. There are a few initial and control parameters used in the hyperchaotic system, which makes the encryption scheme vulnerable to brute-force attacks.

In [165], Fang et al. proposed another block-based image encryption scheme that uses deep convolutional generative adversarial networks (DCGANs), quaternions, an improved Feistel network [166], and a comprehensive scrambling-diffusion process. Their proposed encryption scheme involved creating a new hyperchaotic system that is integrated with DCGANs to generate a complex key stream. This stream is combined with quaternions and an enhanced Feistel network, which encrypts color plaintext images via a key block matrix. The security of the encryption algorithm is assessed in terms of quantitative and qualitative analysis. Again, the hyperchaotic make their proposed encryption systems vulnerable to brute-force attacks due to a small number of initial and control parameters, which is also a source of small key space.

In [167], Man et al. used Least Squares Generative Adversarial Networks (LSGAN) to create a robust random number generator that is trained with six diverse chaotic systems. Their method successfully passes NIST randomness tests for encryption keys. However, LSGAN's susceptibility to adversarial attacks.

In [168], Wu et al. merged ANC with SHA-256 [169], which controls the chaotic systems, to strengthen the image encryption scheme against known-plaintext and chosen-plaintext attacks. The authors used a GAN to create an intermediate image and then XOR it based on a logistic map for the final ciphertext. It also leverages the non-linearity of the neural network to improve resilience. However, there may be weaknesses related to ANC if it has vulnerabilities or if smart attackers use advanced techniques to understand the complex workings of the neural network.

TABLE 6. Summary of existing techniques based on quantum encryption and quantum stegnography.

Methodology Name	Application Domain	Real-World Performance	Robustness Against Attacks	Disadvantages	Potential Solutions
Anitha et al. [107]	Network-Centric	Complex Data	Resistance to Attacks	Untested Resilience	Cryptographic Testing, Updates
Guo et al. [110]	Feistel-Based	Statistical Resistance	Quantum Vulnerability		Quantum-Resistant Algorithms
Liu et al. [113]	Three-Level Encryption	Robust Block, Bit, Pixel	Potential Cipher Attacks		Enhanced Techniques, Security Protocols
Janani et al. [119]	Telemedicine Encryption	Multiple Layers	Reliance on Seeds	Untested	Improved Seed Generation, Testing
Qu et al. [124]	Secure Healthcare Transmission	Three-Layer Encryption	Quantum Vulnerability		Quantum-Resistant Techniques
Wen et al. [127]	Chaotic Map Encryption	Cryptographic Robustness	Chaotic Map Vulnerabilities	small key space	Pattern Obfuscation, Advanced Testing
Peng et al. [128]	Secure Data Transmission	Enhanced Efficiency	Hash Function Vulnerability	Weak hashing	Improved Hash Algorithms, Security
Jiang et al. [132]	Quantum LSB Steganography	Advanced Cyberattacks	LSB Manipulation	Block Embedding	Enhanced Encryption Techniques
Yang et al. [133]	Quantum Hash Function	Security Amplification	Vulnerability to Modified Quantum Walks	Unverified Resilience	Testing, Parameter Adjustments
Qu et al. [136]	CFRQIE for Quantum Image Steganography	Controlled Access Security	Vulnerability to Advanced Quantum Attacks	-	Quantum-Resistant Techniques
Qu et al. [137]	QIS-IEMD Quantum Steganography	Superior Imperceptibility, Efficiency	Vulnerabilities in Modification Ranges	-	Improved Security Protocols
Zhou et al. [139]	NEQR and LSB Steganography	PSNR, Capacity, Security	Operator-Controlled Keys	-	Evolving Key Management
Jiang et al. [142]	Moiré Pattern Steganography	Keyless Image Embedding	Vulnerability to Evolving Decryption Methods	-	Key Management, Algorithm Updates
Qu et al. [143]	EMD-Based Quantum Steganography	Robust Performance, Security Metrics	Security and Computational Complexity	(2N + 1) Notation System	Testing, Complexity Reduction
Sharma et al. [144]	Graph Signal Processing Steganography	Visual Quality, Improved Correlation	Quantum Scrambling Vulnerability	-	Improved Quantum Scrambling
Atty et al. [146]	Hadamard Transformation Steganography	Capacity, Invisibility, Security	Hadamard Transformation, NEQR Weaknesses	-	Algorithm Updates, Security Testing
Hu et al. [148]	Quantum Steganography XOR Algorithm	Imperceptibility, Security	XOR Operation Vulnerability	-	Improved XOR Operation, Real-world Testing

In [170], Alsafyani et al. proposed an advanced face feature encryption method that combines image optimization, cryptography, and deep learning. Their approach integrates an optical chaotic map to bolster key security within a 5D conservative chaotic method. Using ML-based concealment of data with a hidden factor and secure Crypto GANs and a chaotic optical map, the encryption and decryption of facial images are controlled. However, a weak optical chaotic map, or the Crypto GANs, makes the system vulnerable to cyberattacks. Additionally, while aiming to maintain privacy, adversarial methods may target the decryption process or the ML-based data concealment, which can be risky in terms of the security of the encrypted facial images.

In [115], Li et al. proposed a steganography method that embeds encrypted images within plaintext cover images using chaos encryption and CNN transformations. Employing GANs enhances the concealment by creating stego images that resemble the cover image. Adversarial methods might also target the weight allocation mechanism, which affects network efficacy and compromises concealed information secrecy.

In [171], Hao et al. developed a blockchain-based information sharing protocol for zero-trust environments that is specifically capable of filtering fabricated data and securing participant privacy. Potential privacy issues may arise if the security measures of the protocol are not sufficiently robust.

Table 7 encapsulates an overview of cryptographic schemes with a foundation in adversarial neural networks.

VIII. CHAOTIC NEURAL NETWORK

A chaotic neural network integrates the principles of chaos theory to secure digital data. This incorporation of chaotic dynamics enhances the ability of a network to handle complex and large amounts of data and improves its robustness in terms of security. In [172], Bigdeli et al. proposed an image encryption/decryption algorithm based on a chaotic convolutional neural network (CCNN) with two layers, such as a chaotic neuron (CN) [173] and a permutation neuron (PN) [174]. While the method aims for robustness through iteration, vulnerabilities arise in the weaknesses of the CNN design. Moreover, sophisticated cryptanalysis could also exploit the patterns of the plaintext images in a few iterations.

In [175], Chauhan et al. proposed an image encryption scheme that utilizes a CCNN and depends on unpredictable chaotic systems to determine neural network weights. Vulnerabilities in this approach arise in the design of the network and the chaotic sequences that are generated for weight determination.

In [176], Maddodi et al. combined neural networks and chaos for the secure transmission of digital images. By employing a CCNN for encryption and dynamic parameter updates, the system provides robust security for digital data. However, there are challenges and weaknesses in the dynamic parameters of the chaotic neural network.

In [177], Wang et al. proposed an image encryption technique that is based on complex and time-delayed neural networks. Their proposed scheme has a large key space with a multicable hyperchaotic system. There are a few vulnerabilities in the complex network that cause decryption failure and affect the retrieval of the original image data.

In [178], Chen et al. proposed a color image encryption technique that integrates DNA encoding [179], [180] and chaos to enhance the security of digital data. Further, the authors utilized a fractional-order discrete Hopfield neural network (FODHNN) [181] for the generation of random sequences based on chaos. Employing DNA encoding and diffusion techniques, along with confusion and diffusion operations, can further strengthen the security of the encrypted data.

A. HOPFIELD CHAOTIC NN

In [182], Chen et al. proposed a three-dimensional neural network and investigated its dynamic behavior with the aim of focusing specifically on synchronization. They used the synchronized network to secure the digital grayscale images. As the synchronized network is specifically used for distributed systems in recent years [183], [184], [185], [186], it might not be fit to provide robust security to the digital images, and it can also impact the encryption accuracy.

In [187], Wang et al. proposed a chaos-based color image encryption scheme in which multiple chaotic maps and a Hopfield chaotic neural network are incorporated. The chaotic maps used in their proposed scheme have only two control parameters and three initial conditions, which are not enough to provide a large key space. A small key space can make the encryption scheme vulnerable to brute force attacks [56].

In [188], Hu et al. investigated an existing color image encryption algorithm [189]. The authors used a Hopfield chaotic neural network (HCNN) to find permutation and diffusion keys for cryptanalysis. The weaknesses related to a chosen plaintext attack make decryption easy for attackers from the original data. This security challenge compromises the integrity of the encryption scheme.

In [190], Liu et al. proposed a color image encryption scheme that is based on diffusion and scrambling operations. After incorporating the first-level diffusion, a second diffusion matrix is also derived from a HCNN. The aim of their proposed encryption scheme is to prevent chosen-plaintext attacks and enhance key sensitivity. Additionally, secondary scrambling steps target specific pixels for enhanced security. The possible vulnerabilities in this encryption method can be the weaknesses of the second diffusion process driven by the HCNN and the secondary scrambling step.

In [191], Sha et al. employed fractional-order Hopfield neural networks (FO-HNN) and a three-input logic valve-based diffusion technique in cryptography for enhanced image security. In [192], Wu et al. proposed a color image encryption scheme to secure grayscale images. A distinct five-dimensional hyperchaotic system [193] with the HCNN is integrated into their encryption algorithm. This approach utilized image chunking [194] for key generation and pseudo-random sequences from these systems as key streams, which is a source for enabling pixel-level scrambling and the dynamic selection of DNA operation rules. However, the generated chaotic sequences are predictable due to the non-optimized parameters used in their scheme, which can compromise the security of the encrypted images. The summary of their cryptographic schemes, which are built on chaotic neural networks, is outlined in Table 8.

IX. DEEP LEARNING BASED IMAGE ENCRYPTION

Deep learning-based image encryption utilizes neural networks to improve the security of digital data. These networks are trained to learn complex patterns in images and create robust encryption techniques. In [195], Ding et al. proposed a deep learning-based network that acts as a stream cipher generator to create private keys (DeepKeyGen) to encrypt medical images. Their proposed encryption framework employs a GAN and DeepKeyGen, which aim to learn the mapping between initial images and their corresponding secret keys. The authors evaluated its performance using the Montgomery County chest radiograph dataset, the Ultrasonic Brachial Plexus dataset, and the BraTS18 dataset. However, the efficiency of DeepKeyGen is compromised as the GAN struggles to capture the intricate features in medical images.

In [196], Zhou et al. introduced an optical encryption method using two-channel detection and deep learning.

TABLE 7. Summary of existing techniques based on adversarial neural networks.

Methodology Name	Application Domain	Real-World Performance	Robustness Against Attacks	Disadvantages	Potential Solutions
Maung et al. [152]	Image Encryption	High accuracy	Vulnerability to pixel shuffling with secret key	Reliance on pixel shuffling, Limited resilience	Improve key management, Verify against evolving attacks
Meraouche et al. [153]	Communication Security	Asymmetric key training, Encryption/Decryption	Vulnerability in key generation attacks	Potential adversarial attacks on key generation	Enhance key generation security
Li et al. [158]	Adversarial Network Encryption	Proficiency against robust opponents	Struggle to adapt to evolving attacks	Limited adaptability, Vulnerability to adversarial training	Improve adaptability, Address adversarial training vulnerabilities
Coutinho et al. [159]	ANC Cryptographic Algorithms	Learn OTP algorithm	Vulnerability to adversarial attacks on learning process	Reliance on neural networks, Susceptibility to AI-generated attacks	Enhance learning process security, Address susceptibility to AI attacks
Fang et al. [161]	Image Encryption	Enhanced security	Vulnerable to brute-force	Chaotic system instability, Small key space	Increase key space, Improve parameters
Fang et al. [165]	Image Encryption	Quantitative and qualitative analysis	Vulnerable to brute-force	Hyperchaotic system vulnerability, Small key space	Increase key space, Optimize system
Man et al. [167]	Random Number Generator	Passes NIST tests	Susceptible to adversarial	LSGAN vulnerability	Enhance LSGAN robustness
Wu et al. [168]	Image Encryption	ANC with SHA-256	Weaknesses related to ANC	ANC vulnerabilities, Smart attackers understanding network	Improve ANC security, Address attacks
Alsafyani et al. [170]	Face Feature Encryption	5D chaotic method	Weak optical chaotic map or Crypto GANs	Cyber-attacks, Adversarial targeting decryption	Enhance optical chaotic map, Improve Crypto GANs security
Li et al. [115]	Steganography	Chaos encryption, CNN transformations	Adversarial targeting weight	Targeting weight allocation, Compromising secrecy	Improve weight allocation, Enhance GANs security
Hao et al. [171]	Blockchain-based Protocol	Zero trust environment	Potential privacy issues	Insufficiently robust measures	Strengthen security measures

They employed random binary masks [197] and a neural network to encrypt and decrypt images, mapping speckled images to their originals. However, security risks arise if the neural network or matrix keys are exposed, allowing for possible reverse engineering. Additionally, dependence on deep learning for decryption may pose vulnerabilities in noisy or distorted image conditions.

In [198], Ahmad et al. devised a Perceptual Encryption (PE) method for color and grayscale images, enhancing security with minor bitrate increases compared to traditional methods. However, vulnerabilities may arise if smaller block sizes compromise encryption strength, enabling potential decryption weaknesses. Additionally, their application in a smart hospital using outsourced healthcare cloud services for tuberculosis diagnosis, employing an EfficientNetV2-based model [199] and noise-based data augmentation [200], might face challenges if synthetic data lacks accuracy or fails to represent the complexity of medical images, affecting diagnostic reliability.

In [201], Schiopu et al. proposed an innovative dual step approach for lossless image compression that incorporates deep learning to predict pixel values more accurately than traditional methods. The context tree-based bit-plane codec encodes prediction errors, which offers varying compression performance and complexity trade-offs. Inefficiencies in the ability of the codec to model and encode prediction errors impact compression performance, especially across diverse image datasets.

In [202], Abdellatef et al. proposed an image encryption approach to link CT images used in the diagnosis of COVID-19 with facial images. Using a CNN, the authors extracted facial features to adjust initial states by generating chaotic matrices applied in the Chaotic Magic Transform (CMT) [203] and bitwise XOR operations. The inadequacies

TABLE 8. Summary of existing techniques based on chaotic neural network.

Methodology name	Application domain	Real-world performance	Robustness against attacks	Disadvantages	Potential solutions
Bigdeli et al. [172]	Image Encryption/Decryption	Iterative robustness	Vulnerable to sophisticated cryptanalysis	Weaknesses in CNN design	Improve CNN design, Address cryptanalysis vulnerabilities
Chauhan et al. [175]	Image Encryption	Chaotic neural network weights	Design vulnerabilities	Chaotic sequence weaknesses	Enhance network design, Strengthen chaotic sequences
Maddodi et al. [176]	Digital Image Transmission		Robust security with CCNN	Challenge in dynamic parameters	Address dynamic parameter challenges
Wang et al. [177]	Image Encryption	Large key space, Multicable hyperchaotic system	Complex network vulnerabilities	Decryption failure	Improve complex network, Address decryption failure issues
Chen et al. [178]	Color Image Encryption	DNA encoding, Chaos, FODHNN	Enhanced security with DNA encoding	Weak Diffusion techniques	Strengthen diffusion operations, Improve chaos-based security
Chen et al. [182]	3D Neural Network	Digital Grayscale Image Security	Synchronization limitations	Impact on encryption accuracy	Explore alternatives for digital image security, Address synchronization limitations
Wang et al. [187]	Chaos-Based Color Image Encryption	Chaotic maps, Hopfield Neural Network	Limited key space	Vulnerable to brute force attacks	Increase chaotic map parameters, Enhance key space for better security
Hu et al. [188]	Color Image Encryption	Hopfield Chaotic Neural Network	Weaknesses in chosen-plaintext attack	Easy decryption	Strengthen chosen-plaintext attack resilience, Improve key generation
Liu et al. [190]	Color Image Encryption	Diffusion and Scrambling Operations	Weaknesses in HCNN-driven diffusion	Vulnerability in secondary scrambling	Optimize HCNN-driven diffusion, Enhance secondary scrambling security
Sha et al. [191]	Image Security	Fractional-Order Hopfield Neural Networks, Logic Valve-Based Diffusion	-	-	-
Wu et al. [192]	Color Image Encryption	Five-Dimensional Hyperchaotic System, HCNN	Predictable chaotic sequences	Non-optimized parameters	Optimize chaotic sequence parameters, Improve randomness for better security

in the contribution of chaotic matrices compromise the encryption process, making it insufficient for pixel scrambling and affects the overall security of the encrypted CT images.

In [204], Raja et al. proposed optimal deep learning with secure drone communication (ODLIE-SDC) techqniue for the classification and encryption of digital images. Their proposed method combines hyperchaotic map-based image encryption using the rider optimization algorithm (ROA) [205] for key generation. In their proposed approach, image classification is performed through the utilization of EfficientNet-B4-CBAM [206] for feature extraction and an enhanced stacked autoencoder (ESAE) [207] for classification. The hyperparameters of EfficientNet-B4-CBAM are determined using Bayesian optimization (BO) [208]. However, encryption lacks resilience against sophisticated attacks that compromise data security. Additionally, reliance on rider optimization and Bayesian optimization limits adaptability in dynamic scenarios.

In [209], Ding et al. proposed a DeepEDN that operates as a deep learning-based system to secure digital images using a Cycle-GAN [210]. Decryption involves a reconstruction network, whereas an ROI-mining network facilitates object extraction from enciphered images. The evaluation was conducted on a chest X-ray dataset. The Cycle-GAN is not suitable for proper concealment of sensitive information.

A. DEEP HASHING

In [211], Wang et al. proposed Weighted Generative Adversarial Networks (WeGAN) to create hashing codes by transferring clustering data from images. WeGAN involves three key modules: hashing, learning to derive individual image codes from image sets to generate image content, and tag representations. While the discriminator is used for weighted loss functions to handle uncertainties between images and tags, the security of the WeGAN is compromised as the discriminator fails to distinguish between generated and original data accurately.

In [212], Li et al. proposed a Bi-Half Net, which is an unsupervised deep hashing layer aiming to maximize binary code entropy by ensuring an equal distribution between bit values. They bypassed adding terms to the loss function due to optimization challenges, which can create a parameter-free network layer to mold continuous image features towards this optimal half-half bit distribution. This layer maximizes the Wasserstein distance penalty between learned features and the non-ideal bit distribution, which is the source of minimizing the entropy value of the encrypted images.

In [213], Liu et al. proposed a Deep Supervised Hashing (DSH) algorithm for efficient image retrieval on large datasets that utilizes CNNs to tackle image variability. Their proposed encryption scheme is trained on image pairs (similar or dissimilar) to create similarity-preserving binary codes. A detailed loss function enhances the discriminability of the output space by integrating supervised information from input pairs while regularizing real-valued outputs to approximate desired discrete values. This allows query image encoding through network propagation and subsequent quantization for data retrieval. However, the hyperparameters of CNN are not fully optimized in the encryption scheme, making it suspectable against different cyberattacks, such as entropy attacks, histogram attacks, and differential attacks.

In [214], Zhang et al. proposed a novel Deep Reinforcement Learning approach for Image Hashing (DRLIH), presenting hashing learning as a sequential decision-making process to enhance retrieval accuracy. This pioneering method uses recurrent neural networks (RNNs) [215] as agents within a hashing network, allowing sequential actions for image projection into binary codes and considering errors from previous functions. Furthermore, a sequential learning strategy in DRLIH captures decision-making that makes the combined state representation of the internal and image features of RNN. However, the weak sequential learning strategy might limit the overall effectiveness of DRLIH in learning robust image hashing.

In [216], Cui et al. proposed SCAlable Deep Hashing (SCADH) to enhance image retrieval by leveraging supervised user tags. Their proposed framework uses deep neural networks to jointly learn image representations and hash functions. This enhances the discriminative power of social tag semantics. Additionally, a discrete hash optimization scheme is also proposed to avoid information loss from binary quantization. However, the effectiveness of SCADH relies on the quality of weakly supervised user tags that can limit the hash code's discriminative power.

In [217], Zhang et al. proposed a supervised learning system to generate compact hashing codes from raw images. The authors organized triplet-based training to optimize similarity margins and enforce adjacency consistency. The proposed system utilizes a deep neural network for feature extraction and hash function optimization. However, triplet-based training does not capture real-world data.

In [218], Gattupalli et al. proposed a supervised semantic image hashing scheme that incorporates Deep Hashing using Tag Embeddings (WDHT) and user-generated tags to train hash codes. The reliance of WDHT on these tags for weak supervision limits its efficiency, as the tags inaccurately capture image content.

In [219], Verwilst et al. proposed an improved deep image hashing scheme by integrating variational autoencoder advancements, which shows better performance in terms of security and computational time complexity. This approach struggles with diverse image features and faces challenges in handling complex representations, which affects adaptability across different datasets. Table 9 provides a summary of cryptographic schemes that utilize deep learning techniques.

X. MACHINE LEARNING BASED IMAGE ENCRYPTION

In recent years, machine learning algorithms have been employed in encryption techniques to enhance the security of digital images while simultaneously reducing computational complexity. The reduction in the computational time of encryption algorithms may facilitate the seamless integration of encryption schemes into real-time applications. In [220], Shafique et al. developed an approach to selecting encryption algorithms (EAs) customized for specific applications using pattern recognition and machine learning techniques while evaluating various methods such as suport vector machine (SVM), linear regression (LR), decsion tree (DT). SVM emerged as the preferred technique, exhibiting 98.7% classification accuracy. However, focusing solely on accuracy might disregard factors like vulnerability to attacks and the EA's adaptability across diverse security needs. Relying on a single machine learning model might restrict the algorithm's suitability across different datasets and application scenarios.

In [221], Liu et al. adapted AlexNet, a modified convolutional neural network supplemented with a preprocessing module to encrypt image text, using chaotic sequences from Logistic-Sine and Lorenz systems. This fusion formed a real-time encryption model, which shows a recognition accuracy of 94.37% in the feature extraction process. AlexNet limits its adaptability across various real-time scenarios.

In [222], Zhang et al. proposed a machine learning-based system, High Efficiency Video Coding (HEVC), that optimizes coding complexity through a CU depth decision strategy. Their proposed approach integrates a joint classifier and RD complexity model that reduces computational load by an average of 51.45% compared to the original HEVC test model. The efficiency of the proposed model is limited by its inability.

In [223], Sinhal et al. proposed a secure color image watermarking scheme by utilizing YCbCr color space, integer wavelet transform (IWT) [224], and discrete cosine transform (DCT) [225]. Their proposed scheme enhances the security of the digital images through a Mersenne Twister random number generator for block selection during watermark insertion. An artificial neural network (ANN) optimizes computational efficiency. The Mersenne Twister generator is compromised, which poses a risk to watermark security.

TABLE 9. Summary of existing techniques based on deep learning methods.

Methodology	Application Domain	Real-World Performance	Robustness Against Attacks	Disadvantages	Potential Solutions
Ding et al. [195]	DeepKeyGen (GAN-based)	Medical Image Encryption	Compromised efficiency in GAN feature capture		Improve GAN feature capture, Enhance medical image intricacy learning
Zhou et al. [196]	Optical Encryption (Two-Channel + Deep Learning)	Image Encryption	Security risks if neural network	matrix keys exposed	Strengthen key protection, Address potential reverse-engineering risks
Ahmad et al. [198]	Perceptual Encryption (PE)	Color and Grayscale Image Encryption	Vulnerabilities with smaller block sizes	Challenges in smart hospital application	Optimize block size, Improve accuracy of synthetic data, Enhance model robustness
Schiopu et al. [201]	Deep Learning-Based Lossless Compression	Image Compression	Codec inefficiencies in modeling prediction errors		Enhance codec's ability to model prediction errors
Abdellatef et al. [202]	Chaotic Matrices + CNN (DeepEnc)	Linking CT Images with Facial Images	Inadequacies in chaotic matrices contribution		Improve chaotic matrices contribution, Enhance pixel scrambling
Raja et al. [204]	ODLIE-SDC (ROA + BO)	Image Classification and Encryption	Lack of resilience against sophisticated attacks		Strengthen encryption against attacks, Enhance adaptability in dynamic scenarios
Ding et al. [209]	DeepEDN (Cycle-GAN-based)	Digital Image Security	Unsuitability of Cycle-GAN for proper information concealment		Explore alternatives to Cycle-GAN, Improve sensitive information concealment

In [226], Revanna et al. proposed an image classification and encryption system using the Optical Character Recognition (OCR) [227] and K-NN methods. Their proposed approach prioritizes documents based on OCR-identified text and numbers and employs multi-dimensional chaotic maps for encryption with varied security levels. The system is vulnerable to attacks on the OCR system, which makes the system risky.

In [228], Arumugam et al. proposed an enhanced medical image encryption scheme by combining DNA subsequence operations and an improved Combined Linear Congruential Generator (C-LCG). Their proposed method involves scrambling the original image with C-LCG and bit rotation operation (BRO), which applies the DNA subsequence operations for effective encryption, and emphasizes safety improvements through machine learning. The encryption scheme is vulnerable to attacks on the underlying algorithms, which poses a risk to information confidentiality. Cryptographic schemes based on machine learning are summarized in Table 11.

A detailed comparison of a few of the existing encryption schemes, which are reviewed in the proposed survey, is also conducted. The comparison is made in relation to the applications they serve and the technologies employed in their respective schemes. This thorough examination aims to provide an understanding of encryption approaches in accordance with the implementation of the encryption scheme in real-time applications. Tables 12 and 13 provides a summarized analysis of existing schemes, encompassing the applications and technologies utilized in image encryption algorithms.

XI. CHALLENGES AND FUTURE DIRECTIONS

Based on the proposed survey of the existing cryptographic techniques, certain challenges are highlighted. Moreover, the corresponding future directions and advancements to address these challenges are also outlined as follows:

- **Quantum Computing Threats**
  Challenge: The advent of quantum computers creates threats to traditional cryptographic algorithms specifically in the area of image encryption. Moreover, quantum computers can breach the security of such encryption schemes.

TABLE 10. Continued: Summary of existing techniques based on deep learning methods.

Wang et al. [211]	WeGAN (Weighted GAN)	Image Clustering	Discriminator failure in distinguishing generated and original data		Strengthen discriminator, Improve data distinction
Li et al. [212]	Bi-Half Net	Unsupervised Hashing	Maximized binary code entropy,	Optimization challenges	Address optimization challenges, Optimize hyperparameters
Liu et al. [213]	DSH (Deep Supervised Hashing)	Image Retrieval	Suboptimal hyperparameter optimization		Optimize hyperparameters, Enhance robustness
Zhang et al. [214]	DRLIH (Deep RL for Image Hashing)	Image Hashing	Weak sequential learning strategy		Strengthen sequential learning, Improve robustness
Cui et al. [216]	SCADH (SCAlable Deep Hashing)	Image Retrieval	Reliance on weakly supervised user tags		Improve tag quality, Enhance discriminative power
Zhang et al. [217]	Supervised Learning	Image Hashing	Limitations in triplet-based training		Enhance training strategies, Capture real-world data
Gattupalli et al. [218]	WDHT (Weakly Supervised Deep Hashing with Tags)	Semantic Image Hashing	Inaccurate tags for weak supervision		Improve tag accuracy, Enhance efficiency
Verwilst et al. [219]	Improved Deep Image Hashing	Image Hashing	Challenges with diverse features	Challenges with complex representations	Address feature diversity, Improve handling of complex representations

TABLE 11. Summary of existing techniques based on machine learning methods.

Methodology	**Application Domain**	**Real-World Performance**	**Robustness Against Attacks**	**Disadvantages**	**Potential Solutions**
Shafique et al. [220]	Pattern Recognition and ML for EA Selection	Customized Encryption Algorithms	98.7% SVM classification accuracy	Limited focus on adaptability, Single ML model restriction	Consider broader security needs, Explore multiple ML models
Liu et al. [221]	AlexNet with Chaotic Sequences	Real-time Image Text Encryption	Recognition accuracy of 94.37% in feature extraction	Limited adaptability in real-time scenarios	Enhance real-time adaptability, Explore alternative architectures
Zhang et al. [222]	HEVC Optimization using ML	Coding Complexity Reduction (HEVC)	Average 51.45% reduction in computational load	Model limitations impact efficiency	Enhance model capabilities, Address model limitations
Sinhal et al. [223]	Watermarking with ML	Secure Color Image Watermarking	Mersenne Twister generator compromise	Risk to watermark security	Strengthen watermark security, Explore alternative generators
Revanna et al. [226]	OCR and K-NN for Encryption	Document Classification and Encryption	Vulnerability to OCR attacks	Risk to system security	Strengthen OCR system security, Explore robust encryption methods
Arumugam et al. [228]	DNA Subsequence Operations	Medical Image Encryption	Vulnerability to attacks on algorithms	Risk to information confidentiality	Enhance algorithm security, Explore alternative encryption methods

Future Direction: Research efforts should be focused on developing quantum-resistant encryption techniques, exploring post-quantum cryptography, and investigating more enhanced QKD for secure transmission of information.

- **Integration of Quantum and Classical Approaches:** **Challenge:** Integrating quantum and classical computing approaches simultaneously in image encryption is a difficult task. Combining the strengths of both frameworks while addressing their interoperability is a challenge.

  Future Direction: Future research should explore hybrid encryption schemes that incorporate the computational advantages of quantum computing for different tasks while maintaining a high level of data security.

TABLE 12. Evaluation of current schemes in terms of their application.

Schemes	Secure Communication	Cloud Storage	Real-Time Monitoring	Quantum cryptography	Internet of Things (IoT)	Surveillance
Wang et al. [80]	✓		✓	✓	✓	
Hai et al. [83]	✓		✓	✓	✓	
Ghai et al. [89]	✓	✓	✓	✓	✓	
Kuang et al. [95]	✓	✓			✓	
Iavich et al. [105]	✓	✓	✓	✓	✓	
Liu et al. [113]	✓	✓		✓		✓
Ahmad et al. [134]	✓	✓				✓
Yu et al. [145]	✓	✓				
Luo et al. [140]	✓		✓		✓	✓
Liu et al. [151]	✓	✓		✓		
Mehra et al. [157]	✓					✓
Liao et al. [169]	✓	✓		✓		✓
Hui et al. [174]	✓	✓	✓			✓
Yu et al. [181]	✓				✓	
Li et al. [186]	✓		✓			
Li et al. [193]	✓					✓
Liu et al. [194]	✓			✓		
Koppu et al. [203]	✓		✓		✓	
Zhu et al. [206]	✓		✓	✓	✓	
Kumar et al. [225]	✓			✓		✓

TABLE 13. Evaluation of current schemes concerning the employed technologies.

Schemes	Symmetric cryptography	Secure hash algorithms	Neural network/ Chaos	Stegnography techniques	QKD	Machine/Deep Learning
Liu et al. [221]	✓	✓				
Zhang et al. [214]	✓	✓				✓
Zhang et al. [217]	✓	✓				✓
Shafique et al. [220]	✓		✓			✓
Revanna et al. [226]	✓		✓			✓
Liu et al. [113]	✓		✓		✓	
Peng et al. [128]	✓		✓		✓	
Yang et al. [133]	✓			✓	✓	
Qu et al. [137]	✓		✓	✓	✓	
Hu et al. [148]	✓		✓	✓	✓	
Maung et al. [152]	✓		✓			✓
Coutinho et al. [159]	✓		✓			✓
Man et al. [167]	✓		✓			✓
Qu et al. [136]	✓		✓	✓		
Jiang et al. [142]	✓		✓	✓	✓	

- **Limited Quantum Hardware Resources:** Based on the proposed survey that highlights the vulnerabilities of existing cryptographic approaches, several challenges and gaps in the existing research within the field of cryptography have been identified. Addressing these challenges and pursuing the outlined future directions is essential for advancing the state of cryptography. The challenges and their corresponding future directions are delineated below:
  Challenge: Quantum hardware resources such as qubits and quantum gates are prone to cyberattacks due to limited error correction techniques. This limits the practicality and efficiency of quantum-based image encryption techniques.
  Future Direction: Continued advancements in quantum hardware and the development of scalable quantum processors are essential to enhance the security of quantum-based encryption techniques.
- **Adversarial Attacks in Machine Learning-Based Encryption:**
  Challenge: Machine learning-based encryption schemes are vulnerable to adversarial attacks where an attacker modifies the input data to break the integrity.
  Future Direction: Developing adversarial-resistant machine learning models and the incorporation of techniques such as adversarial training for encryption are significant robust directions.
- **Explainability and Interpretability:**
  Challenge: Deep learning models, especially neural networks, are often considered as "black boxes" with limited interpretability. Understanding the decision-making process of these models is crucial to robust security in image encryption applications.
  Future Direction: Developing the deep learning models using strategies such as simpler model architectures, visualization, and counterfactual explanations for image encryption can enable the users to understand and evaluate the security mechanisms.
- **Scalability and Efficiency:**
  Challenge: Some machine learning-based encryption schemes may face challenges related to scalability and efficiency when applied to real-time applications or large-scale image datasets.
  Future Direction: Improving the scalability and efficiency of these schemes through algorithmic optimization, parallelization, batch processing, and distributed

computing can be essential and helpful for practical implementation.

XII. CONCLUSION

The proposed research presents a comprehensive overview of recent cryptographic algorithms, including image encryption algorithms. The proposed survey encompasses various cryptographic categories, such as quantum encryption, quantum random number generation for image encryption, adversarial neural networks, deep hashing, and chaotic neural networks, as well as machine learning and deep learning-based encryption schemes. These categories are thoroughly explored in terms of their application domains, real-world performance, and resilience against cyberattacks. Furthermore, the survey identifies vulnerabilities and proposes potential solutions to address these challenges. A detailed comparison is made between the applications and technologies employed in existing cryptographic schemes to determine the suitability of each technique for specific applications. Additionally, a comparison between the proposed survey and an existing survey reveals a substantial difference in the covered categories. The proposed survey, which covers most categories not included in the existing survey, proves to be invaluable for a comprehensive understanding of existing cryptographic techniques. Finally, the research highlights the challenges that can be faced during the development of cryptographic schemes and then provides the corresponding future directions that can be used to overcome these challenges and promote advancements in cryptographic research.

ACKNOWLEDGEMENT

ADU authors acknowledge financial support from Abu Dhabi University's Office of Research and Grant Programs.

FUNDING STATEMENT

Abu Dhabi University's Office of Sponsored Programs in the United Emirates (Grant Number: 19300752) funded this endeavor.

REFERENCES

[1] W. Li, C. Feng, K. Yu, and D. Zhao, "MISS-D: A fast and scalable framework of medical image storage service based on distributed file system," *Comput. Methods Programs Biomed.*, vol. 186, Apr. 2020, Art. no. 105189.

[2] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan, "The rise of 'big data' on cloud computing: Review and open research issues," *Inf. Syst.*, vol. 47, pp. 98–115, Jan. 2015.

[3] Z. Zhang, T. Zhen, and Z. Li, "Overview of big data storage methods," *Sci. J. Intell. Syst. Res. Volume*, vol. 3, no. 9, pp. 1–8, 2021.

[4] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electr. Power Syst. Res.*, vol. 215, Feb. 2023, Art. no. 108975.

[5] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 746–789, 1st Quart., 2020.

[6] H. N. Saha, A. Mandal, and A. Sinha, "Recent trends in the Internet of Things," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2017, pp. 1–4.

[7] H. Verma, M. Jain, K. Goel, A. Vikram, and G. Verma, "Smart home system based on Internet of Things," in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2016, pp. 2073–2075.

[8] M. N. Mohammed, S. F. Desyansah, S. Al-Zubaidi, and E. Yusuf, "An Internet of Things-based smart homes and healthcare monitoring and management system: Review," *J. Phys., Conf. Ser.*, vol. 1450, no. 1, Feb. 2020, Art. no. 012079.

[9] Y. Zheng, Z. Li, X. Xu, and Q. Zhao, "Dynamic defenses in cyber security: Techniques, methods and challenges," *Digit. Commun. Netw.*, vol. 8, no. 4, pp. 422–435, Aug. 2022.

[10] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Proc. IFIP Int. Conf. Commun. Multimedia Secur.* Aveiro, Portugal. Cham, Switzerland: Springer, 2014, pp. 63–72.

[11] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Comput. Secur.*, vol. 111, Dec. 2021, Art. no. 102490.

[12] A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Comput. Secur.*, vol. 68, pp. 160–196, Jul. 2017.

[13] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "A novel pixel-split image encryption scheme based on 2D salomon map," *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 118845.

[14] S. Minaee, Y. Boykov, F. Porikli, A. Plaza, N. Kehtarnavaz, and D. Terzopoulos, "Image segmentation using deep learning: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 7, pp. 3523–3542, Jul. 2022.

[15] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107810.

[16] M. Keshk, B. Turnbull, E. Sitnikova, D. Vatsalan, and N. Moustafa, "Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems," *IEEE Access*, vol. 9, pp. 55077–55097, 2021.

[17] R. K. Jha, "Cybersecurity and confidentiality in smart grid for enhancing sustainability and reliability," *Recent Res. Rev. J.*, vol. 2, no. 2, pp. 215–241, 2023.

[18] G. Mustafa, R. Ashraf, M. A. Mirza, A. Jamil, and Muhammad, "A review of data security and cryptographic techniques in IoT based devices," in *Proc. 2nd Int. Conf. Future Netw. Distrib. Syst.*, Jun. 2018, pp. 1–9.

[19] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100075.

[20] S. A. Laskar, "Secure data transmission using steganography and encryption technique," *Int. J. Cryptogr. Inf. Secur.*, vol. 2, no. 3, pp. 161–172, Sep. 2012.

[21] G. J. Matthews and O. Harel, "Data confidentiality: A review of methods for statistical disclosure limitation and methods for assessing privacy," Tech. Rep., 2011.

[22] A. K. Pandey, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, R. Kumar, and R. A. Khan, "Key issues in healthcare data integrity: Analysis and recommendations," *IEEE Access*, vol. 8, pp. 40612–40628, 2020.

[23] A. Anand and A. K. Singh, "Watermarking techniques for medical data authentication: A survey," *Multimedia Tools Appl.*, vol. 80, no. 20, pp. 30165–30197, Aug. 2021.

[24] J. Sun, X. Yao, S. Wang, and Y. Wu, "Non-repudiation storage and access control scheme of insurance data based on blockchain in IPFS," *IEEE Access*, vol. 8, pp. 155145–155155, 2020.

[25] S. Aggarwal and N. Kumar, "Digital signatures," in *Advances in Computers*, vol. 121. Amsterdam, The Netherlands: Elsevier, 2021, pp. 95–107.

[26] B. Preneel, "Cryptographic hash functions," *Trans. Emerg. Telecommun. Technol.*, vol. 5, no. 4, pp. 431–448, 1994.

[27] H. K. Lee, T. Malkin, and E. Nahum, "Cryptographic strength of SSL/TLS servers: Current and recent practices," in *Proc. 7th ACM SIGCOMM Conf. Internet Meas.*, Oct. 2007, pp. 83–92.

[28] M. S. Haque and M. U. Chowdhury, "A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV)," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.*, Niagara Falls, ON, Canada. Cham, Switzerland: Springer, Oct. 2017, pp. 113–1220.

[29] N. N. Hurrah, S. A. Parah, N. A. Loan, J. A. Sheikh, M. Elhoseny, and K. Muhammad, "Dual watermarking framework for privacy protection and content authentication of multimedia," *Future Gener. Comput. Syst.*, vol. 94, pp. 654–673, May 2019.

[30] A. Saxena, D. MISRA, R. Ganesamoorthy, J. L. A. Gonzales, H. A. Almashaqbeh, and V. Tripathi, "Artificial intelligence wireless network data security system for medical records using cryptography management," in *Proc. 2nd Int. Conf. Advance Comput. Innov. Technol. Eng. (ICACITE)*, Apr. 2022, pp. 2555–2559.

[31] M. A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab, M. A. Orgun, W. Iqbal, I. Rashid, and A. Yaseen, "Privacy preservation in e-Healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2018.

[32] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, Jun. 2022, Art. no. e4049.

[33] M. Kumari, S. Gupta, and P. Sardana, "A survey of image encryption algorithms," *3D Res.*, vol. 8, no. 4, pp. 1–35, Dec. 2017.

[34] M. K. Hasan, S. Islam, R. Sulaiman, S. Khan, A. A. Hashim, S. Habib, M. Islam, S. Alyahya, M. M. Ahmed, S. Kamil, and M. A. Hassan, "Lightweight encryption technique to enhance medical image security on Internet of Medical Things applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021.

[35] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[36] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006.

[37] R.-C. Wang, W.-S. Juang, and C.-L. Lei, "Robust authentication and key agreement scheme preserving the privacy of secret key," *Comput. Commun.*, vol. 34, no. 3, pp. 274–280, Mar. 2011.

[38] M. Ahmad and M. S. Alam, "A new algorithm of encryption and decryption of images using chaotic mapping," *Int. J. Comput. Sci. Eng.*, vol. 2, no. 1, pp. 46–50, 2009.

[39] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Opt. Lasers Eng.*, vol. 84, pp. 26–36, Sep. 2016.

[40] S. Jiao, T. Lei, Y. Gao, Z. Xie, and X. Yuan, "Known-plaintext attack and ciphertext-only attack for encrypted single-pixel imaging," *IEEE Access*, vol. 7, pp. 119557–119565, 2019.

[41] A. Shafique, A. Mehmood, M. Elhadef, and K. H. Khan, "A lightweight noise-tolerant encryption scheme for secure communication: An unmanned aerial vehicle application," *PLoS ONE*, vol. 17, no. 9, Sep. 2022, Art. no. e0273661.

[42] G. Raja, S. Anbalagan, A. Ganapathisubramaniyan, M. S. Selvakumar, A. K. Bashir, and S. Mumtaz, "Efficient and secured swarm pattern multi-UAV communication," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7050–7058, Jul. 2021.

[43] N. Ravi, R. Chitanvis, and M. El-Sharkawy, "Applications of drones using wireless sensor networks," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Jul. 2019, pp. 513–518.

[44] Z. Liu, L. Wang, X. Wang, X. Shen, and L. Li, "Secure remote sensing image registration based on compressed sensing in cloud setting," *IEEE Access*, vol. 7, pp. 36516–36526, 2019.

[45] M. Babel, F. Pasteau, C. Strauss, M. Pelcat, L. Bédat, M. Blestel, and O. Déforges, "Preserving data integrity of encoded medical images: The lar compression framework," *Advances in Reasoning-Based Image Processing Intelligent Systems: Conventional and Intelligent Paradigms*. Springer, 2012, pp. 91–125.

[46] J. Ahmad, H. Larijani, R. Emmanuel, M. Mannion, A. Javed, and A. Ahmadinia, "An intelligent real-time occupancy monitoring system with enhanced encryption and privacy," in *Proc. IEEE 17th Int. Conf. Cognit. Informat. Cognit. Comput. (ICCI*CC)*, Jul. 2018, pp. 524–529.

[47] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 133, no. 8, p. 331, Aug. 2018.

[48] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, "Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain," *IEEE Access*, vol. 9, pp. 59108–59130, 2021.

[49] B. Pulido-Gaytan, A. Tchernykh, J. M. Cortés-Mendoza, M. Babenko, G. Radchenko, A. Avetisyan, and A. Y. Drozdov, "Privacy-preserving neural networks with homomorphic encryption: Challenges and opportunities," *Peer Peer Netw. Appl.*, vol. 14, no. 3, pp. 1666–1691, 2021.

[50] M. S. Mehmood, M. R. Shahid, A. Jamil, R. Ashraf, T. Mahmood, and A. Mehmood, "A comprehensive literature review of data encryption techniques in cloud computing and IoT environment," in *Proc. 8th Int. Conf. Inf. Commun. Technol. (ICICT)*, Nov. 2019, pp. 54–59.

[51] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *Computing*, vol. 23, no. 4, p. 25, 2010.

[52] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Performance evaluation of symmetric encryption algorithms on power consumption for wireless devices," *Int. J. Comput. Theory Eng.*, vol. 1, no. 4, pp. 343–351, 2009.

[53] L. Zhang, W. Wang, and Y. Zhang, "Privacy preserving association rule mining: Taxonomy, techniques, and metrics," *IEEE Access*, vol. 7, pp. 45032–45047, 2019.

[54] W. El-Shafai, F. Khallaf, E.-S.-M. El-Rabaie, and F. E. A. El-Samie, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 10, pp. 9007–9035, Oct. 2021.

[55] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-based image encryption scheme," *Inf. Sci.*, vol. 520, pp. 130–141, May 2020.

[56] P. N. Lone, D. Singh, V. Stoffová, D. C. Mishra, U. H. Mir, and N. Kumar, "Cryptanalysis and improved image encryption scheme using elliptic curve and affine Hill cipher," *Mathematics*, vol. 10, no. 20, p. 3878, Oct. 2022.

[57] C. Zhang, J. Chen, and D. Chen, "Cryptanalysis of an image encryption algorithm based on a 2D hyperchaotic map," *Entropy*, vol. 24, no. 11, p. 1551, Oct. 2022.

[58] A. S. Alanazi, N. Munir, M. Khan, M. Asif, and I. Hussain, "Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes," *IEEE Access*, vol. 9, pp. 93795–93802, 2021.

[59] A. S. Sajitha and A. S. Rekh, "Review on various image encryption schemes," *Mater. Today, Proc.*, vol. 58, pp. 529–534, Jan. 2022.

[60] C. Tiken and R. Samli, "A comprehensive review about image encryption methods," *Harran Üniversitesi Mühendislik Dergisi*, vol. 7, no. 1, pp. 27–49, 2022.

[61] T. Ramanathan, M. J. Hossen, M. S. Sayeed, and J. E. Raja, "Survey on computational intelligence based image encryption techniques," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 19, no. 3, p. 1428, Sep. 2020.

[62] O. Salman, I. H. Elhajj, A. Kayssi, and A. Chehab, "A review on machine learning–based approaches for Internet traffic classification," *Ann. Telecommun.*, vol. 75, nos. 11–12, pp. 673–710, Dec. 2020.

[63] A. A. Abdullah and S. S. Mahdi, "Hybrid quantum-classical key distribution," *Int. J. Innov. Technol. Exploring Eng. (IJITEE)*, vol. 8, no. 12, pp. 4786–4791, 2019.

[64] M. A. Mahmoud, T. Mekkawy, and A. D. Elbayoumy, "Enhanced image encryption algorithm by quantum key distribution," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1172, no. 1, Aug. 2021, Art. no. 012011.

[65] Y. Liu, Z. Jiang, X. Xu, F. Zhang, and J. Xu, "Optical image encryption algorithm based on hyper-chaos and public-key cryptography," *Opt. Laser Technol.*, vol. 127, Jul. 2020, Art. no. 106171.

[66] N. F. Bar, H. Yetis, and M. Karakose, "A quantum-classical hybrid classifier using multi-encoding method for images," in *Proc. 27th Int. Conf. Inf. Technol. (IT)*, Feb. 2023, pp. 1–4.

[67] H. Yetis and M. Karaköse, "Variational quantum circuits for convolution and window-based image processing applications," *Quantum Sci. Technol.*, vol. 8, no. 4, Oct. 2023, Art. no. 045004.

[68] S. Kim and R. Casper, *Applications of Convolution in Image Processing With MATLAB*. Washington, DC, USA: Univ. Washington, 2013, pp. 1–20.

[69] X.-H. Song, S. Wang, A. A. Abd El-Latif, and X.-M. Niu, "Quantum image encryption based on restricted geometric and color transformations," *Quantum Inf. Process.*, vol. 13, no. 8, pp. 1765–1787, Aug. 2014.

[70] A. Vaish and M. Kumar, "Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain," *Optik*, vol. 145, pp. 273–283, Sep. 2017.

[71] W. Hao, T. Zhang, X. Chen, and X. Zhou, "A hybrid NEQR image encryption cryptosystem using two-dimensional quantum walks and quantum coding," *Signal Process.*, vol. 205, Apr. 2023, Art. no. 108890.

[72] A. Saini, A. Tsokanos, and R. Kirner, "Quantum randomness in cryptography—A survey of cryptosystems, RNG-based ciphers, and QRNGs," *Information*, vol. 13, no. 8, p. 358, Jul. 2022.

[73] R.-G. Zhou and Y.-B. Li, "Quantum image encryption based on Lorenz hyper-chaotic system," *Int. J. Quantum Inf.*, vol. 18, no. 5, Aug. 2020, Art. no. 2050022.

[74] S. Miyake and K. Nakamae, "A quantum watermarking scheme using simple and small-scale quantum circuits," *Quantum Inf. Process.*, vol. 15, no. 5, pp. 1849–1864, May 2016.

[75] J. Braumüller, J. Cramer, S. Schlör, H. Rotzinger, L. Radtke, A. Lukashenko, P. Yang, S. T. Skacel, S. Probst, M. Marthaler, L. Guo, A. V. Ustinov, and M. Weides, "Multiphoton dressing of an anharmonic superconducting many-level quantum circuit," *Phys. Rev. B, Condens. Matter*, vol. 91, no. 5, Feb. 2015, Art. no. 054523.

[76] R. I. Abdelfatah, "Quantum image encryption using a self-adaptive hash function-controlled chaotic map (SAHF-CCM)," *IEEE Access*, vol. 10, pp. 107152–107169, 2022.

[77] S. Iranmanesh, R. Atta, and M. Ghanbari, "Implementation of a quantum image watermarking scheme using NEQR on IBM quantum experience," *Quantum Inf. Process.*, vol. 21, no. 6, p. 194, Jun. 2022.

[78] W. Hu, R.-G. Zhou, J. Luo, and B. Liu, "LSBs-based quantum color images watermarking algorithm in edge region," *Quantum Inf. Process.*, vol. 18, no. 1, p. 16, Jan. 2019.

[79] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, and L.-B. Zhang, "An efficient image encryption scheme using gray code based permutation approach," *Opt. Lasers Eng.*, vol. 67, pp. 191–204, Apr. 2015.

[80] M.-X. Wang, H.-M. Yang, D.-H. Jiang, B. Yan, J.-S. Pan, and T. Wang, "A novel quantum image watermarking scheme for tamper localization and self-recovery," *Quantum Inf. Process.*, vol. 21, no. 8, p. 277, Aug. 2022.

[81] R. Zhang, D. Xiao, and Y. Chang, "A novel image authentication with tamper localization and self-recovery in encrypted domain based on compressive sensing," *Secur. Commun. Netw.*, vol. 2018, pp. 1–15, Mar. 2018.

[82] J.-W. Jiang, T. Zhang, W. Li, and S.-M. Wang, "A quantum image watermarking scheme based on quantum Hilbert scrambling and steganography about the Moiré fringe," *Quantum Eng.*, vol. 2023, pp. 1–12, Mar. 2023.

[83] G. Hai-Ru, D. Ya-Ying, and X. Quan, "Quantum image watermarking algorithm based on blocked spatial domain," *Chin. J. Quantum Electron.*, vol. 35, no. 5, p. 527, 2018.

[84] Y. Zhou, R.-G. Zhou, X. Liu, and G. Luo, "A quantum image watermarking scheme based on two-bit superposition," *Int. J. Theor. Phys.*, vol. 58, no. 3, pp. 950–968, Mar. 2019.

[85] R.-G. Zhou, P. L. Yang, X. A. Liu, and H. Ian, "Quantum color image watermarking based on fast bit-plane scramble and dual embedded," *Int. J. Quantum Inf.*, vol. 16, no. 7, Oct. 2018, Art. no. 1850060.

[86] X. Jin, S. Yin, N. Liu, X. Li, G. Zhao, and S. Ge, "Color image encryption in non-RGB color spaces," *Multimedia Tools Appl.*, vol. 77, no. 12, pp. 15851–15873, Jun. 2018.

[87] A. V. Zea, J. F. Barrera, and R. Torroba, "Innovative speckle noise reduction procedure in optical encryption," *J. Opt.*, vol. 19, no. 5, May 2017, Art. no. 055704.

[88] Y. Yang, X. Xiao, X. Cai, and W. Zhang, "A secure and privacy-preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images," *IEEE Signal Process. Lett.*, vol. 27, pp. 256–260, 2020.

[89] D. Ghai, H. K. Gianey, A. Jain, and R. S. Uppal, "Quantum and dual-tree complex wavelet transform-based image watermarking," *Int. J. Modern Phys. B*, vol. 34, no. 4, Feb. 2020, Art. no. 2050009.

[90] A. Shafique, M. M. Hazzazi, A. R. Alharbi, and I. Hussain, "Integration of spatial and frequency domain encryption for digital images," *IEEE Access*, vol. 9, pp. 149943–149954, 2021.

[91] Y. Ou, C. Sur, and K. H. Rhee, "Region-based selective encryption for medical imaging," in *Proc. Int. Workshop Frontiers Algorithmics*, Lanzhou, China. Cham, Switzerland: Springer, Aug. 2007, pp. 62–73.

[92] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105837.

[93] W.-W. Hu, R.-G. Zhou, A. El-Rafei, and S.-X. Jiang, "Quantum image watermarking algorithm based on Haar wavelet transform," *IEEE Access*, vol. 7, pp. 121303–121320, 2019.

[94] P. Fan, M. Hou, W. Hu, and K. Xiao, "Quantum image encryption based on block geometric and Haar wavelet transform," *Int. J. Theor. Phys.*, vol. 61, no. 11, p. 260, Nov. 2022.

[95] R. Kuang, D. Lou, A. He, C. McKenzie, and M. Redding, "Pseudo quantum random number generator with quantum permutation pad," in *Proc. IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, Oct. 2021, pp. 359–364.

[96] A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 1, pp. 101–111, Jan. 2014.

[97] P. Ayubi, S. Setayeshi, and A. M. Rahmani, "Deterministic chaos game: A new fractal based pseudo-random number generator and its cryptographic application," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102472.

[98] M. Ahmad, M. N. Doja, and M. S. Beg, "A new chaotic map based secure and efficient pseudo-random bit sequence generation," in *Proc. Int. Symp. Secur. Comput. Commun.*, Bengaluru, India. Cham, Switzerland: Springer, Sep. 2018, pp. 543–553.

[99] M. Iavich, T. Kuchukhidze, S. Gnatyuk, and A. Fesenko, "Novel certification method for quantum random number generators," *Int. J. Comput. Netw. Inf. Secur.*, vol. 13, no. 3, pp. 28–38, Jun. 2021.

[100] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps," *Nature Commun.*, vol. 9, no. 1, p. 5365, Dec. 2018.

[101] E. Abbadi, "Image encryption based on singular value decomposition," *J. Comput. Sci.*, vol. 10, no. 7, pp. 1222–1230, Jul. 2014.

[102] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum random number generation on a mobile phone," *Phys. Rev. X*, vol. 4, no. 3, Sep. 2014, Art. no. 031056.

[103] N. D. Truong, J. Y. Haw, S. M. Assad, P. K. Lam, and O. Kavehei, "Machine learning cryptanalysis of a quantum random number generator," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 403–414, Feb. 2019.

[104] N. Lauritzen, *Concrete Abstract Algebra: From Numbers to Gröbner Basesc*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[105] M. Iavich, T. Kuchukhidze, G. Iashvili, and S. Gnatyuk, "Hybrid quantum random number generator for cryptographic algorithms," *Radioelectronic Comput. Syst.*, no. 4, pp. 103–118, Nov. 2021.

[106] L. Hirvonen and K. Suhling, "Photon counting imaging with an electron-bombarded pixel image sensor," *Sensors*, vol. 16, no. 5, p. 617, Apr. 2016.

[107] R. Anitha and B. Vijayalakshmi, "Quantum chaos-based encryption technique for transmission of medical images," in *Proc. Int. Conf. Commun., Comput. Electron. Syst. (ICCCES)*. Cham, Switzerland: Springer, 2021, pp. 601–614.

[108] H. Khanzadi, M. Eshghi, and S. E. Borujeni, "Image encryption using random bit sequence based on chaotic maps," *Arabian J. Sci. Eng.*, vol. 39, no. 2, pp. 1039–1047, Feb. 2014.

[109] S. Patel, V. Thanikaiselvan, D. Pelusi, B. Nagaraj, R. Arunkumar, and R. Amirtharajan, "Colour image encryption based on customized neural network and DNA encoding," *Neural Comput. Appl.*, vol. 33, no. 21, pp. 14533–14550, Nov. 2021.

[110] L. Guo, H. Du, and D. Huang, "A quantum image encryption algorithm based on the Feistel structure," *Quantum Inf. Process.*, vol. 21, no. 1, pp. 1–18, Jan. 2022.

[111] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

[112] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19853–19873, Jul. 2020.

[113] X. Liu, D. Xiao, and C. Liu, "Three-level quantum image encryption based on Arnold transform and logistic map," *Quantum Inf. Process.*, vol. 20, no. 1, pp. 1–22, Jan. 2021.

[114] R. Vidhya and M. Brindha, "A novel approach for chaotic image encryption based on block level permutation and bit-wise substitution," *Multimedia Tools Appl.*, vol. 81, no. 3, pp. 3735–3772, Jan. 2022.

[115] Q. Li, X. Wang, X. Wang, B. Ma, C. Wang, Y. Xian, and Y. Shi, "A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks," *IEEE Access*, vol. 8, pp. 168166–168176, 2020.

[116] T. Li, J. Shi, X. Li, J. Wu, and F. Pan, "Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin cubes," *Entropy*, vol. 21, no. 3, p. 319, Mar. 2019.

[117] X. Liu, D. Xiao, and C. Liu, "Double quantum image encryption based on Arnold transform and qubit random rotation," *Entropy*, vol. 20, no. 11, p. 867, Nov. 2018.

[118] M. Sharma and A. Bhargava, "Chaos based image encryption using two step iterated logistic map," in *Proc. Int. Conf. Recent Adv. Innov. Eng. (ICRAIE)*, Dec. 2016, pp. 1–5.

[119] T. Janani and M. Brindha, "A secure medical image transmission scheme aided by quantum representation," *J. Inf. Secur. Appl.*, vol. 59, Jun. 2021, Art. no. 102832.

[120] X. Liu, D. Xiao, W. Huang, and C. Liu, "Quantum block image encryption based on Arnold transform and sine chaotification model," *IEEE Access*, vol. 7, pp. 57188–57199, 2019.

[121] E. Y. Baagyere, P. A. Agbedemnab, Z. Qin, M. I. Daabo, and Z. Qin, "A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers," *IEEE Access*, vol. 8, pp. 100438–100447, 2020.

[122] J. Kh-Madhloom, M. K. A. Ghani, and M. R. Baharon, "ECG encryption enhancement technique with multiple layers of AES and DNA computing," *Intell. Autom. Soft Comput.*, vol. 28, no. 2, pp. 493–512, 2021.

[123] F. Prior, K. Smith, A. Sharma, J. Kirby, L. Tarbox, K. Clark, W. Bennett, T. Nolan, and J. Freymann, "The public cancer radiology imaging collections of the cancer imaging archive," *Sci. Data*, vol. 4, no. 1, pp. 1–7, Sep. 2017.

[124] Z. Qu and H. Sun, "A secure information transmission protocol for healthcare cyber based on quantum image expansion and Grover search algorithm," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2551–2563, Sep. 2023.

[125] R.-G. Zhou, Q. Wu, M.-Q. Zhang, and C.-Y. Shen, "Quantum image encryption and decryption algorithms based on quantum image geometric transformations," *Int. J. Theor. Phys.*, vol. 52, no. 6, pp. 1802–1817, Jun. 2013.

[126] P. W. Shor, "Quantum computing," *Documenta Math.*, vol. 1, no. 1000, p. 1, 1998.

[127] H. Wen, C. Zhang, P. Chen, R. Chen, J. Xu, Y. Liao, Z. Liang, D. Shen, L. Zhou, and J. Ke, "A quantum chaotic image cryptosystem and its application in IoT secure communication," *IEEE Access*, vol. 9, pp. 20481–20492, 2021.

[128] H. Peng, B. Yang, L. Li, and Y. Yang, "Secure and traceable image transmission scheme based on semitensor product compressed sensing in telemedicine system," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2432–2451, Mar. 2020.

[129] A. S. Lewis and G. Knowles, "Image compression using the 2-D wavelet transform," *IEEE Trans. Image Process.*, vol. 1, no. 2, pp. 244–250, Apr. 1992.

[130] J. S. Seo, J. Haitsma, T. Kalker, and C. D. Yoo, "A robust image fingerprinting system using the radon transform," *Signal Process., Image Commun.*, vol. 19, no. 4, pp. 325–339, Apr. 2004.

[131] C.-W. Tang and H.-M. Hang, "A feature-based robust digital image watermarking scheme," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 950–959, Apr. 2003.

[132] N. Jiang, N. Zhao, and L. Wang, "LSB based quantum image steganography algorithm," *Int. J. Theor. Phys.*, vol. 55, no. 1, pp. 107–123, Jan. 2016.

[133] Y.-G. Yang, P. Xu, R. Yang, Y.-H. Zhou, and W.-M. Shi, "Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption," *Sci. Rep.*, vol. 6, no. 1, p. 19788, Jan. 2016.

[134] M. Ahmad, U. Shamsi, and I. R. Khan, "An enhanced image encryption algorithm using fractional chaotic systems," *Proc. Comput. Sci.*, vol. 57, pp. 852–859, Jan. 2015.

[135] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons Fractals*, vol. 35, no. 2, pp. 408–419, Jan. 2008.

[136] Z. Qu, S. Chen, and X. Wang, "A secure controlled quantum image steganography algorithm," *Quantum Inf. Process.*, vol. 19, no. 10, pp. 1–25, Oct. 2020.

[137] Z. Qu, H. Sun, and M. Zheng, "An efficient quantum image steganography protocol based on improved EMD algorithm," *Quantum Inf. Process.*, vol. 20, no. 2, pp. 1–29, Feb. 2021.

[138] Z. S. Younus and M. K. Hussain, "Image steganography using exploiting modification direction for compressed encrypted data," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2951–2963, Jun. 2022.

[139] R.-G. Zhou, J. Luo, X. Liu, C. Zhu, L. Wei, and X. Zhang, "A novel quantum image steganography scheme based on LSB," *Int. J. Theor. Phys.*, vol. 57, no. 6, pp. 1848–1863, Jun. 2018.

[140] Y. Luo, J. Lin, J. Liu, D. Wei, L. Cao, R. Zhou, Y. Cao, and X. Ding, "A robust image encryption algorithm based on Chua's circuit and compressive sensing," *Signal Process.*, vol. 161, pp. 227–247, Aug. 2019.

[141] H. Hu, Y. Cao, J. Xu, C. Ma, and H. Yan, "An image compression and encryption algorithm based on the fractional-order simplest chaotic circuit," *IEEE Access*, vol. 9, pp. 22141–22155, 2021.

[142] N. Jiang and L. Wang, "A novel strategy for quantum image steganography based on Moiré pattern," *Int. J. Theor. Phys.*, vol. 54, no. 3, pp. 1021–1032, Mar. 2015.

[143] Z. Qu, Z. Cheng, W. Liu, and X. Wang, "A novel quantum image steganography algorithm based on exploiting modification direction," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 7981–8001, Apr. 2019.

[144] V. K. Sharma, P. C. Sharma, H. Goud, and A. Singh, "Hilbert quantum image scrambling and graph signal processing-based image steganography," *Multimedia Tools Appl.*, vol. 81, no. 13, pp. 17817–17830, May 2022.

[145] Z. Yu, Z. Zhe, Y. Haibing, P. Wenjie, and Z. Yunpeng, "A chaos-based image encryption algorithm using wavelet transform," in *Proc. 2nd Int. Conf. Adv. Comput. Control*, vol. 2, Mar. 2010, pp. 217–222.

[146] B. Abd-El-Atty, A. A. A. El-Latif, and M. Amin, "New quantum image steganography scheme with Hadamard transformation," in *Proc. Int. Conf. Adv. Intell. Syst. Inform.* Cham, Switzerland: Springer, 2017, pp. 342–352.

[147] S. Prajwalasimha, "Pseudo-hadamard transformation-based image encryption scheme," IN *Integrated Intelligent Computing, Communication and Security*. Springer, 2019, pp. 575–583.

[148] W.-W. Hu, R.-G. Zhou, X.-A. Liu, J. Luo, and G.-F. Luo, "Quantum image steganography algorithm based on modified exploiting modification direction embedding," *Quantum Inf. Process.*, vol. 19, no. 5, p. 137, May 2020.

[149] G. Lin, Q. Wu, L. Chen, L. Qiu, X. Wang, T. Liu, and X. Chen, "Deep unsupervised learning for image super-resolution with generative adversarial network," *Signal Process., Image Commun.*, vol. 68, pp. 88–100, Oct. 2018.

[150] D. Kim, J. Chung, J. Kim, D. Y. Lee, S. Y. Jeong, and S. Jung, "Constrained adversarial loss for generative adversarial network-based faithful image restoration," *ETRI J.*, vol. 41, no. 4, pp. 415–425, Aug. 2019.

[151] J. Liu, Y. Ke, Z. Zhang, Y. Lei, J. Li, M. Zhang, and X. Yang, "Recent advances of image steganography with generative adversarial networks," *IEEE Access*, vol. 8, pp. 60575–60597, 2020.

[152] M. Maung, A. Pyone, and H. Kiya, "Encryption inspired adversarial defense for visual classification," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2020, pp. 1681–1685.

[153] I. Meraouche, S. Dutta, H. Tan, and K. Sakurai, "Learning asymmetric encryption using adversarial neural networks," *Eng. Appl. Artif. Intell.*, vol. 123, Aug. 2023, Art. no. 106220.

[154] S. K. Rajput and N. K. Nishchal, "Image encryption based on interference that uses fractional Fourier domain asymmetric keys," *Appl. Opt.*, vol. 51, no. 10, p. 1446, 2012.

[155] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Process.*, vol. 113, pp. 104–112, Aug. 2015.

[156] G. K. Soni, H. Arora, and B. Jain, "A novel image encryption technique using Arnold transform and asymmetric RSA algorithm," in *Proc. Int. Conf. Artif. Intell., Adv. Appl.* Cham, Switzerland: Springer, 2020, pp. 83–90.

[157] I. Mehra and N. K. Nishchal, "Optical asymmetric image encryption using gyrator wavelet transform," *Opt. Commun.*, vol. 354, pp. 344–352, Nov. 2015.

[158] Z. Li, X. Yang, K. Shen, R. Zhu, and J. Jiang, "Information encryption communication system based on the adversarial networks foundation," *Neurocomputing*, vol. 415, pp. 347–357, Nov. 2020.

[159] M. Coutinho, R. de Oliveira Albuquerque, F. Borges, L. G. Villalba, and T.-H. Kim, "Learning perfectly secure cryptography to protect communications with adversarial neural cryptography," *Sensors*, vol. 18, no. 5, p. 1306, Apr. 2018.

[160] A. N. K. Telem, C. M. Segning, G. Kenne, and H. B. Fotsin, "A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network," *Adv. Multimedia*, vol. 2014, pp. 1–13, Jan. 2014.

[161] 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 Appl.*, vol. 81, no. 15, pp. 21811–21857, Jun. 2022.

[162] J. Liu, Y. Ma, S. Li, J. Lian, and X. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimedia Tools Appl.*, vol. 77, no. 17, pp. 22787–22808, Sep. 2018.

[163] K. Loukhaoukha, J.-Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle," *J. Electr. Comput. Eng.*, vol. 2012, pp. 1–13, Jan. 2012.

[164] Z. Li, C. Peng, L. Li, and X. Zhu, "A novel plaintext-related image encryption scheme using hyper-chaotic system," *Nonlinear Dyn.*, vol. 94, no. 2, pp. 1319–1333, Oct. 2018.

[165] P. Fang, H. Liu, and C. Wu, "A novel chaotic block image encryption algorithm based on deep convolutional generative adversarial networks," *IEEE Access*, vol. 9, pp. 18497–18517, 2021.

[166] W. Feng, Z. Qin, J. Zhang, and M. Ahmad, "Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding," *IEEE Access*, vol. 9, pp. 145459–145470, 2021.

[167] Z. Man, J. Li, X. Di, X. Liu, J. Zhou, J. Wang, and X. Zhang, "A novel image encryption algorithm based on least squares generative adversarial network random number generator," *Multimedia Tools Appl.*, vol. 80, no. 18, pp. 27445–27469, Jul. 2021.

[168] J. Wu, W. Xia, G. Zhu, H. Liu, L. Ma, and J. Xiong, "Image encryption based on adversarial neural cryptography and SHA controlled chaos," *J. Modern Opt.*, vol. 68, no. 8, pp. 409–418, May 2021.

[169] X. Liao, A. Kulsoom, and S. Ullah, "A modified (Dual) fusion technique for image encryption using SHA-256 hash and multiple chaotic maps," *Multimedia Tools Appl.*, vol. 75, no. 18, pp. 11241–11266, Sep. 2016.

[170] M. Alsafyani, F. Alhomayani, H. Alsuwat, and E. Alsuwat, "Face image encryption based on feature with optimization using secure crypto general adversarial neural network and optical chaotic map," *Sensors*, vol. 23, no. 3, p. 1415, Jan. 2023.

[171] X. Hao, W. Ren, R. Xiong, T. Zhu, and K.-K.-R. Choo, "Asymmetric cryptographic functions based on generative adversarial neural networks for Internet of Things," *Future Gener. Comput. Syst.*, vol. 124, pp. 243–253, Nov. 2021.

[172] N. Bigdeli, Y. Farid, and K. Afshar, "A novel image encryption/decryption scheme based on chaotic neural networks," *Eng. Appl. Artif. Intell.*, vol. 25, no. 4, pp. 753–765, Jun. 2012.

[173] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Hopfield attractor-trusted neural network: An attack-resistant image encryption," *Neural Comput. Appl.*, vol. 32, no. 15, pp. 11477–11489, Aug. 2020.

[174] Y. Hui, H. Liu, and P. Fang, "Neuron perceptron-driven image encryption incorporating hyper-chaotic system," in *Proc. CAA Symp. Fault Detection, Supervision, Saf. Tech. Processes (SAFEPROCESS)*, Dec. 2021, pp. 1–6.

[175] M. Chauhan and R. Prajapati, "Image encryption using chaotic based artificial neural network," *Int. J. Sci. Eng. Res.*, vol. 5, no. 6, pp. 1–6, 2014.

[176] G. Maddodi, A. Awad, D. Awad, M. Awad, and B. Lee, "A new image encryption algorithm based on heterogeneous chaotic neural network generator and DNA encoding," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 24701–24725, Oct. 2018.

[177] S. Wang, L. Hong, and J. Jiang, "An image encryption scheme using a chaotic neural network and a network with multistable hyperchaos," *Optik*, vol. 268, Oct. 2022, Art. no. 169758.

[178] L.-P. Chen, H. Yin, L.-G. Yuan, A. M. Lopes, J. A. T. Machado, and R.-C. Wu, "A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations," *Frontiers Inf. Technol. Electron. Eng.*, vol. 21, no. 6, pp. 866–879, Jun. 2020.

[179] P. N. Lone, D. Singh, and U. H. Mir, "Image encryption using DNA coding and three-dimensional chaotic systems," *Multimedia Tools Appl.*, vol. 81, no. 4, pp. 5669–5693, Feb. 2022.

[180] G. Arthi, V. Thanikaiselvan, and R. Amirtharajan, "4D hyperchaotic map and DNA encoding combined image encryption for secure communication," *Multimedia Tools Appl.*, vol. 81, no. 11, pp. 15859–15878, May 2022.

[181] F. Yu, X. Kong, H. Chen, Q. Yu, S. Cai, Y. Huang, and S. Du, "A 6D fractional-order memristive Hopfield neural network and its application in image encryption," *Frontiers Phys.*, vol. 10, Mar. 2022, Art. no. 847385.

[182] L. Chen, H. Yin, T. Huang, L. Yuan, S. Zheng, and L. Yin, "Chaos in fractional-order discrete neural networks with application to image encryption," *Neural Netw.*, vol. 125, pp. 174–184, May 2020.

[183] M. Paprocki and K. Erwiński, "Synchronization of electrical drives via EtherCAT fieldbus communication modules," *Energies*, vol. 15, no. 2, p. 604, Jan. 2022.

[184] Y. Zhao, W. Xu, X. You, N. Wang, and H. Sun, "Cooperative reflection and synchronization design for distributed multiple-RIS communications," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 5, pp. 980–994, Aug. 2022.

[185] Q. Wang, J. Hu, Y. Wu, and Y. Zhao, "Output synchronization of wide-area heterogeneous multi-agent systems over intermittent clustered networks," *Inf. Sci.*, vol. 619, pp. 263–275, Jan. 2023.

[186] T. Li, H. Wang, D. He, and J. Yu, "Synchronized provable data possession based on blockchain for digital twin," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 472–485, 2022.

[187] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on Hopfield chaotic neural network," *Opt. Lasers Eng.*, vol. 115, pp. 107–118, Apr. 2019.

[188] Y. Hu, S. Yu, and Z. Zhang, "On the security analysis of a Hopfield chaotic neural network-based image encryption algorithm," *Complexity*, vol. 2020, pp. 1–10, Jul. 2020.

[189] Q. Wang, X. Zhang, and X. Zhao, "Color image encryption algorithm based on bidirectional spiral transformation and DNA coding," *Phys. Scripta*, vol. 98, no. 2, Feb. 2023, Art. no. 025211.

[190] L. Liu, L. Zhang, D. Jiang, Y. Guan, and Z. Zhang, "A simultaneous scrambling and diffusion color image encryption algorithm based on Hopfield chaotic neural network," *IEEE Access*, vol. 7, pp. 185796–185810, 2019.

[191] Y. Sha, J. Mou, J. Wang, S. Banerjee, and B. Sun, "Chaotic image encryption with Hopfield neural network," *Fractals*, vol. 31, no. 6, Jan. 2023, Art. no. 2340107.

[192] 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*, vol. 24, no. 10, p. 1474, Oct. 2022.

[193] X. Li, J. Zeng, Q. Ding, and C. Fan, "A novel color image encryption algorithm based on 5-D hyperchaotic system and DNA sequence," *Entropy*, vol. 24, no. 9, p. 1270, Sep. 2022.

[194] Z.-L. Liu and C.-M. Pun, "Reversible data hiding in encrypted images using chunk encryption and redundancy matrix representation," *IEEE Trans. Depend. Secure Comput.*, vol. 19, no. 2, pp. 1382–1394, Mar. 2022.

[195] Y. Ding, F. Tan, Z. Qin, M. Cao, K. R. Choo, and Z. Qin, "DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 9, pp. 4915–4929, Sep. 2022.

[196] Q. Zhou, X. Wang, M. Jin, L. Zhang, and B. Xu, "Optical image encryption based on two-channel detection and deep learning," *Opt. Lasers Eng.*, vol. 162, Mar. 2023, Art. no. 107415.

[197] Y. Kim, J. Song, I. Moon, and Y. H. Lee, "Interference-based multiple-image encryption using binary phase masks," *Opt. Lasers Eng.*, vol. 107, pp. 281–287, Aug. 2018.

[198] I. Ahmad and S. Shin, "A perceptual encryption-based image communication system for deep learning-based tuberculosis diagnosis using healthcare cloud services," *Electronics*, vol. 11, no. 16, p. 2514, Aug. 2022.

[199] M. Tan and Q. V. Le, "EfficientNetv2: Smaller models and faster training," in *Proc. Int. Conf. Mach. Learn.*, 2021, pp. 10096–10106.

[200] P. Panda and K. Roy, "Implicit adversarial data augmentation and robustness with noise-based learning," *Neural Netw.*, vol. 141, pp. 120–132, Sep. 2021.

[201] I. Schiopu and A. Munteanu, "Deep-learning-based lossless image coding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 7, pp. 1829–1842, Jul. 2020.

[202] E. Abdellatef, E. A. Naeem, and F. E. A. El-Samie, "DeepEnc: Deep learning-based CT image encryption approach," *Multimedia Tools Appl.*, vol. 83, no. 4, pp. 11147–11167, Jan. 2024.

[203] S. Koppu and V. M. Viswanatham, "A fast enhanced secure image chaotic cryptosystem based on hybrid chaotic magic transform," *Model. Simul. Eng.*, vol. 2017, pp. 1–12, Jan. 2017.

[204] N. K. Raja, E. L. Lydia, T. A. Acharya, K. Radhika, E. Yang, and O. Yi, "Rider optimization with deep learning based image encryption for secure drone communication," *IEEE Access*, vol. 11, pp. 121646–121655, 2023.

[205] D. Binu and B. S. Kariyappa, "RideNN: A new rider optimization algorithm-based neural network for fault diagnosis in analog circuits," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 1, pp. 2–26, Jan. 2019.

[206] X. Zhu, X. Zhang, Z. Sun, Y. Zheng, S. Su, and F. Chen, "Identification of oil tea (*Camellia oleifera* C.Abel) cultivars using EfficientNet-B4 CNN model with attention mechanism," *Forests*, vol. 13, no. 1, p. 1, Dec. 2021.

[207] C. Brunner, A. Kő, and S. Fodor, "An autoencoder-enhanced stacking neural network model for increasing the performance of intrusion detection," *J. Artif. Intell. Soft Comput. Res.*, vol. 12, no. 2, pp. 149–163, Apr. 2021.

[208] P. I. Frazier, "Bayesian optimization," in *Recent Advances in Optimization and Modeling of Contemporary Problems*. Catonsville, MD, USA: Informs, 2018, pp. 255–278.

[209] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, "DeepEDN: A deep-learning-based image encryption and decryption network for Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1504–1518, Feb. 2021.

[210] J. Harms, Y. Lei, T. Wang, R. Zhang, J. Zhou, X. Tang, W. J. Curran, T. Liu, and X. Yang, "Paired cycle-GAN-based image correction for quantitative cone-beam computed tomography," *Med. Phys.*, vol. 46, no. 9, pp. 3998–4009, Sep. 2019.

[211] Y. Wang, L. Zhang, F. Nie, X. Li, Z. Chen, and F. Wang, "WeGAN: Deep image hashing with weighted generative adversarial networks," *IEEE Trans. Multimedia*, vol. 22, no. 6, pp. 1458–1469, Jun. 2020.

[212] Y. Li and J. Van Gemert, "Deep unsupervised image hashing by maximizing bit entropy," in *Proc. AAAI Conf. Artif. Intell.*, vol. 35, no. 3, May 2021, pp. 2002–2010.

[213] H. Liu, R. Wang, S. Shan, and X. Chen, "Deep supervised hashing for fast image retrieval," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 2064–2072.

[214] Y. Peng, J. Zhang, and Z. Ye, "Deep reinforcement learning for image hashing," 2018, *arXiv:1802.02904*.

[215] N. Abughazalah, A. Latif, M. W. Hafiz, M. Khan, A. S. Alanazi, and I. Hussain, "Construction of multivalued cryptographic Boolean function using recurrent neural network and its application in image encryption scheme," *Artif. Intell. Rev.*, vol. 56, no. 6, pp. 5403–5443, Jun. 2023.

[216] H. Cui, L. Zhu, J. Li, Y. Yang, and L. Nie, "Scalable deep hashing for large-scale social image retrieval," *IEEE Trans. Image Process.*, vol. 29, pp. 1271–1284, 2020.

[217] R. Zhang, L. Lin, R. Zhang, W. Zuo, and L. Zhang, "Bit-scalable deep hashing with regularized similarity learning for image retrieval and person re-identification," *IEEE Trans. Image Process.*, vol. 24, no. 12, pp. 4766–4779, Dec. 2015.

[218] V. Gattupalli, Y. Zhuo, and B. Li, "Weakly supervised deep image hashing through tag embeddings," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 10367–10376.

[219] M. Verwilst, N. Žižakic, L. Gu, and A. Pižurica, "Deep image hashing based on twin-bottleneck hashing with variational autoencoders," in *Proc. IEEE 23rd Int. Workshop Multimedia Signal Process. (MMSP)*, Oct. 2021, pp. 1–6.

[220] A. Shafique, A. Mehmood, M. Alawida, A. N. Khan, and A. U. R. Khan, "A novel machine learning technique for selecting suitable image encryption algorithms for IoT applications," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–21, Jul. 2022.

[221] L. Liu, M. Gao, Y. Zhang, and Y. Wang, "Application of machine learning in intelligent encryption for digital information of real-time image text under big data," *EURASIP J. Wireless Commun. Netw.*, vol. 2022, no. 1, p. 21, Dec. 2022.

[222] Y. Zhang, S. Kwong, X. Wang, H. Yuan, Z. Pan, and L. Xu, "Machine learning-based coding unit depth decisions for flexible complexity allocation in high efficiency video coding," *IEEE Trans. Image Process.*, vol. 24, no. 7, pp. 2225–2238, Jul. 2015.

[223] R. Sinhal, D. K. Jain, and I. A. Ansari, "Machine learning based blind color image watermarking scheme for copyright protection," *Pattern Recognit. Lett.*, vol. 145, pp. 171–177, May 2021.

[224] X. Huang, Y. Dong, G. Ye, and Y. Shi, "Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform," *Frontiers Comput. Sci.*, vol. 17, no. 3, Jun. 2023, Art. no. 173804.

[225] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Med. Biol. Eng. Comput.*, vol. 57, no. 11, pp. 2517–2533, Nov. 2019.

[226] C. R. Revanna and C. Keshavamurthy, "A novel priority based document image encryption with mixed chaotic systems using machine learning approach," *Facta Universitatis Ser., Electron. Energetics*, vol. 32, no. 1, pp. 147–177, 2019.

[227] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, p. 767, 1995.

[228] S. Arumugam and K. Annadurai, "An efficient machine learning based image encryption scheme for medical image security," *J. Med. Imag. Health Informat.*, vol. 11, no. 6, pp. 1533–1540, Jun. 2021.

ABID MEHMOOD (Member, IEEE) received the Ph.D. degree in computer science from Deakin University, Australia. He is currently an Assistant Professor with Abu Dhabi University. His research interests include information security and privacy, data mining, machine learning, and cloud computing.

ARSLAN SHAFIQUE received the Ph.D. degree from Riphah International University, Pakistan. He is currently a Researcher with the University of Glasgow, U.K. He has more than 20 high-impact factor publications, including contributions to prestigious transactions within his area of expertise. His name has been listed in the list of the World's Top 2% Scientists Rankings 2023 (by Stanford University and Elsevier). His research encompasses a wide range of topics, including cybersecurity, machine learning, artificial intelligence, and the Internet of Things (IoT).

MOATSUM ALAWIDA received the Ph.D. degree in computer science/cybersecurity (cryptography) from the School of Computer Sciences, Universiti Sains Malaysia, in 2020. He has published more than 15 articles in high impact factor journals. His research interests include chaotic systems, chaos-based applications, multimedia security, blockchain, cybersecurity, quantum-based cryptography, and cryptography. He has also served as a referee for some renowned journals, such as IEEE Transactions on Cybernetics, *Signal Processing*, *Information Sciences*, *Journal of Information Security and Applications*, IEEE Access, *Wireless Personal Communications*, the *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, *Optik*, *Optics and Laser Technology*, *IET Information Security*, *IET Image Processing*, *Security and Communication Networks*, *Chaos, Solitons and Fractals*, *Physica A: Statistical Mechanics and its Applications*, and *Signal Processing: Image Communication*.

ABDUL NASIR KHAN received the M.C.S. and M.S. (CS) degrees from COMSATS University Islamabad, Abbottabad Campus, in 2005 and 2008, respectively, and the Ph.D. degree from the University of Malaya, Malaysia, in 2014. He is an Associate Professor with the Department of Computer Science, COMSATS University Islamabad, Abbottabad. He has published many research articles in well reputed international journals. He is a domain expert of multiple international research funding bodies; and received multiple awards, fellowships, and research grants. His areas of research interests include cybersecurity, mobile cloud computing, ad hoc networks, and the IoT.