Received: 25 July 2025 | Revised: 18 September 2025 | Accepted: 11 October 2025 | Published online: 12 December 2025

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2025, Vol. 00(00) 1-13
DOI: 10.47852/bonviewJCCE52026947

BON VIEW PUBLISHING

Exploring Image Encryption Techniques: Challenges and Real-Life Application Insights with AI Influence

Dyala Ibrahim[1,*], Omar Isam Al Mrayat[2], Ahmad Reda Alzighaibi[3], Hasan Hashim[3], and El-Sayed Atlam[4,5]

[1] *Department of Cyber Security, Amman Arab University, Jordan*

[2] *Department of Software Engineering, Amman Arab University, Jordan*

[3] *Department of Information Systems, Taibah University, Saudi Arabia*

[4] *Department of Computer Science, Taibah University, Saudi Arabia*

[5] *Department of Computer Science, Tanta University, Egypt*

Abstract: In today's rapidly evolving digital landscape, the importance of data security cannot be overstated. Every day, vast amounts of information are generated and shared, with each data type (whether text, image, audio, or video) possessing its own unique characteristics and vulnerabilities. Among these, image data stand out due to their intricate structure and the sheer volume of sensitive information that they can contain. Images are different from text data. Text data are straightforward data and are easy to protect. Images are difficult to protect because they are not straightforward. Ways used for encryption have long been considered suitable for encrypting image data. However, currently, they are not. Criminals are developing techniques every day to defeat the right-spotting methods of the business world. Further, this prompts scientists and professionals to find effective solutions. This is where artificial intelligence (AI) comes into play. Techniques for securing images enhanced by AI have the potential to improve image encryption significantly in a manner that increases both protective security efficiency and processing efficiency. This paper discusses various image encryption techniques in detail, including both ancient and modern methods for protecting visual information. It also discusses AI that helps in enhancing the accuracy and efficacy of these encryption techniques. When it comes to encryption of images, AI makes it more powerful. It can also counter newer threats that are emerging. Therefore, security is more dependable and efficient. This paper gives a detailed review of state-of-the-art methods and their effectiveness over traditional methods. By delving into various AI techniques for image encryption, this paper shows that the incorporation of these techniques makes image encryption more secure and efficient.

Keywords: data security, security for image, encryption, artificial intelligence, image encryption

1. Introduction

Transforming an image into a ciphered form is called image encryption. The image encryption process converts the original image into a coded image (cipher image) that can only be decoded or deciphered by the intended recipient [1]. The concentration on image datasets has to do with the complexity of the images and their extensive use in real-life applications. To facilitate the encryption and decryption processes, a configuration key is required for the conversion from a plain image into an encrypted image [2]. The security of encryption relies heavily on these keys. There are two types of encryption methods based on keys: private or single key (symmetric key cryptography) and public keys (asymmetric key cryptography). In the private key [3] system, the same key is used for encryption and decryption. In the public key [4, 5] system, encryption and decryption keys are different; the encryption key is made public, and the decryption key is kept private. Figure 1 illustrates the block diagram of image encryption that explains the step-by-step operation of image encryption. It outlines the primary steps of the procedure in detail, starting with the original image, moving on to the encryption techniques, and concluding with a safe, encrypted image.

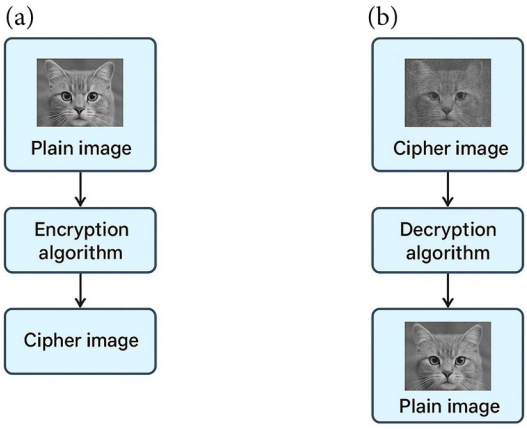
The terminologies used in encryption and decryption are the following [6]:

Plain image: the original and readable image (meaningful image).
Cipher image: the encrypted image and unreadable image (meaningless image).
Encryption: the process of transforming the original image into an encrypted image.
Decryption: the process of recovering and retrieving the cipher image back to the original image.
Key: the main configuration for the encryption and decryption processes.

This paper takes a closer look at diverse ways to encrypt images, covering both classic approaches and the latest advancements used to protect visual information. It also discusses how artificial intelligence (AI) is making a difference by improving the precision and effectiveness of these encryption methods. With the help of AI, image encryption becomes stronger and can better respond to new security threats, leading to more reliable and efficient protection overall.

***Corresponding author:** Dyala Ibrahim, Department of Cyber Security, Amman Arab University, Jordan. Email: d.ibrahim@aau.edu.jo

Figure 1
Structure of image encryption: (a) encryption process at the sender side and (b) decryption process at the receiver side



1.1. Image encryption approaches

According to literature, there are many traditional image encryption approaches, and each one has several shortcomings. In the succeeding subsection, each one of these techniques will be covered in depth. Figure 2 shows the taxonomy of image encryption techniques. Various image encryption techniques are depicted in this figure, demonstrating how various approaches are applied to safeguard visual information and preserve images. It demonstrates both conventional and contemporary methods, making it simple to understand how each protects digital images.

Various image encryption methodologies have been developed using symmetric, asymmetric, steganographic, and hashing techniques. In the subsequent subsection, we detail various image encryption methodologies, accompanied by a comparative analysis of the techniques in a tabular format.

1.1.1. Image encryption based on symmetric methods

Symmetric encryption involves the use of the same secret key to perform both the encryption and decryption operations [7]. The form of cryptography in which both the encryption and decryption processes rely on the same binary key is referred to as single-key or private-key cryptography [8, 9]. There are numerous algorithms associated with this type of cipher, such as Blowfish [10], [11], data encryption standard (DES) [12], and advanced encryption standard (AES) [13]. All of the above methods use a specific approach that encrypts the plaintext (original message). Then, they convert it to unreadable text (encrypted) after decryption using a fixed size of data as a block and a fixed size of key. The process of symmetric cipher is explained as shown in Figure 3 [14]. It demonstrates that the information is locked (encrypted) and unlocked (decrypted) using the same secret key. The steps are outlined in detail in the diagram, which begins with the original message, moves it through encryption using a shared key, and concludes with the message being safely recovered by someone who also has that key.

This type of cryptography has many pros: the key is short compared with other types, symmetric ciphers are simple and

Figure 2
Taxonomy of image encryption techniques

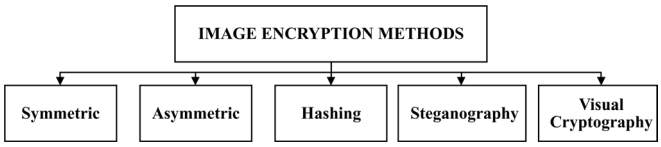
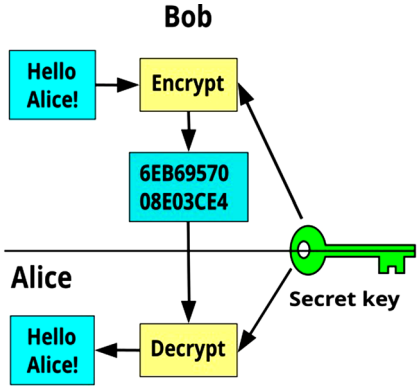


Figure 3
The symmetric cipher explanation process



uncomplicated to use and analyzed, and symmetric-key ciphers can be effectively employed as basic components for constructing different mathematical functions such as digital signature schemes, hash functions, and pseudorandom number generators (PRNGs) that are efficient in computation. Conversely, the main cons of symmetric cipher are key distribution, which means that the key must be kept during communication between two parties, and the key management problem, which means that numerous key pairs necessitate meticulous management in large networks. Therefore, effective key management requires the involvement of an unconditionally trusted third party (TTP) [14, 15].

Many methods have been developed to achieve key security objectives such as integrity, confidentiality, nonrepudiation, and authentication. Encryption plays a crucial role in addressing these challenges, especially when data are transmitted over unsecured wired or wireless channels. In the study reported by Kuppuswamy et al. [16], a new hybrid encryption method was introduced, combining the widely known Rivest–Shamir–Adleman (RSA) algorithm with a newly developed symmetric key (SSK) algorithm. This approach enhances security and privacy, making it particularly well suited for communication and financial applications. The symmetric SSK algorithm is fast and efficient, requiring small memory and fast encryption. This is one of the major pros of their work. The study presents a significant decrease in encryption time and a remarkable improvement in performance. However, challenges arise from general hybrid systems. One beneficial aspect of the hybrid method is that it employs an efficient way in which a public key is used for key exchange (as RSA) and a symmetric key is used for efficient data encryption. Moreover, hybrid methods have drawbacks. We have to manage both keys; for instance, the indirectness of the complexity problem is added, and the RSA's computational load in key generation is already something that we have to face.

In addition, Alemami et al. [17] proposed the Optimization Advanced Encryption Standard (OAES) algorithm, which is an enhanced version of the AES algorithm. The main problem in the proposed method is the key generation process. New keys will be generated using a random number and a sine map. Before undergoing five stages of coding cycles, the original message is multiplied with one more random matrix (4 × 4). A random substitution box is employed. The adopted model gives good security for encrypting any message. It makes it difficult to determine the original message. The main pros of the proposed method are enhanced security: the combination of AES and chaotic maps adds extra layers of complexity and makes it harder for hackers to break the encryption. The proposed method has potential for real-world use: because AES is already widely used, this method could be adapted for practical applications with additional security needs. However, the cons are increased complexity: adding chaotic maps to AES makes the system more complicated, which might make

implementation and maintenance harder, and performance overhead. The extra steps involved could slow down encryption and decryption, especially for copious amounts of data or on devices with limited power.

Ge et al. [18] proposed a novel indistinguishable color image encryption method based on efficient scrambling–diffusion. This method is secured, and the encryption process is faster in a way. Our ciphertext is divided into vertical and horizontal pixels for an enhanced security level, followed by scrambling–diffusion to encrypt it. A change in any pixel, no matter how little, could cascade through all color planes and in the ciphered image. The structures of all dynamic systems that have been used are simple, but they are characterized in such a way that they can quickly generate high-quality pseudorandom sequences. The scrambling–diffusion technique will simultaneously process the pixels for execution efficiency. The approach is very efficient and is secured from attacks for real-life applications with good security. The main drawback of the process that they used is that the encryption technique is more complex than the basic way. Consequently, this might make it harder to implement or understand without technical knowledge. The proposed method may be slower due to the use of multiple mechanisms.

Duan and Li [19] presented an innovative verifiable dynamic encryption scheme (v-PADSSE) through a public key cryptosystem. It aims to prevent data retrieval issues caused by the cloud server's backend limitations. The proposed scheme obtains verification information (VI) for each keyword and creates a verification list (VL) for its storage. In the cloud data during the dynamic updating process, the security index can be swiftly updated by acquiring fresh confirmation information from the VL. The assessment of the safety and performance of the v-PADSSE scheme shows that the scheme is safe and effective. However, storage overhead limitation due to storage for verification data: the VL stores verification metadata (e.g., update counts and flags), which adds storage requirements compared to simpler SSE schemes that omit such metadata, and linear growth in cost: performance (both time and storage) grows linearly with the number of documents and keywords. For very large-scale applications (where n and m are huge), this may become a bottleneck.

Lu et al. [20] proposed a new symmetric image encryption scheme by considering a new product trigonometric chaotic map. The proposed method relies on the features of the product trigonometric chaotic map such as the bifurcation diagram, Lyapunov exponent, approximate entropy, permutation entropy, time series diagrams, cobweb graphs, and NIST tests. The results demonstrate that the proposed technique provides a prominent level of security with a faster rate. However, complexity overhead is the core limitation of their work.

Many authors employed various multi-image encryption methods that were dependent on a new spatiotemporal chaotic system and fractal geometry to enhance the resistance of the proposed system. The suggested method was developed by creating another system called the Chebyshev improved coupled sine map lattice (CICSML), which was built on the coupled map lattice (CML) system for spatiotemporal chaos. The findings provide great defenses and resistance to attackers. However, chaotic systems are greatly affected by their initial conditions and parameters. Scientists found that if the map behaves in a predictable manner or if the key space is limited in some way, then chaos-based encryption schemes become weak. A smart hacker can take advantage of the way in which random numbers are made chaotic [21].

In addition, Rehman [22] suggested an image encryption mechanism that offers improved security using chaotic maps and quantum mechanics. This also deals with the limitation of a classic one-dimensional chaotic system, which is periodic and predictable. By tapping into the uncertainty of quantum theory, the plan employs 2D quantum coding and an algorithm from a one-dimensional sine-based chaotic map (1D SBCM) to produce high-entropy sequences for secure key generation. The results confirm that the proposed system is secured against attacks and intrusions. However, when things become complex, they can be impractical and sometimes even unpredictable. There are several investigators proposing new image encryption techniques to improve the security level and create effective techniques to resist potential attacks by utilizing symmetric cryptography. Researchers are constantly generating innovative ideas in this area of research to enhance image security.

1.1.2. Image encryption based on asymmetric methods

An asymmetric method is a type of cryptography that is based on two separated keys: one public key is used for encryption, and the other key is a private key used for decryption [23]. Asymmetric cryptography solves the key distribution and key management problems that are found in symmetric-key cryptography. This problem is one of the biggest challenges, which is securely sharing the secret key. If the key is intercepted during transmission, anyone can decrypt the data. This makes it crucial to find safe ways to share keys, which can be complicated [24].

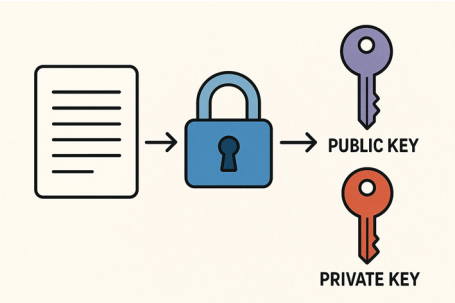
Asymmetric image encryption has various applications that leverage its unique security features. Using asymmetric encryption, one can send images efficiently and securely over the internet. For instance, in messaging applications, users have the option to encrypt images to ensure that only the intended recipient can decrypt and view them [25]. Digital rights management technology helps in preventing unauthorized copying of copyright images [26]. In healthcare, images of the patient (such as X-rays and MRIs) can be encrypted in medical imaging. Only authorized personnel can view these images with asymmetric encryption [27]. Users have the option to encrypt their image data before uploading to the cloud. If someone somehow penetrates the storage, he or she cannot view any of the images without having the decryption key [28]. Asymmetric encryption is applied in E-commerce to secure images of products. This prevents tampering and assures customers of getting the right product and right visuals [29]. Users can encrypt images before posting them on social media platforms. This creates a barrier against infringement, enabling users to retain control over their private images [30]. Stored in a blockchain, image data can be secured using asymmetric encryption. Asymmetric encryption will ensure authenticity and prevention of modification [31]. Internet of Things (IoT) devices: asymmetric encryption can protect images captured by IoT devices, such as smart cameras, ensuring that only authorized users can access the visual data [32].

Figure 4 [14] explains how an asymmetric cipher works. It shows that two different keys are used: a public key to lock (encrypt) the message and a private key to unlock (decrypt) it. The diagram walks through each step, starting with the sender encrypting the information using the recipient's public key and ending with the recipient safely unlocking the message using their private key.

Several works on this type of cryptography have been published. Al Saffar et al. [33] proposed a new encryption technique based on the asymmetric cryptosystem, which is called the Massey–Omura scheme. This method depends on a hard mathematical problem that is a discrete logarithm problem. The results prove that the technique is secure and fast, but it suffers from high complexity.

Furthermore, other authors developed a fresh asymmetric method based on a one-way crypto method, that is, SHA-3. This method is a hashing variant. Huang et al. [34] proposed a novel image-encryption scheme based on SHA-3, which enhances resistance to chosen-plaintext and known-plaintext attacks. In this method, the original image utilizes the hashing values that are generated by SHA-3, further creating a chaotic map. The given image is separated into blocks, which goes through sparse transformation, scrambling, and merging to provide an encrypted image. To return to its original size, zeros are padded to the encrypted image. The image pixel is extracted based on the placement

Figure 4
The asymmetric cipher explanation process



of the number. The process continues with the application of an integer wavelet transform (IWT) onto the cover image, which gives out four coefficients. These coefficients contain the extracted figures, and the inverse IWT will recover the carrier image with the embedded data [34]. This paper's primary benefit is its increased plaintext sensitivity and resistance to attacks. The scheme is designed to withstand KPA and CPA using the plaintext's SHA-3 hash values to seed chaotic systems. By doing this, attackers cannot alter known inputs to determine the key. However, the approach incurs significant computational overhead due to the use of SHA-3 hashing, block-wise sparse transforms, two scrambling rounds, compressive sensing, and quantization. Its applicability in real-time or resource-constrained scenarios is uncertain in the absence of performance benchmarks.

According to other research, hashing methods can further enhance security. Chen and Ye [35] introduced an asymmetric image encryption technique against SHA-3, RSA, and compressive sensing. According to the experiments, the proposed method can reconstruct the original image well. The technique is resistant to known plaintext attacks and chosen plaintext attacks because the keystreams are linked to the original image [35]. The primary advantage of this paper RSA integration enables a public-key architecture for secure key distribution and asymmetric encryption by encrypting SHA-3-derived plaintext keys into ciphertext keys. The keystream is dynamically connected to the plaintext (by SHA-3 and MTM), strengthening resistance against known-plaintext and chosen-plaintext attacks as each plaintext modifies the keying material. In addition, combined compression and encryption by compressive sensing CS decreases data size while encrypting, resulting in improved transmission and storage efficiency. The combination of hashing (SHA-3), RSA operations, compressive sensing, DWT/IDWT transforms, and several scrambling phases may be computationally demanding, potentially inappropriate for real-time or resource-constrained circumstances.

In contrast, some authors use chaotic phase masks and vector light fields to enhance the encryption technique's security level. The work of Rao et al. [36] elucidated a new scheme for image encryption for asymmetric crypto based on use chaotic phase masks and vectorial light. The proposed technique was processed under two layers. The first layer is performed by decomposing a binary image into two different chaotic phase masks in the fractional Fourier domain, followed by a method that truncates both phase and amplitude. At stage two, the truncated phase part is encoded into a vectorial light field. The two-layer encryption, asymmetric technique, and vector field ensure that the design is quite secure and easily implementable as it depends on intensity. The proposed method is secure against potential attacks. However, low clarity on essential elements is restricted by the absence of full-text access, including the characteristics of the structured phase masks, key generation details, encryption/decryption procedures, and security proofs, and the lack of quantitative assessment numerical measures to support performance claims is not mentioned, including error rates, robustness to noise, encryption/decryption speed, and key space size. Although the scheme is labeled as "highly secure," it offers low protection against wider attack surfaces and fails to consider threats such as optical-channel vulnerabilities, adaptive chosen-ciphertext attacks, side-channel attacks, and physical tampering.

Furthermore, a novel asymmetric image encryption technique with high security and quality was devised by a few [37]. In addition, Du and Ye [38] proposed a substantial image encryption asymmetric method based on the integer wavelet transformation (IWT) and RSA algorithm. In the first step, the two plain characteristic parameters (PCP) of an image are taken along with two random numbers. Subsequently, a new parameter transformation model (PTM) is developed to manipulate these parameters in a nonlinear way. After which, we can obtain three cipher characteristic parameters (CCP). RSA operations are applied to the abovementioned CCPs to generate three ciphertexts. Subsequently, an initial value obtaining model (IOM) is then constructed for plain and cipher messages, which generates initial values for a 3D chaotic system that produces three chaotic sequences. The results show that this algorithm quickly encrypts and efficiently protects against brute-force and noise attacks but suffers from complexity overhead [38].

Many researchers propose new image encryption techniques to increase security levels and build effective techniques to resist potential attacks using asymmetric cryptography. This area of research will generate more ideas to enhance image security.

1.1.3. Image encryption based on hashing methods

Hash is one-way cryptography with no key so that there is no need to worry regarding managing and exchanging the encryption key [39, 40]. This type of crypto (cipher) is useful for protecting the authenticity of information in telecommunication, computer networks, and blockchain [40].

There are many algorithms for text encryption, but not much research has been conducted on encryption of digital images or video files. Cheddad et al. [41] developed a new technique to encrypt a digital image using a 1D SHA-2 password-based algorithm and a compound forward transform. The main advantage of this algorithm is that it will narrow down a continuous tone payload (a steganographic term) to a balanced bit distribution sequence. This balance is significant for applications such as steganography and watermarking as it helps in maintaining a balanced perceptibility effect on the cover image. The use of SHA-2 hashing to protect passwords and key material converts sensitive values into fixed-length, irreversible digests, thereby mitigating the risk of credential disclosure and weakening key-dependency exploits. A hash function ensures that the encryption is dependent on both the image data and the password, increasing resistance to certain attacks. Hash functions are thoroughly researched: although SHA-2 has good preimage and collision resistance, among other things, their primary work limitation is secure key distribution because the algorithm is symmetric (based on password + SHA-2). The plan is completely broken if the password is compromised. There is no public key element [41].

Sheng and Li [42] developed an image encryption algorithm that incorporates the lattice hash function and privacy protection to address trust issues with cloud platforms. The algorithm proposes a new chaotic system based on the tent map and sine map through which random matrices can be generated for the lattice hash functions without considering periodic windows. A security key is generated by combining the image feature vector and the initial key. To increase security, the Paillier cryptosystem encrypts the feature vector to create a ciphertext image index. Furthermore, the enhanced 2D-line map randomizes the positions of the pixels, thereby avoiding storage of pixel subscripts. Private searching over encrypted data ensures strong security while allowing accurate searching of data. It is thought that using lattice-based cryptographic structures (or hash functions) provides security against adversaries with quantum-capable resources because many lattice issues (such as shortest vector, SIS, etc.) are challenging even

in post-quantum environments. The significance of this is growing. However, the complexity overhead resulting from lattice hash functions is typically more computationally demanding (in terms of both time and memory) than that of lightweight chaotic maps or straightforward XOR/diffusion techniques. This could potentially be a bottleneck, particularly for large images, real-time videos, or devices with limited resources [42].

DNA computing has an immense potential for data encryption. This is because DNA computing can simultaneously perform many calculations. DNA computing also takes much less space. Finally, DNA computing is very secure and prevents adversaries from breaking the codes. Li et al. [43] designed a new DNA computing algorithm for encrypting high-dimensional images. The DNA hash encoding module is complementing it with the content-aware encryption module. The authors made multiple hash mappings of image pixels with DNA bases using the unique property of hashing functions. The mapper of the model uses the advantages of both hashing and DNA computing. The findings demonstrate that this technique has a clear edge over existing techniques in key space, histogram analysis, pixel correlation, information entropy, and sensitivity measurements [43].

To increase security against attacks, others presented a color image encryption technique using a hash table, Hilbert curve, and hyper-chaotic synchronization methods. The proposed method is based on the rearranging (permutation) and spreading (diffusion) of the image. In addition, secure key information transmission relies on the synchronization of hyper-chaotic systems. The first key is generated using the hash value of the original image while another structure utilizing a hyper-chaotic sequence aids in the re-organization of the pixels and bits. The encrypted data are used to accelerate the diffusion process via the implementation of the Hilbert curves. Tests done to evaluate the algorithm showed a strong ability for encryption. It may effectively resist a variety of attacks. This scheme was appropriate for secure image communication applications. However, complexity overhead is the main limitation of their method [44].

Hashing is utilized in blockchain image encryption. Chithra and Aparna [45] introduced a security scheme to enhance blockchain image security using spiral mapping and hashing techniques. Read more below. A new secure method is proposed in encryption using blockchain and steganography. It may scramble 2D image data in cipher blocks using random rearrangement and spiral mapping. In addition, a linking based on SHA-512 hashes may take place in cipher blocks. Furthermore, the audio signal of GSM may embed cipher blocks and hashing hash for additional security. The use of the least significant bit (LSB) method creates a strong correlation between images. The results indicate that the suggested method is effective and enhances performance by securely delivering cipher blocks embedded in audio signals. However, the embedding via LSB in audio tends to be vulnerable to many forms of manipulation or noise. For example, if the audio undergoes compression, re-sampling, and filtering or is played through systems that alter bits, the hidden cipher blocks may be damaged or lost. Thus, this hinders robustness [45].

1.1.4. Image encryption based on steganography methods

Steganography is one of the image encryption techniques that hide information inside images. It is often used in multimedia communication [46]. El-Khamy et al. [46] presented a method of hybrid DNA encoding that uses Choquet's fuzzy integral sequences for security enhancement. The initial phase takes place through some distortion of the original image using a simple chaotic map, followed by encoding it. DNA bases (AT, CG, GC, and TA) are used to form four encoded images. A sequence of Choquet's fuzzy integral is simultaneously generated, DNA-encoded, and transformed into four pseudorandom sequences. They use a complementary DNA XOR rule guided by a code to diffuse the DNA-encoded image sequences. The gained images are then fused together, followed by encryption, with the help of wavelet fusion. A new steganography technique is applied to enhance security further. It successfully merges encryption with steganography to ensure data security. However, the complexity overhead of the proposed method due to the multiple layers (chaotic map, DNA coding, fuzzy integral sequences, diffusion, wavelet fusion, splitting, embedding etc.) introduces significant computational cost in both time and memory. This might be nontrivial, especially for large images or high-throughput applications [46].

Image steganography refers to the technique that helps in resisting the statistical steganalysis attack. The steganalysis techniques question the safety of steganography. They do this by locating the disguised messages in the images, thereby revealing the message and estimating its size [47]. As image steganography becomes more popular for hiding secret data, image steganalysis has emerged as the countermeasure. This method uses a variety of image processing tools such as cropping, filtering, and blurring to detect and extract, neutralize, and destroy any hidden data in the image [48]. The deep learning techniques used for steganalysis change with the data type and set of tools that we use. Every data type has unique statistical properties, the author state, whereas every steganography technique hides secret information differently. Steganography refers to a method of concealing information in plain sight and enables information to be embedded in images, speech, or any other data. For using image steganography, one may use the approach of LSB embedding or spatial domain techniques. In the same way, one could use a spread spectrum or echo hiding techniques for speech steganography. Deep learning approaches must be calibrated for all data and cover type and fine-tuned accordingly to work effectively [49].

1.1.5. Image encryption using visual cryptography methods

Visual cryptography (VC) is a technique of encrypting images that relies on the principle of decomposing the secret image into encrypted images (shares) or shadows such that by overlapping a specified number of shares, the original image is recovered [50]. Numerous schemes are employed in this encryption, including but not limited to binary, color images, segment-based visual cryptography, extended visual cryptography, flip-based visual cryptography, hierarchical visual cryptography, and threshold visual cryptography [51]. The primary use of VeraCrypt in authentication systems is to verify users' identities and limit unauthorized access to systems [51]. Many researchers have integrated visual cryptography with biometrics to improve the security and reliability of authentication systems [52–54].

1.2. Comparisons among image encryption techniques

In this section, a comparison among image encryption techniques will be covered. A comparison among hash, symmetric, and asymmetric ciphers is presented in Table 1.

As shown in Table 1, the comparison among these three ciphers shows that each cipher is useful and important in its application. Hash may be used in password storage and authentication [55], digital signatures [56], cryptographic protocols (e.g., TLS/SSL) [57], data fingerprinting [58], digital forensics [59], and load balancing and caching [60].

Symmetric ciphers may be used in real-life applications such as authentication [61], data storage protection [62], backup and disaster recovery [63], digital rights management (DRM) [64], wireless communication [65], and secure internet transactions [66, 67]. Asymmetric ciphers may be used in real-life applications such as blockchain [68] and file encryption [69].

Table 2 shows a comparison between steganography and cryptography according to many factors.

As shown in Table 2, steganography and cryptography are important techniques in real-life applications. Steganography may be

Table 1
A comparison among hash, symmetric, and asymmetric ciphers

Algorithm	Hash	Symmetric	Asymmetric
No. of keys	0	1	2
Key length	256 bits	128 bits	2048 bits
Common algorithms	SHA	AES	RSA
Key management	N/A	Big issue	Easy and secure
Impact of key compromise	N/A	Loss for both sender and receiver	Only loss for the owner of asymmetric
Speed	Fast	Fast	Slow
Complexity	Medium	Medium	High
Examples	SHA-224, SHA-256, SHA-384, SHA-512	AES, Blowfish, RC4, 3DES	RSA, ECC, DSA

Table 2
A comparison between steganography and cryptography

Key point	Steganography	Cryptography
Supported security principles	Authentication, confidentiality	Data integrity, confidentiality, authentication, and nonrepudiation
Target	Communication	Data security and protection
Methods	Transform domain, spatial domain, model-based and ad-hoc	Substitution, transposition, block ciphers, stream ciphers
Basic	Cover writing with multimedia	Encryption
Types of attacks	Steg-analysis	Cryptanalysis
Relies in	Key	Not specific parameters
Application	Multimedia	Text file
Popularity	Not frequent	Widely used

used in data storage and protection [70], educational content protection [71], blockchain and cryptocurrency [72], embedded systems and IoT [73], medical data protection [74], banking and financial sector [75], and digital watermarking [76].

2. The Influence of AI on the Accuracy and the Effectiveness of Image Encryption Techniques

In this section, many points will be covered.

2.1. AI in key generation

In this subsection, we will demonstrate how AI methods such as deep learning and neural networks are being applied to create or refine encryption keys, making encryption algorithms more efficient and secure.

Ananda Priya et al. [77] proposed a fresh Hill cipher variant that utilizes rhotrices and the corresponding algebra to encrypt feasible text and decipher ciphertext. The modernized Hill cipher technique employs an AI to generate its key matrices. It also uses matrix operations to encrypt the plaintext and decrypt the ciphertext. The enhanced edition of Hill cipher is more dependable and accurate compared to basic cipher that refers to the power of AI in key generation processes [77].

Ding et al. [78] used deep learning to improve stream ciphers for the encryption and decryption of medical images to protect patient privacy. The key generation system known as DeepKeyGen uses deep learning to generate a private key for stream cipher encryption. DeepKeyGen utilizes generated adversarial networks (GANs) to produce keys that are further improved through a transformation domain by tweaking the "style" of the keys. Therefore, the GAN produces effective private keys. The system transfers an input image to a secured key. The evaluation in this study uses three datasets: Montgomery County chest X-ray, ultrasonic brachial plexus, and BraTS18. According to the findings and security analysis, DeepKeyGen can be leveraged for generating secure private keys that function at a higher security level. However, the high overhead of training and computation due to DeepKeyGen learns the mapping and generates private keys using a GAN. It takes a lot of computational resources, training time, stability problems, and hyperparameter tuning to train GANs. This might get costly for medical photos, which can be huge, 3D, etc. When compared to more straightforward stream cipher- or PRNG-based key generators, the generation process's runtime at inference may also be important.

In addition, Naipaul said that secure algorithms for key agreements such as public key cryptography, the Diffie–Hellman key exchange, and elliptic curve cryptography can be used for secure sharing of AI models. The presented technique is secure and efficient in its key generation and key replacement processes. Consequently, the proposed approach safeguards the confidentiality and integrity of the AI model during sharing. However, it introduces substantial computational overhead and implementation complexity, which may affect scalability and performance [79].

In addition, others have proposed a tactical option to save cryptographic keys to reduce the complex storage and distribution process. Kuznetsov et al. [80] studied different generation methods of biometric keys using deep learning models. They focused on the use of convolutional neural networks for extracting face features.

Cryptographic extractors based on a code help in filtering out the extracted features. To evaluate the effectiveness of the models and extractors, researchers will look at type 1 and 2 errors. Studies show that by fine-tuning their algorithm, the error rate can be reduced. Consequently, the keys produced may have the potential to be used for biometric authentication. The effectiveness and performance assurance of the solution can be post-quantum secured by code-based cryptographic extractors. The study reveals that advanced biometric data and deep learning can help in designing secure, efficient, and user-friendly authentication and encryption protocols. However, variability in biometric traits and the presence of noise in the biometric data (such as face images) can influence the efficacy of the systems. It is difficult to ensure reproducible cryptographic keys from the data. The paper reports error rates. However, if environmental or capture conditions change, performance can degrade rapidly.

As stated above, AI has affected cryptography key generation as it led to new and novel key generation techniques. Here is an overview of its impact.

Smarter feature extraction: neural networks, which are part of AI, can discover complex patterns in biometrics (such as facial images or fingerprints) to produce unique and secure keys.

1) **Better randomness:** AI algorithms excel at creating cryptographic keys with a strong level of randomness and unpredictability, which makes them more difficult to break.
2) **Improved efficiency:** by fine-tuning algorithms and parameters, AI makes the key generation process more efficient and reduces errors.
3) **Post-quantum security:** AI supports the use of post-quantum cryptographic techniques, ensuring keys remain secure even against the power of quantum computing.
4) **Flexibility and scalability:** AI-powered methods can scale and adapt to various needs, from securing IoT devices to enabling secure communication and AI model sharing.

AI-based cryptographically secure key generation has ushered in a new and future-ready era of smarter and stronger keys. Many case studies demonstrate the significance of AI in key generation such as the following:

Case study 1: using biometric AI keys to secure patient data in a Swedish hospital.

Context: security of medical data was becoming a major concern at a contemporary hospital in Stockholm. Electronic health records needed to be instantly accessible to doctors, but password systems were cumbersome and frequently forgotten. The hospital's IT security team was concerned regarding data breaches in the meantime.

AI-driven solution: to deploy a deep learning-based biometric key generation system, the hospital teamed up with a nearby AI business. Physicians used facial recognition to authenticate instead of passwords. A cryptographic key, a secure string used to encrypt and decrypt patient files, was created by an AI model using distinctive face traits. To preserve anonymity, the system included a "fuzzy extractor," which produced the same key even when there were minor facial differences (such as changed lighting or glasses).

Result:

No need to reset their passwords; doctors could log in in just 2 s.

Only helper data that could not rebuild faces were saved, not raw biometric data.

IT reported no security problems involving illegal access after six months.

Case study 2: voice biometrics and AI are used on college campuses to provide secure exam access.

Context: during online tests, impersonation increased at an Indian university. Students were utilizing credentials that had been stolen to log in as one another. Instead of using a password, the exam board sought a method to link access to a student's true identity.

AI-powered solution: they implemented a speech biometric system powered by AI. Students read aloud a random statement prior to every exam. Vocal patterns were processed by a deep neural network, which produced a speaker-specific cryptographic key. Only the correct voice could access the exam because of this key, which encrypted the content and could only be decrypted if the student repeated the authentication.

Result:

The rate of impersonation decreased by 95%.

The students reported few disruptions.

Because of the model's tolerance, the system functioned even when there were minor colds or accent changes.

2.2. AI in attacks

In this subsection, we will elaborate how AI is also being used to crack encryption systems. It will provide a detailed look at the constant battle between making strong encryption and making methods to crack it.

Recently, Olaniyan presented research focuses on the future of cryptography in the era of quantum computing and AI. The study delves into the threats that quantum computing and AI-driven cryptanalysis pose to encryption standards such as AES. Quantum algorithms, specifically Grover's and Shor's, can reduce the time to break encryption drastically, and AES can be compromised. Simultaneously, the advanced pattern recognition and anomaly detection capabilities of AI provide new opportunities to exploit the vulnerabilities of a cryptography algorithm, especially machine learning-based side-channel attacks [81].

CAPTCHA is an authentication method that is used to distinguish humans from bots and prevent the bots from passing the systems. However, with an AI technique, it is easy to recognize the pattern and crack the systems. von Ahn et al. [82] introduced a new category of challenging problems that can enhance security measures. Similar to how cryptographic research has advanced algorithms for factoring and discrete logarithms, they aim to use difficult AI problems not only to improve security but also to drive progress in AI. They proposed two types of AI problems as the foundation for constructing CAPTCHAs and demonstrated that solving these problems can also enable steganographic communication. This creates a win–win scenario: either the problems remain unsolvable, providing a reliable way to distinguish humans from machines, or they are solved, unlocking new methods for covert communication in certain channels.

In addition, others presented a low-cost method for performing an AI-based chosen-plaintext attack that takes advantage of the open-source nature of popular CAPTCHA libraries. Using a deep learning model trained on a standard personal computer, this method can effectively break CAPTCHAs generated by two libraries. This poses a serious security risk, especially for small businesses that depend on these open-source CAPTCHA solutions [83].

In brief, AI plays a dual role in encryption usage. This reinforcement is strengthening sturdier and more secure systems on one side. It turns out that Apple's own software is being exploited to undermine this very strengthened apparatus as objective reinterpretation shows. The use of machine learning to run malware and malicious activity on encrypted data could locate flaws and patterns that other methods do not find. AI can simplify side-channel attacks by interpreting cues such as power consumption or electromagnetic signals to discern encryption keys. The use of deep learning to predict probable keys enhances brute-force techniques, making them faster and more effective in general.

The constant tug-of-war:

1) Improving encryption: developers are using AI to make encryption smarter and more adaptable, helping systems resist attacks by testing for vulnerabilities more thoroughly.
2) Growing threats: as AI improves, attackers may use it to exploit weaknesses in legacy encryption schemes and even challenge next-generation schemes such as quantum-resistant encryption.
3) Ethical dilemmas: the use of AI to crack encryption raises fundamental questions, especially when governments, hackers, or surveillance programs misuse it.

This constant push-and-pull between hackers and engineers is creating new innovations in cryptography. It also highlights the need to balance it with ethical usage of AI. The following case study proves this:

Case study: UK CEO targeted by Deepfake voice attack.

Context: in 2023, a German-sounding CEO called a UK-based energy company and urgently requested a €220,000 money transfer for a covert transaction. The tone, accent, and urgency of the call all matched, making it plausible.

AI-driven attack: the CEO's voice from YouTube appearances and public speeches was synthesized by hackers using AI voice cloning technologies. The finance officer was forced to comply by the AI-generated voice, which provided precise instructions and even insisted on confidentiality.

Result:

The money was transferred within an hour.

The real CEO knew nothing about it.

The attackers vanished, leaving only a Deepfake trail.

2.3. AI-driven optimization

First, we determine whether it is possible to improve and adapt existing encryption methods with the help of AI. Further, we will explain this point.

Yusuf et al. [84] recently highlighted the practical issues and benefits of introducing AI into current encryption systems. The study recommended expanding the system to accommodate the increase in operational activities and function with the older system. A blended approach is essentially a mix of conventional encryption and AI-powered encryption methods. Small- and medium-sized businesses (SMBs) can ensure the security of their financial data with an adaptive digital transformation strategy. Findings show that basic encryption algorithms are still relevant today. If we just depend on those algorithms, there can be no security in the future. AI-based solutions help in detecting incidents in real time and can be scaled according to a threat's intensity. In the future, secure financial transactions will depend on homomorphic encryption, quantum-resistant algorithms, and other advanced technologies [84].

Furthermore, various researchers studied encryption methods such as homomorphic encryption and secure multiparty computation to evaluate whether biometrics against new threats are safe enough. The research further illustrates how AI can enhance encryption and efficiency and how machine learning can assist in discovering and correcting security vulnerabilities. The paper looks at how different biometrics such as fingerprint scanning and facial recognition can enhance security in payment systems. It studies their impact using data and real-world cases. This study shows how encryption and AI can make financial exchanges safer and can protect consumers better [85].

AI enhances encryption by making algorithms efficient and enabling them to adapt to changing data patterns quickly. It can pinpoint vulnerabilities, foresee potential dangers, and modify encryption techniques on-the-fly to maintain robust and dependable security as data evolve.

Case study: AI improves delivery paths for a Lisbon family-owned bakery.

Context: Participant A and her two sons run a small bakery in the center of the city. Every morning, they begin their deliveries early, bringing fresh bread and pastries to more than 40 cafés. However, unpredictable traffic, last-minute orders, and increasing fuel costs made daily delivery management challenging. Participant B, the eldest son, often stayed up late each night planning the optimal delivery routes—a process that took him nearly 2 h.

AI-driven attack: looking for a smarter way, they teamed up with a local AI startup. The new system used past delivery data, live traffic updates, and café order trends to automatically calculate the most efficient delivery routes by doing in seconds what João used to spend hours on. It relied on advanced AI techniques such as reinforcement learning to keep improving the plan each day.

The impact:

Participant B's planning time dropped from 2 h to just a couple of minutes.

Their vans drove 15% fewer kilometers, saving on fuel and wear-and-tear.

Best of all, they could take on 10 new café clients without adding another vehicle.

3. Challenges and Future Perspectives

This section sheds light on various future methods for enhancing Solent's pledge for developing a sustainable region.

3.1. Scalability and efficiency

Security and efficiency are issues when it comes to scaling encryption to large datasets or high-resolution images. We will discuss those challenges in this subsection.

Computational overhead: encrypting a large quantity of data can consume lots of computer power and memory. This can slow down a task such as real-time processing [86].

1) Delays: the data sizes have been increasing, and it has become difficult to encrypt and decrypt without compromising on the delays, especially in delay-sensitive applications [87].
2) Energy usage: the heavy processing needs can lead to higher energy consumption, posing challenges for battery-powered devices or large data centers [88].
3) Security risks: encryption needs to scale without security weakening, or larger datasets will reveal patterns or weaknesses in the encryption [89].
4) Flexibility issues: the variation in encryption suitable for various file types, resolution, and kind of data complicates standardization [90].
5) Costs: when scaling, often there are extra hardware, software, and maintenance costs, which a smaller organization will not likely afford [91].
6) Algorithm efficiency: a lot of traditional cryptographic techniques were never meant for immense overloads. Therefore, innovativeness is important to guarantee effectiveness and safety [92].

Encryption technology should be innovative and efficient enough to allow hardware acceleration and parallel processing.

3.2. Standardization and interoperability

Image encoding standardization is based on the interoperability

of techniques across platforms. We will present benchmarks for image encryption techniques in this direction. It is needed to standardize image encryption standards so that it can be compatible with anything and everything. It is easier to implant technology, and it works across devices. It helps in making it easier and keeps everything secure. By being thoroughly tested, these standards are approved to meet tough security requirements that help adoption. Through simple rules, it helps in creating a well-connected, safe, and user-friendly online community that can encourage better connections with technology [93].

3.3. Post-quantum security

In this direction, we will present some suggestions on how image encryption can evolve to deal with the threat posed by quantum computing and the threat to classical cryptographic methods. As quantum computing advances and poses challenges to traditional cryptographic methods, image encryption will evolve in several keyways [94–100]:

1) Quantum-resistant algorithms: image encryption will increasingly rely on new algorithms that can resist quantum attacks, such as lattice-based or hash-based methods, which will either replace or supplement older techniques.
2) Hybrid encryption approaches: we will see a smooth transition to hybrid systems combining classical and quantum-resistant encryption. Such a thinking will be compatible with the existing system and simultaneously prepare for a secure future with quantum.
3) Lightweight encryption: as IoT sensors and smartphones manage more and larger images, encryption will have to be agile, lighter, and efficient but strong enough for safe transmission.
4) AI-driven encryption: AI plays a key role in making encryption better by exposing vulnerabilities in encryption, optimizing security measures, and adapting encryption methods to counter new threats such as quantum computing.
5) Quantum key distribution (QKD): quantum encryption algorithms (QKD) will be increasingly popular because they use "quantum mechanics" for the exchange of cryptographic keys.
6) More layered encryption: to defend our sensitive data against both new quantum threats and the attacks on data that we have today, experts are using multilayered encryption systems, which add an extra layer or two for good measure.
7) Global standards and cooperation: governments and organizations will focus on creating global standards for quantum-resistant encryption to ensure smooth integration, reliability, and broad adoption.
8) Quantum-specific encryption: to mitigate risk and future-proof the latest encryption proposals against quantum attacks, advanced encryption methods are in the works. As quantum computing matures, encryption methods are created for quantum computing environments, facilitating the secure storage and transmission of images in quantum computing environments.

Image encryption will adapt to quantum attacks in the future to protect sensitive data and images through a variety of approaches, as discussed above.

4. Conclusion

This paper analyzes image encryption with the latest research and development related to image encryption in detail. To the best of our knowledge, it is the first comprehensive survey on image encryption from the perspective of AI. This paper compares encryption techniques in detail. It shows the strengths and weaknesses of each method with respect to several factors. As one investigates on how the encryption methods can be improved through AI, it will become obvious as to how efficiency and accuracy can be enhanced. The key generation, attack detection and defense, and optimization of encryption algorithms using AI enable them to operate better in the real world. Anyone interested in how AI could interact with image encryption researchers would benefit from the full study.

In addition to showing the current state of the affairs, this paper discusses the issues and future scope of image encryption, especially in the aspect of AI. Researchers can get useful information from such dialogues, which can assist the researchers toward deciding the course of their future research. The review considers the emerging threats to security and the need for new, better, efficient, and scalable encryption implementations to deal with them. Future research may involve utilizing AI for image encryption among other applications. In the future, a new encryption scheme will be more secure and flexible with real-time applications. This study will not only pave the way for future research, but it can also serve as a tool to address tomorrow's challenges in image encryption.

Recommendations

The findings revealed that traditional image encryption methods are increasingly inadequate against evolving cyber threats, and AI integration offers significant security enhancements but faces implementation complexity and standardization challenges. Therefore, comprehensive training programs on AI-enhanced cryptography for cybersecurity professionals and researchers are recommended. Because AI-driven encryption systems demonstrate superior resistance to attacks and adaptability to emerging threats, organizations are recommended to adopt hybrid approaches that gradually integrate AI components into existing encryption infrastructure. This study shows that AI-enhanced encryption will be crucial for future security applications, particularly in post-quantum environments. Therefore, immediate investment in developing standardized frameworks for AI-enhanced image encryption and quantum-resistant algorithms is recommended to ensure long-term security viability across different platforms and applications.

Acknowledgement

The authors are grateful to the Department of Cyber Security and Department of Software Engineering at Amman Arab University, Amman, Jordan, for their institutional support and access to research resources.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Dyala Ibrahim: Conceptualization, Methodology, Software, Validation, Investigation, Writing – original draft, Writing – review & editing, Supervision, Project administration. **Omar Isam Al Mrayat:** Methodology, Software, Validation, Investigation, Writing – original draft, Supervision, Project administration. **Ahmad Reda Alzighaibi:**

Formal analysis, Writing – original draft, Visualization. **Hasan Hashim:** Writing – original draft, Visualization. **El-Sayed Atlam:** Writing – original draft, Visualization.

References

[1] Man, Z., Li, J., Di, X., Liu, X., Zhou, J., Wang, J., & Zhang, X. (2021). A novel image encryption algorithm based on least squares generative adversarial network random number generator. *Multimedia Tools and Applications*, *80*(18), 27445–27469. https://doi.org/10.1007/s11042-021-10979-w

[2] Popek, G. J., & Kline, C. S. (1979). Encryption and secure computer networks. *ACM Computing Surveys*, *11*(4), 331–356. https://doi.org/10.1145/356789.356794

[3] Ma, H., & Zhang, Z. (2020). A new private information encryption method in Internet of Things under cloud computing environment. *Wireless Communications and Mobile Computing*, *2020*(1), 8810987. https://doi.org/10.1155/2020/8810987

[4] Hellman, M. (1978). An overview of public key cryptography. *IEEE Communications Society Magazine*, *16*(6), 24–32. https://doi.org/10.1109/MCOM.1978.1089772

[5] Kaur, M., Singh, S., & Kaur, M. (2021). Computational image encryption techniques: A comprehensive review. *Mathematical Problems in Engineering*, *2021*(1), 5012496. https://doi.org/10.1155/2021/5012496

[6] SaberiKamarposhti, M., Ghorbani, A., & Yadollahi, M. (2024). A comprehensive survey on image encryption: Taxonomy, challenges, and future directions. *Chaos, Solitons & Fractals*, *178*, 114361. https://doi.org/10.1016/j.chaos.2023.114361

[7] Ahmadi, M., Kaur, J., Rani Nayak, D., Nutan, R., Taw, S., & Afaq, Y. (2023). A review of various symmetric encryption algorithms for multiple applications. In *Proceedings of the KILBY 100 7th International Conference on Computing Sciences 2023*, 1–6. http://dx.doi.org/10.2139/ssrn.4491217

[8] Ubochi Nwamouh, C., Olaniyi Sadiq, B., Ukagwu, K. J., & Nnamchi, S. N. (2023). A comparative analysis of symmetric cryptographic algorithm as a data security tool: A survey. *Journal of Science and Technology Research*, *5*(3), 144–168. https://doi.org/10.5281/zenodo.8313097

[9] Al-Zabin, L. R., Al-Wesabi, O. A., Al Hajri, H., Abdullah, N., Khudayer, B. H., & Al Lawati, H. (2023). Probabilistic detection of indoor events using a wireless sensor network-based mechanism. *Sensors*, *23*(15), 6918. https://doi.org/10.3390/s23156918

[10] Hussien, R. A., Radhi, S. S., Rashid, F. F., Abdulla, E. N., & Abass, A. K. (2024). Design and performance analysis of secure optical communication system by implementing Blowfish cipher algorithm. *Results in Optics*, *16*, 100708. https://doi.org/10.1016/j.rio.2024.100708

[11] Cahyani, A. P., & Susanto, A. (2023). A good result for Blowfish image encryption based on Stepic. *Advance Sustainable Science, Engineering and Technology*, *6*(1), 0240107. https://doi.org/10.26877/asset.v6i1.17332

[12] Dhamala, N., & Acharya, K. P. (2024). A comparative analysis of DES, AES and Blowfish based DNA cryptography. *Adhyayan Journal*, *11*(11), 69–80. https://doi.org/10.3126/aj.v11i11.67080

[13] Muhammed, R. K., Aziz, R. R., Hassan, A. A., Aladdin, A. M., Saydah, S. J., Rashid, T. A., & Hassan, B. A. (2024). Comparative analysis of AES, Blowfish, Twofish, Salsa20, and Chacha20 for image encryption. *Kurdistan Journal of Applied Research*, *9*(1), 52–65. https://doi.org/10.24017/science.2024.1.5

[14] Ubaidullah Bokhari, M., & Shallal, Q. M. (2016). A review on symmetric key encryption techniques in cryptography. *International Journal of Computer Applications*, *147*(10), 43–48. https://doi.org/10.5120/ijca2016911203

[15] Sajitha, A. S., & Shobha Rekh, A. (2022). Review on various image encryption schemes. *Materials Today: Proceedings*, *58*, 529–534. https://doi.org/10.1016/j.matpr.2022.03.058

[16] Kuppuswamy, P., Al Khalidi Al-Maliki, S. Q. Y., John, R., Haseebuddin, M., & Meeran, A. A. S. (2023). A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm. *Bulletin of Electrical Engineering and Informatics*, *12*(2), 1148–1158. https://doi.org/10.11591/eei.v12i2.4967

[17] Alemami, Y., Mohamed, M. A., & Atiewi, S. (2023). Advanced approach for encryption using advanced encryption standard with chaotic map. *International Journal of Electrical and Computer Engineering*, *13*(2), 1708. https://doi.org/10.11591/ijece.v13i2.pp1708-1723

[18] Ge, B., Shen, Z., & Wang, X. (2023). Symmetric color image encryption using a novel cross–plane joint scrambling–diffusion method. *Symmetry*, *15*(8), 1499. https://doi.org/10.3390/sym15081499

[19] Duan, G., & Li, S. (2023). Verifiable and searchable symmetric encryption scheme based on the public key cryptosystem. *Electronics*, *12*(18), 3965. https://doi.org/10.3390/electronics12183965

[20] Lu, Q., Yu, L., & Zhu, C. (2022). Symmetric image encryption algorithm based on a new product trigonometric chaotic map. *Symmetry*, *14*(2), 373. https://doi.org/10.3390/sym14020373

[21] Huang, L., & Gao, H. (2024). Multi-image encryption algorithm based on novel spatiotemporal chaotic system and fractal geometry. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *71*(8), 3726–3739. https://doi.org/10.1109/TCSI.2024.3407809

[22] Rehman, M. U. (2024). Quantum-enhanced chaotic image encryption: Strengthening digital data security with 1-D sine-based chaotic maps and quantum coding. *Journal of King Saud University - Computer and Information Sciences*, *36*(3), 101980. https://doi.org/10.1016/j.jksuci.2024.101980

[23] Kumar, S., Singh, B. K., Akshita, Pundir, S., Batra, S., & Joshi, R. (2020). A survey on symmetric and asymmetric key based image encryption. In *2nd International Conference on Data, Engineering and Applications*, 1–5. https://doi.org/10.1109/IDEA49133.2020.9170703

[24] Ye, G., Jiao, K., Wu, H., Pan, C., & Huang, X. (2020). An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem. *International Journal of Bifurcation and Chaos*, *30*(15), 2050233. https://doi.org/10.1142/S0218127420502338

[25] Chennamma, H. R., & Madhushree, B. (2023). A comprehensive survey on image authentication for tamper detection with localization. *Multimedia Tools and Applications*, *82*(2), 1873–1904. https://doi.org/10.1007/s11042-022-13312-1

[26] Thanh, T. M., & Iwakiri, M. (2014). Incomplete encryption based on multi-channel AES algorithm to digital rights management. In *Knowledge and Systems Engineering: Proceedings of the Fifth International Conference*, *1*, 199–211. https://doi.org/10.1007/978-3-319-02741-8_18

[27] Ningthoukhongjam, T. R., Devi Heisnam, S., & Singh Khumanthem, M. (2024). Medical image encryption through chaotic asymmetric cryptosystem. *IEEE Access*, *12*, 73879–73888. https://doi.org/10.1109/ACCESS.2024.3404088

[28] Mohammed, Z. A., Gheni, H. Q., Hussein, Z. J., & Al-Qurabat, A. K. M. (2024). Advancing cloud image security via AES algorithm enhancement techniques. *Engineering, Technology & Applied Science Research*, *14*(1), 12694–12701. https://doi.org/10.48084/etasr.6601

[29] Gao, F. (2019). Data encryption algorithm for e-commerce platform based on blockchain technology. *Discrete and Continuous Dynamical Systems - Series S*, *12*(4&5), 1457–1470. https://doi.org/10.3934/dcdss.2019100

[30] Ren, L., & Zhang, D. (2025). Integrating visual cryptography for efficient and secure image sharing on social networks. *Applied Sciences*, *15*(8), 4150. https://doi.org/10.3390/app15084150

[31] Khan, P. W., & Byun, Y. (2020). A blockchain-based secure image encryption scheme for the industrial Internet of Things. *Entropy*, *22*(2), 175. https://doi.org/10.3390/e22020175

[32] Salim, K. G., Al-alak, S. M. K., & Jawad, M. J. (2021). Improved image security in Internet of Thing (IoT) using multiple key AES. *Baghdad Science Journal*, *18*(2), 0417. https://doi.org/10.21123/bsj.2021.18.2.0417

[33] Al Saffar, N. F. H., Al-Saiq, I. R., & Abo Alsabeh, R. R. M. (2022). Asymmetric image encryption scheme based on Massey Omura scheme. *International Journal of Electrical and Computer Engineering*, *12*(1), 1040. https://doi.org/10.11591/ijece.v12i1.pp1040-1047

[34] Huang, X., Dong, Y., Zhu, H., & Ye, G. (2022). Visually asymmetric image encryption algorithm based on SHA-3 and compressive sensing by embedding encrypted image. *Alexandria Engineering Journal*, *61*(10). https://doi.org/10.1016/j.aej.2022.01.015

[35] Chen, Z., & Ye, G. (2022). An asymmetric image encryption scheme based on hash SHA-3, RSA and compressive sensing. *Optik*, *267*, 169676. https://doi.org/10.1016/j.ijleo.2022.169676

[36] Rao, S. K., Nishchal, N. K., & AlFalou, A. (2024). Optical asymmetric image encryption using vectorial light field encoding. *Optics Communications*, *554*, 130097. https://doi.org/10.1016/j.optcom.2023.130097

[37] Liu, S., & Ye, G. (2023). Asymmetric image encryption algorithm using a new chaotic map and an improved radial diffusion. *Optik*, *288*, 171181. https://doi.org/10.1016/j.ijleo.2023.171181

[38] Du, S., & Ye, G. (2023). IWT and RSA based asymmetric image encryption algorithm. *Alexandria Engineering Journal*, *66*, 979–991. https://doi.org/10.1016/j.aej.2022.10.066

[39] Shehab, M., & Alzabin, L. R. (2025). Evaluating the effectiveness of stealth protocols and proxying in hiding VPN usage. *Journal of Computational and Cognitive Engineering*, *4*(2), 186–194. https://doi.org/10.47852/bonviewJCCE42023642

[40] Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., & Kolhatin, A. (2021). Performance analysis of cryptographic hash functions suitable for use in blockchain. *International Journal of Computer Network & Information Security*, *13*(2), 1–15. https://doi.org/10.5815/ijcnis.2021.02.01

[41] Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010). A hash-based image encryption algorithm. *Optics Communications*, *283*(6), 879–893. https://doi.org/10.1016/j.optcom.2009.10.106

[42] Sheng, L., & Li, C. (2023). Weakly supervised coarse-to-fine learning for human action segmentation in HCI videos. *Multimedia Tools and Applications*, *82*(9), 12977–12993. https://doi.org/10.1007/s11042-022-13792-1

[43] Li, H., Zhang, L., Cao, H., & Wu, Y. (2023). Hash based DNA computing algorithm for image encryption. *Applied Sciences*, *13*(14), 8509. https://doi.org/10.3390/app13148509

[44] Wang, X., Zhang, X., Gao, M., Tian, Y., Wang, C., & Iu, H. H.-C. (2023). A color image encryption algorithm based on hash table, Hilbert curve and hyper-chaotic synchronization. *Mathematics*, *11*(3), 567. https://doi.org/10.3390/math11030567

[45] Chithra, P. L., & Aparna, R. (2023). Blockchain-based image encryption with spiral mapping and hashing techniques in dual level security scheme. *International Journal of Information and Computer Security*, *21*(1/2), 185. https://doi.org/10.1504/IJICS.2023.131100

[46] El-Khamy, S. E., Korany, N. O., & Mohamed, A. G. (2020). A new fuzzy-DNA image encryption and steganography technique. *IEEE Access*, *8*, 148935–148951. https://doi.org/10.1109/ACCESS.2020.3015687

[47] Yutia, S. N., Tyas, S. H. Y., & Haryadi, D. (2024). Trends in research and artificial intelligence methods for steganalysis—A systematic literature review (SLR). In *2024 International Conference on ICT for Smart Society*, 1–6. https://doi.org/10.1109/ICISS62896.2024.10751004

[48] Kuznetsov, A., Luhanko, N., Frontoni, E., Romeo, L., & Rosati, R. (2024). Image steganalysis using deep learning models. *Multimedia Tools and Applications*, *83*(16), 48607–48630. https://doi.org/10.1007/s11042-023-17591-0

[49] Kheddar, H., Hemis, M., Himeur, Y., Megías, D., & Amira, A. (2024). Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions. *Neurocomputing*, *581*, 127528. https://doi.org/10.1016/j.neucom.2024.127528

[50] Ibrahim, D. R., Teh, J. S., & Abdullah, R. (2021). An overview of visual cryptography techniques. *Multimedia Tools and Applications*, *80*(21–23), 31927–31952. https://doi.org/10.1007/s11042-021-11229-9

[51] Ibrahim, D., Sihwail, R., Zainol Ariffin, K. A., Abuthawabeh, A., & Mizher, M. (2023). A novel color visual cryptography approach based on Harris hawks optimization algorithm. Symmetry, *15*(7), 1305. https://doi.org/10.3390/sym15071305

[52] Ibrahim, D. R., Abdullah, R., & Teh, J. S. (2022). An enhanced color visual cryptography scheme based on the binary dragonfly algorithm. *International Journal of Computers and Applications*, *44*(7),623–632. https://doi.org/10.1080/1206212X.2020.1859244

[53] Mohan, J., & R, D. R. (2021). Enhancing home security through visual cryptography. *Microprocessors and Microsystems*, *80*, 103355. https://doi.org/10.1016/j.micpro.2020.103355

[54] Bachiphale, P. M., & Zulpe, N. S. (2024). A comprehensive review of visual cryptography for enhancing high-security applications. *Multimedia Tools and Applications*, *84*(26), 31023–31045. https://doi.org/10.1007/s11042-024-20426-1

[55] Hasan, H. A., Al-Layla, H. F., & Ibraheem, F. N. (2022). A review of hash function types and their applications. *Wasit Journal of Computer and Mathematics Science*, *1*(3), 75–88. https://doi.org/10.31185/wjcm.52

[56] Fathalla, E., & Azab, M. (2024). Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations. *IEEE Access*, *12*, 175969–175987. https://doi.org/10.1109/ACCESS.2024.3485602

[57] Hamilton, M., & Marnane, W. P. (2016). Implementation of a secure TLS coprocessor on an FPGA. *Microprocessors and Microsystems*, *40*, 167–180. https://doi.org/10.1016/j.micpro.2015.10.009

[58] Akbar, M., Ahmad, I., Mirza, M., Ali, M., & Barmavatu, P. (2024). Enhanced authentication for de-duplication of big data on cloud storage system using machine learning approach. *Cluster Computing*, *27*(3), 3683–3702. https://doi.org/10.1007/s10586-023-04171-y

[59] Liu, G., He, J., & Xuan, X. (2021). A data preservation method based on blockchain and multidimensional hash for digital forensics. *Complexity*, *2021*(1), 5536326. https://doi.org/10.1155/2021/5536326

[60] Sankar, V., Bharanikumar, V., & Swaminathan, L. (2024). Dy-

namic load balancing and resource optimization algorithm for reverse proxy servers. In *2024 International Conference on Cognitive Robotics and Intelligent Systems*, 572–577. https://doi.org/10.1109/ICC-ROBINS60238.2024.10533888

[61] Avoine, G., Bingol, M. A., Carpent, X., & Yalcin, S. B. O. (2013). Privacy-friendly authentication in RFID systems: On sublinear protocols based on symmetric-key cryptography. *IEEE Transactions on Mobile Computing*, *12*(10), 2037–2049. https://doi.org/10.1109/TMC.2012.174

[62] Bandaru, V. N. R., Gayatri Sarman Kaligotla, V. S. H., Varma, U. D. S. P., Prasadaraju, K., & Sugumaran, S. (2024). A enhancing data security solutions for smart energy systems in IoT-enabled cloud computing environments through lightweight cryptographic techniques. *IOP Conference Series: Earth and Environmental Science*, *1375*(1), 012003. https://doi.org/10.1088/1755-1315/1375/1/012003

[63] Beretas, C. (2024). Information systems security, detection and recovery from cyber attacks. *Universal Library of Engineering Technology*, *1*(1), 27–40. https://doi.org/10.70315/uloap.ulete.2024.0101005

[64] Alhamalawy, D. M., Attiya, G. M., Abdoun, Z. M. A., & Mohamed, M. A. A. (2024). A comprehensive survey on digital rights management systems (DRM) and advanced encryption techniques. *Alryada Journal for Computational Intelligence and Technology*, *1*(1), 10–38. https://doi.org/10.21608/ajcit.2024.320988.1006

[65] Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., & Smirnov, O. (2024). Wireless network encryption: Stream ciphers, computational modeling, and security analysis. In A. L. Imoize, W. Montlouis, M. S. Obaidat, S. I. Popoola, & M. Hammoudeh (Eds.), *Computational modeling and simulation of advanced wireless communication systems* (pp. 379–402). CRC Press. https://doi.org/10.1201/9781003457428-16

[66] Mirtskhulava, L., Gulua, N., & Putkaradze, K. (2025). Enhancing mobile communication system security via neural cryptography applications. In *Smart Grid and Innovative Frontiers in Telecommunications: 8th EAI International Conference*, 145–156. https://doi.org/10.1007/978-3-031-78806-2_9

[67] Bashminova, D., Gergokov, M., & Ovchinnikov, V. (2024). Cryptography methods in protecting financial transactions. In *2024 IEEE 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University*, 1–5. https://doi.org/10.1109/ITMS64072.2024.10741926

[68] Chen, C.-L., Lim, Z.-Y., Xue, X., & Chen, C.-H. (2023). Special issue: Symmetric and asymmetric encryption in blockchain. *Symmetry*, *15*(2), 458. https://doi.org/10.3390/sym15020458

[69] Gundu, T., & Maduguma, K. (2024). Multi-key asymmetric cryptography: A model for preserving privacy in work-from-home environments. In *European Conference on Cyber Warfare and Security*, *23*(1), 287–295. https://doi.org/10.34190/eccws.23.1.2290

[70] Shidaganti, G., L, M. V., Vinay, M., & Patil, P. (2024). Enhancing data protection using cryptography and image steganography in cloud environment. In *2024 5th International Conference on Circuits, Control, Communication and Computing*, 93–99. https://doi.org/10.1109/I4C62240.2024.10748507

[71] Gurunath, R., & Samanta, D. (2021). A novel approach for semantic web application in online education based on steganography. *International Journal of Web-Based Learning and Teaching Technologies*, *17*(4), 1–13. https://doi.org/10.4018/IJWLTT.285569

[72] Takaoğlu, M., Özyavaş, A., Ajlouni, N., Alshahrani, A., & Alkasasbeh, B. (2021). A novel and robust hybrid blockchain and steganography scheme. *Applied Sciences*, *11*(22), 10698. https://doi.org/10.3390/app112210698

[73] Hassaballah, M., Hameed, M. A., Awad, A. I., & Muhammad, K. (2021). A novel image steganography method for industrial Internet of Things security. *IEEE Transactions on Industrial Informatics*, *17*(11), 7743–7751. https://doi.org/10.1109/TII.2021.3053595

[74] Shtayt, B. A., Zakaria, N. H., & Harun, N. H. (2021). A comprehensive review on medical image steganography based on LSB technique and potential challenges. *Baghdad Science Journal*, *18*(2), 47. https://doi.org/10.21123/bsj.2021.18.2(Suppl.).0957

[75] Sarjiyus, O., Baha, B. Y., & Garba, E. J. (2021). Enhanced security framework for internet banking services. *Journal of Information Technology and Computing*, *2*(1), 9–29. https://doi.org/10.48185/jitc.v2i1.162

[76] Abdalwahid, S. M. J., Hashim, W. A., Saeed, M. G., Altaie, S. A., & Kareem, S. W. (2024). Investigating the effectiveness of artificial intelligence in watermarking and steganography for digital media security. In *2024 21st International Multi-Conference on Systems, Signals & Devices*, 552–561. https://doi.org/10.1109/SSD61670.2024.10549272

[77] Ananda Priya, B., Gnanachandra, P., & Seenivasan, M. (2023). AI-driven innovations in cryptography: Enhancing key generation and security. *E3S Web of Conferences*, *399*, 08001. https://doi.org/10.1051/e3sconf/202339908001

[78] Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K.-K. R., & Qin, Z. (2022). DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption. *IEEE Transactions on Neural Networks and Learning Systems*, *33*(9), 4915–4929. https://doi.org/10.1109/TNNLS.2021.3062754

[79] Almalawi, A., Hassan, S., Fahad, A., & Khan, A. I. (2024). A hybrid cryptographic mechanism for secure data transmission in edge AI networks. *International Journal of Computational Intelligence Systems*, *17*(1), 24. https://doi.org/10.1007/s44196-024-00417-8

[80] Kuznetsov, O., Zakharov, D., & Frontoni, E. (2024). Deep learning-based biometric cryptographic key generation with post-quantum security. *Multimedia Tools and Applications*, *83*(19), 56909–56938. https://doi.org/10.1007/s11042-023-17714-7

[81] Majeed, N. D., Al-Askery, A. J., Hasan, F. S., & Abood, S. (2025). A survey on steganography and image encryption techniques. *Electrical Engineering Technical Journal*, *2*(1), 11–24. https://doi.org/10.51173/eetj.v2i1.13

[82] von Ahn, L., Blum, M., Hopper, N. J., & Langford, J. (2003). CAPTCHA: Using hard AI problems for security. In *Advances in Cryptology: International Conference on the Theory and Applications of Cryptographic Techniques*, 294–311. https://doi.org/10.1007/3-540-39200-9_18

[83] Yu, N., & Darling, K. (2019). A low-cost approach to crack python CAPTCHAs using AI-based chosen-plaintext attack. *Applied Sciences*, *9*(10), 2010. https://doi.org/10.3390/app9102010

[84] Yusuf, S. O., Echere, A. Z., Ocran, G., Abubakar, J. E., Paul-Adeleye, A. H., & Owusu, P. (2024). Analyzing the efficiency of AI-powered encryption solutions in safeguarding financial data for SMBs. *World Journal of Advanced Research and Reviews*, *23*(3), 2138–2147. https://doi.org/10.30574/wjarr.2024.23.3.2753

[85] Kuraku, C., Rajaram, S. K., Gollangi, H. K., Boddapati, V. N., & Patra, G. K. (2024). Advanced encryption techniques in biometric payment systems: A big data and AI perspective. *Library Progress International*, *44*(3), 2447–2458.

[86] Kshetri, N., Rahman, M. M., Rana, M. M., Osama, O. F., & Hutson, J. (2024). algoTRIC: Symmetric and asymmetric encryption algorithms for cryptography – A comparative analysis in AI era. *International Journal of Advanced Computer Science and Applications*, *15*(12), 1–14. https://doi.org/10.14569/IJACSA.2024.0151201

[87] Gnatyuk, S., Okhrimenko, T., & Proskurin, D. (2024). AI-based encryption system for secure UAV communication.

In *2024 IEEE 7th International Conference on Actual Problems of Unmanned Aerial Vehicles Development*, 93–98. https://doi.org/10.1109/APUAVD64488.2024.10765879

[88] Ramakrishna, D., & Ali Shaik, M. (2025). A comprehensive analysis of cryptographic algorithms: Evaluating security, efficiency, and future challenges. *IEEE Access*, *13*, 11576–11593. https://doi.org/10.1109/ACCESS.2024.3518533

[89] Rajasekar, V., Venu, K., Sharma, V., & Saracevic, M. (2023). Algorithmic strategies for solving complex problems in financial cryptography. In V. Seethalakshmi, R. K. Dhanaraj, S. Suganyadevi, & M. Ouaissa (Eds.), *Homomorphic encryption for financial cryptography: Recent inventions and challenges* (pp. 207–219). Springer. https://doi.org/10.1007/978-3-031-35535-6_10

[90] Chaudhary, P., & Kumar, V. (2024). A brief overview of cryptographic techniques: Encryption, decryption, RSA and more. *ShodhKosh: Journal of Visual and Performing Arts*, *5*(6), 331–335. https://doi.org/10.29121/shodhkosh.v5.i6.2024.3916

[91] Basu, A., Warzel, D., Eftekhari, A., Kirby, J. S., Freymann, J., Knable, J., …, & Jacobs, P. (2019). Call for data standardization: Lessons learned and recommendations in an imaging study. *JCO Clinical Cancer Informatics*, *3*, 1–11. https://doi.org/10.1200/CCI.19.00056

[92] Tellez, F., & Ortiz, J. (2024). Comparing AI algorithms for optimizing elliptic curve cryptography parameters in e-commerce integrations: A pre-quantum analysis. *International Journal of Advanced Computer Science and Applications*, *15*(6), 1539–1553. https://doi.org/10.14569/IJACSA.2024.01506153

[93] Mahalakshmi, K., & Nagarajan, S. (2025). Comprehensive review and analysis of image encryption techniques. *IEEE Access*, *13*, 109783–109813. https://doi.org/10.1109/ACCESS.2025.3578158

[94] Omshith, R., Balaji, V. P., Rahul, R. V., & U, K. (2024). Enhanced security measures for image privacy: Encryption perspectives. In *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things*, 493–497. https://doi.org/10.1109/IDCIoT59759.2024.10467544

[95] Glisic, S. (2024). Quantum vs post-quantum security for future networks: Survey. *Cyber Security and Applications*, *2*, 100039. https://doi.org/10.1016/j.csa.2024.100039

[96] Gharavi, H., Granjal, J., & Monteiro, E. (2024). Post-quantum blockchain security for the Internet of Things: Survey and research directions. *IEEE Communications Surveys & Tutorials*, *26*(3), 1748–1774. https://doi.org/10.1109/COMST.2024.3355222

[97] Karakaya, A., & Ulu, A. (2024). A survey on post-quantum based approaches for edge computing security. *WIREs Computational Statistics*, *16*(1), e1644. https://doi.org/10.1002/wics.1644

[98] Alnahawi, N., Müller, J., Oupický, J., & Wiesmaier, A. (2024). A comprehensive survey on post-quantum TLS. *IACR Communications in Cryptology*, *1*(2), 1–41. https://doi.org/10.62056/ahee0iuc

[99] Acharya, K., Gandhi, S., & Dalal, P. (2024). Cyber-security of IoT in post-quantum world: Challenges, state of the art, and direction for future research. In N. K. Chaubey & N. Chaubey (Eds.), *Advancing cyber security through quantum cryptography* (pp. 363–396). IGI Global. https://doi.org/10.4018/979-8-3693-5961-7.ch013

[100] Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In *2024 15th International Conference on Network of the Future*, 195–203. https://doi.org/10.1109/NoF62948.2024.10741441

How to Cite: Ibrahim, D., Al Mrayat, O. I., Alzighaibi, A. R., Hashim, H., & Atlam, E. (2025). Exploring Image Encryption Techniques: Challenges and Real-Life Application Insights with AI Influence. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE52026947