Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

PixelChain: A Blockchain Inspired Reversible Cryptographic Framework for Secure Image Encryption

Faizal Nujumudeen

faizalnr@gmail.com

University of Kerala

Research Article

Keywords: Image Encryption, Blockchain-inspired Cryptography, PixelChain, Reversible Encryption, NPCR, UACI, Secure Image Transmission, IoT Security

Posted Date: September 25th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11132326/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

PixelChain: A Blockchain Inspired Reversible Cryptographic Framework for Secure Image Encryption

Abstract: In the era of fast development of the multimedia communication, cloud computing and Internet of Things (IoT) applications, there is a growing need for lightweight image encryption algorithms that can provide both confidentiality and integrity while being reversible and efficient in calculation. While traditional chaos-, DNA-, ECC-, and blockchain-assisted encryption techniques offer robust security, several are too resource-intensive or dependent on external blockchain infrastructure or complex cryptographic operations, making them unsuitable for resource-constrained settings. To overcome these drawbacks, this paper introduces an encryption method called PixelChain Encryption (PCE) which is inspired by the blockchain framework with each one of the image pixels as a cryptographic block, connected by recursive chaining of SHA-256 hash and encrypted with a lightweight XOR-based keystream. Unlike conventional blockchain systems, the proposed method has only the chaining property of cryptography that does not involve any distributed ledgers, consensus mechanisms, and maintains reversibility with low computational complexity. The proposed framework was tested on two datasets of 500 images of the Wonders of the Worlds and Brain Tumour MRI using statistical, security and performance measures. Experiments confirm that the proposed method is well resistant to statistical and differential attacks: The average entropy is 7.996, NPCR is 99.61% and UACI is 50.01%, which is close to zero. The method also provides efficient processing with average encryption times of 42, 168 and 690 milliseconds for images of sizes 256×256, 512×512 and 1024×1024 respectively, and offers good tamper detection through local corruption of decrypted output images. A comparative analysis with the most recent chaos-, DNA-, ECC-, and blockchain-based methods of encryption shows that the proposed PixelChain framework offers competitive security and it has much lower computational complexity, which makes it a viable solution for secure image transmission in cloud computing, IoT, medical imaging, and digital forensic applications.

Keywords: *Image Encryption, Blockchain-inspired Cryptography, PixelChain, Reversible Encryption, NPCR, UACI, Secure Image Transmission, IoT Security.*

1. Introduction

The rapid development of digital imaging technology along with the increased use of multimedia communication over networks has greatly contributed to the need for secure image transmission and/or storage. The use of images is prevalent across multiple areas including, but not limited to, medical diagnosis, military surveillance, remote sensing and cloud-based applications; they can be very large in size, have large amounts of redundancy and contain a high degree of spatial correlation between adjacent pixels. For this reason, conventional encryption algorithms that have been developed for textual data typically will not be effective or optimal when applied directly to image data because they were not specifically designed for that purpose. Classical cryptographic frameworks, such as those based on Shannon's principles of confusion and diffusion [1], strive to hide the statistical relationships between pieces of data while providing excellent resistance to being subjected to cryptanalysis. Even though standard encryption methods (e.g., AES) offer excellent security, they do not directly utilize the unique structural features of image data; thus, several image encryption approaches have been established. These approaches typically leverage pixel-based techniques (i.e., permutation,

substitution, and transformation) to enhance both the confidentiality and performance of the image encryption process.

Out of these chaos-based encryption methods have recently received much interest because the nature of chaos makes them highly sensitive to changes in their initial conditions and randomly generate numbers like a computer's random generator [2]. Numerous other methods utilizing mixed chaotic systems and Josephus traversal methods have rapidly shown the ability to significantly increase the diffusion and confusion properties of encryption algorithms [7]. Additionally, various lightweight chaotic encryption models have been researched to address computational limitations within limited environments [6]; but despite these advancements, chaotic systems are generally very sensitive to parameters, produce poor results with finite precision values, and can suffer from specific statistics if the system has not been developed correctly. Additionally, as a method of strengthening image encryption methods, several researchers have started researching hybrid forms (chaos theory combined with advanced encoding methods such as DNA cryptography) using biological encoding theories to create very complex transformations and strong levels of security for the encrypted data [10]-[13]. While these hybrid encoding methods do provide improved security, they add considerable overhead and complexity to the computational processes used to create/encrypt the image data and therefore limit the real-time systems' ability to use them practically.

The blockchain research that has taken place recently has been concerned more with authenticity verification than direct encryption. To tackle this issue, Fida et al. [26] introduced a blockchain-based counterfeit detection system based on the use of distributed ledgers to ensure product authenticity and traceability. Even though blockchain is useful for verifying the integrity of the system, it is not used as an integral part of the cryptographic transformation. Blockchain Technology has come to be viewed as an effective way to provide a data integrity, immutability, and decentralized security framework. Due to the method of construction of a blockchain, where each block is linked cryptographically (with a digital signature) to its predecessor, there is a very strong ability to detect tampering and manage secure data. Recently, there have been attempts to incorporate blockchain frameworks into the areas of image encryption and sharing systems in both healthcare settings and the Internet of Things [16]-[18][20]. Most current approach’s view blockchain as an external infrastructure used for the purposes of securely storing and authenticating an image, rather than embedding some of the core principles of blockchain into the encryption process itself.

Despite much progress being made in the field of image encryption, there are still many challenges present with existing image encryption methods. Many schemes don't have any inherent ability to detect tampering and instead require the use of an external authentication layer. Many systems also have high computational complexity due to the use of hybrid designs that use multiple cryptographic primitives together to produce a result. Additionally, finding the right balance between security, efficiency, and reversibility is a continuing challenge in instances that require lossless reconstruction such as for medical images. In recent research, lightweight cryptographic frameworks for secure sharing of visual information have also been discussed. In their work, Nujumudeen et al. [31] introduced a visual cryptography approach relying on lightweight XOR-based operations to distribute color images without compromising security and ensuring low reconstruction share costs. The research presents evidence that by using lightweight XOR operations, a secure image protection system with low processing cost can be achieved, which is stimulating the need for reversible image encryption methods suitable for environments restricting resource use.

A new encryption framework must be developed that can provide high levels of structural dependency, security, and the ability to reverse operations at a minimal cost. The proposed

"PixelChain" encryption framework proposes to solve these problems by providing pixel level blockchain-style chains of data elements, which provide a new era of image cryptography through blockchain technology. In blockchain technology, the integrity and security of data elements are achieved through the chaining together of elements using a hash of the preceding element to create an unchangeable series of elements within a single block of content. Changing one block in the series causes a change in all subsequent blocks and as such, makes it easy to determine if any one block has been subject to unauthorized modification. In the proposed PixelChain framework, each pixel is logically linked through a recursive cryptographic hash chain. This chaining creates sequential dependency during keystream generation and strengthens diffusion during encryption. Unlike a conventional blockchain, modifying an encrypted pixel does not recursively modify subsequent ciphertext pixels; instead, the affected region becomes detectable during decryption through localized corruption.

The PixelChain system is a new type of image encryption that has a very different way of encrypting images than conventional systems do. Where traditional image encryption systems operate independently on each pixel or block, every pixel in the PixelChain system relies on all the other pixels in the image to determine its value. This increases the diffusion properties of the resulting encrypted image significantly. As a result, a small change made to the input image, encryption key, or initialization parameters will result in a large change in the output of the encrypted image. In addition, PixelChain's behaviour meets the statistical requirements for image encryption, including high NPCR and UACI values. High levels of NPCR and UACI are two indicators of resistance to differential attacks [3][4]. Additionally, the PixelChain system uses encryption techniques that guarantee that the data can be completely restored to its original form after being decrypted. This feature is critical in applications where any distortion of the image data could result in an incorrect diagnosis. Recent developments in secure transmission of images for medical purposes have demonstrated that an encryption system must not only maintain confidentiality of the data, but also maintain the fidelity of the data [22][23]. The PixelChain system provides a high level of security while still utilizing reversible operations.

The ability to defend against statistical and brute-force attacks is another vital component of contemporary image encryption; most advanced systems today will incorporate key derivation techniques, elliptic curve cryptography, and hybrid frameworks to increase their security [8][9]. However, while these methods are useful, they can also create additional workloads due to their high computational complexity which may restrict their use for real-time or resource-constrained applications. In order to protect smart non-fungible tokens (NFTs) in IoT environments, Wei and Liu [27] presented a lightweight blockchain architecture that uses hybrid secure functions. Their work shows how blockchain can be modified to lower computational costs without compromising integrity and traceability. This is indicative of the motivation for lightweight blockchain-inspired cryptographic approaches that are appropriate for constrained devices. Conversely, the proposed framework can achieve similar levels of security via a lightweight hashing technique that utilizes chaining to reduce processing overhead while maintaining robust levels of security. Additionally, by incorporating blockchain characteristics directly into the encryption process, this framework offers a different approach when compared to previously existing solutions that have used blockchain only for secure storage, access control, and distributed data sharing [19] – [21]. Previous works that addressed the increasing need for blockchains in image storage enhanced security at a system level, but did not introduce any changes to the encryption mechanism itself. The PixelChain framework fills this gap by embedding blockchain features (i.e., chaining, immutability, and tampering) into the core encryption algorithm.

The proposed method has extensibility and adaptability support; it can integrate advanced traversal patterns, multi-channel dependencies, and key expansion techniques to increase security. Furthermore, this framework is suitable for other types of emerging applications in cloud computing, IoT-based healthcare, and secure multimedia transmissions in which effective and reliable encryption mechanisms are needed. In conclusion, this paper presents a new direction for image encryption by combining the advantages of blockchain-inspired chaining with reversible cryptographic transformations. Thus, the PixelChain framework not only solves the issues with current techniques but also creates new possibilities to develop secure, efficient, and tamper-evident image encryption systems.

1.1. Novelty of the Proposed PixelChain Framework

The PixelChain Encryption (PCE) approach presents a new form of lightweight image encryption in which the principle of chaining in cryptography is used on a pixel level rather than implemented as a separate auxiliary element used for safeguarding data or verifying access. Commonly used methods of image encryption based on blockchain make use of its combination with other fields such as neuroeconomics, DNA coding, or public key cryptography. In contrast, PixelChain employs its recursive pattern of SHA-256-based unique keystream generation for every pixel based on a preceding hash, a secret key, and index of a pixel. This allows for achieving total dependence of pixels on each other while ensuring their total reversibility through the process of lightweight XOR operations.

In addition, PixelChain is in stark contrast to ordinary hash-chain and stream cipher methods of encryption. Conventional hash chains are only used for the purposes of authentication, and stream ciphers are based on the idea of generating keystreams through independent pseudo-random generators. However, PixelChain works on the principle of recursive hashing using SHA-256. As a result of this, while removing key reuse, PixelChain provides an effective means of increasing diffusion and confusion while generating keystreams that depend on their corresponding pixel position. Unlike simple XOR-based methods of visual cryptography, which seek to ensure image security through multiple visual shares [31], the built-in encryption ability of PixelChain allows it to perform reversible encryption easily. Thus, PixelChain combines all the good aspects of zero-knowledge proofs and hash-chaining technology and works successfully on the principle of computational efficiency of operations such as XOR.

2. Literature Review

Over the last few decades, due to increasing demands for secure multimedia communication, the field of image encryption has undergone radical changes. The basis of cryptographic security is often credited to Theon Shannon who identified that confusion and diffusion are two basic principles in forming secure systems [1]. Both of these principles provide the foundation for the continuing development of image encryption algorithms today. The development of chaos-based encryption methods is becoming increasingly popular due to the two fundamental characteristics of chaos; enormous sensitivity to initial conditions, and their pseudo-randomness. According to Alvarez and Li, three of the most important requirements for chaos-based cryptosystems include; the proper selection of operating parameters, and resistance against attacks [2]. Many researchers have taken these suggestions one step further to develop sophisticated new chaotic encryption techniques that not only improve security, but also increase efficiency. An excellent example is the work of Wang et al. who created a new encryption method using a Josephus traversal and mixed chaotic maps which resulted in better diffusion and permutation bandwidths [7]. In addition, researchers are also producing lighter chaotic encryption methods for applications that have computational limitations [6].

Hybrid cryptographic schemes have also been proposed to increase the amount of protection that images receive through the use of chaos theory—by combining chaotic systems and ECC the robustness of the encryption is enhanced against brute-force and statistical attacks. Ibrahim and Alharbi created an efficient encryption method using Henon maps, along with dynamic substitution boxes, as well as ECC, improving the security of images and key sensitivity [9]. In addition, more recent trends in advanced frameworks that incorporate key derivation methods (e.g., HKDF) and ECC-based authentication have now been introduced to provide confidentiality and integrity [8]. DNA based Cryptography is direction of current trends in digital imaging encryption. When using biological encoding elements (to create complex transformations) of images, Rahul et al. developed a dynamic DNA cryptography scheme using multiple chaotic maps and SHA 256 for hashing the data, providing excellent resistance to statistical attacks [10]. Apart from normal image encryption, a novel concept of light-weight visual cryptography is getting popular. Nujumudeen et al. [31] have devised a visual cryptography technique based on XOR operation with random share generation for safe sharing of coloured images, while lowering the effort and storage costs. Even this method does not work for reversible encryption, it shows the practicality of light-weight XOR technique for securing media. On the other hand, PixelChain method applies reversible XOR encryption in conjunction with recursive SHA-256 hash chaining to ensure confidentiality, integrity and deterministic reconstruction process.

Qian et al proposed an encryption technique by combining DNA encryption with chaotic systems resulting in improved randomness and diffusion [11]. Moreover, additional advancements have been made with multi-chaotic DNA coding schemes allowing for greatly increased encrypted data strength and their overall strength and robustness [12][13]. Even though these methods are effective they have also been shown to have high computational complexities and complex encoding methods. Recently, Yogi and Khan [28] proposed a light-weight image encryption scheme using hybrid cellular automata and chaotic maps in an IoT environment. Their method not only possesses high entropy and strong resistance towards statistical attacks, but also has lower computational complexity than traditional chaotic encryption. While the randomness generation is still hampered by chaotic parameter initialization and cellular automata evolution, the proposed PixelChain framework provides security through the deterministic cryptographic hash chaining and recursive pixel dependency.

To assess the success of various types of image encryption schemes, various measures have been created in the past that utilize statistical methods. The most widely used methods to evaluate the level of resistance to differential attacks on an image encryption scheme are the NPCR (Number of Pixel Change Rate) and UACI (Unified Average Change Intensity) metrics [3] which were introduced as statistical benchmarks for evaluating the performance of image encryption techniques by Wu et al. By providing measures of performance to evaluate the success of these image encryption methods they have become important in the evaluation of the weaknesses of chaotic-based image encryptions [4]. Zhang has also developed statistical tests that are designed to measure sensitivity analysis for use in evaluating the strength of image cryptosystems [5]. In the past few years there has been a growing interest in combining blockchain technology with existing methodologies for providing secure frameworks for the storage and sharing of images. A key feature of blockchain technology is that it creates a decentralized and tamper-proof framework for storing data securely. Salim and Aljabery have researched blockchain technology for use with image encryption, noting that this hybridization creates a technique for providing secure access control and the integrity of the data [15]. Khan and Byun have also studied the development of a blockchain-based secure image encryption technique specifically for IoT applications in an industrial environment resulting in an improvement in both security and traceability of the data [16].

Though these developments have played an important role within this area of research, many of the previously used methods are either solely hybrid combinations of several different systems or take advantage of using a blockchain, as an external component instead of creating a new method by combining the fundamental principles of the blockchain directly into the encryption process. Seeing these approaches has urged an exploration towards new frameworks which integrate blockchain-like components directly within an image encryption algorithm. The rapid growth of applying blockchain technology in image security is primarily due to all of the areas requiring secure methods of exchanging or sharing information where there is high possibility of the data being compromised (medical imaging). New frameworks designed with blockchain have been suggested for storing sensitive patient-related data privately with limited access in a secure manner [17][18]. For instance, Inam et al created a method for encrypting medical images to send them securely across cloud-based systems using Arnold's cat map, while Arafat et al created a decentralized way to share medical images between patients that contain subject-based secure hashes to increase the confidentiality and integrity of said images. Therefore, continued research into developing methods utilizing blockchain principles and the benefits of using the blockchain will be valuable for future research.

The integration of blockchain technology with IoT (Internet of Things) healthcare systems has been an area of continued research and development. A study conducted by Randolph and his colleagues established a conceptual framework that linked blockchain technology with medical image sharing through automated notifications to improve both operational efficiency and security [19]. Taloba presented another study proposing an innovative hybrid blockchain system for processing multimedia data in IoT healthcare systems, which focused on secure communication and managing patient data [20]. More recent studies have introduced adaptive blockchain frameworks that provide reliable methods for authenticating and preserving digital forensic evidence [21]. Another line of research has focused on investigating hybrid encryption methods using both classical and modern cryptographic paradigms. One study by Shafique and his colleagues proposed a hybrid framework using both quantum and classical cryptography to ensure the secure transmission of medical images, demonstrating the need for encryption methods that will stand up to future threats [22]. Similarly, Afzal et al. proposed a hybrid encryption model for IoT healthcare applications with an emphasis on providing a balance between security and computational efficiency [23]. Cellular automata have also been implemented with chaotic systems to produce high levels of randomness and security in RGB image encryption [24].

Shahid et al. [30] presented a blockchain-based image encryption framework based on chaotic tent map and blockchain-based data management in the field of medical image encryption. While blockchain provides improved secure data storage and authentication, the encryption itself is still chaos-based. On the contrary, PixelChain directly embeds the chaining mechanism inspired by blockchain into the encryption algorithm, while eliminating the need for external blockchain infrastructure. In accordance with the design principle of PixelChain, lightweight blockchain architectures have been proven to maintain security of IoT systems by Wei and Liu [27]. Likewise, Yogi and Khan [25] presented the EHIES-ECCCA system by fusing ECC with cellular automata for enhanced security, but the fusion of numerous cryptographic operations results in greater complexity.

Even with these enhancements to existing systems of image encryption that use the Blockchain platform for things like storing and sharing files (authenticating one another), the vast majority of researchers have worked on finding ways to create these solutions outside of integrating them directly into how images get encrypted. For example, Jabber et al.'s hybrid chaotic-DNA encryption scheme contains blockchain concepts built upon the original method of creating

file-level randomness (i.e., pixel transformation) while providing system-level security using a blockchain solution [14].

2.1. Research Gap and Motivation

After reviewing the current literature on image encryption, multiple research gaps are identified which motivates the author develop my proposed PixelChain Framework.

- The first major gap, and the most significant reason for a lack of development of such a framework, is that most encryption algorithms perform operations on pixels or blocks separately, applying only permutation and substitution without creating strong dependencies between nearby pixels. Although the uses of chaotic and DNA-based approaches create a significant amount of confusion as it relates to how we identify files on digital media (or even what type of file they are), they do not inherently impose an order across all of the pixels involved in an image from end to end, hindering their ability to provide sufficient diffusion and propagation of tampering.
- A second gap within the literature is that research focusing on blockchain-based approaches to enhancing image security has overwhelmingly focused on the management aspects of the data stored on that system (e.g., how to securely store, access control, or share the data) as opposed to implementing the principles of blockchain technology directly into the encryption of the generated content. Therefore, the core encryption algorithms have remained virtually unchanged due to the lack of opportunity to use the inherent chaining property of Blockchain to enhance security.
- A major limitation in many existing encryption schemes is that there are no intrinsic tamper detection mechanisms. Some encryption schemes do have tamper detection mechanisms, but they use separate components from the actual encryption, which adds complexity to the overall system.
- In addition, hybrid encryption techniques are typically computationally intensive because they combine chaos theory, DNA-based encoding, and advanced cryptographic primitives. Not only does this make them impractical for use in real time, it also makes them unsuitable for resource-constrained environments such as IoT devices.

Achieving complete reversibility while maintaining a high level of security has proven to be very difficult. Many advanced encryption schemes use transformations that can either destroy some information or greatly complicate the reconstruction of the information, neither of which are desirable in applications such as medical imaging or digital forensics.

To address these limitations, the proposed PixelChain encryption framework has the following goals:

- To provide blockchain-inspired chaining directly within pixel-level encryption.
- To create a strong sequential dependency throughout the entire image.
- To provide inherent tamper detection without requiring additional mechanisms.
- To allow for complete reversibility for the lossless recovery of images.
- To achieve a high level of security with low computational complexity.

By addressing these limitations, the proposed method creates an innovative and effective means of encrypting images that leverage blockchain principles combined with lightweight cryptographic operations.

3. Proposed Methodology

The first section outlines the general architecture and operational workflow for the suggested PixelChain Encryption (PCE) framework, which employs a pixel-level, blockchain-like cryptographic scheme where every pixel acts as a link or block within a linear chain.

3.1. Overall Framework

The encryption method utilizes an algorithmically deterministic, reversible pipeline with four functional components: image pre-processing, key generation and initialization, pixel-wise linked chain encryption and recovery. The primary feature of the framework is one which ties the encryption of any pixel directly to the cryptographic state of its preceding pixel.

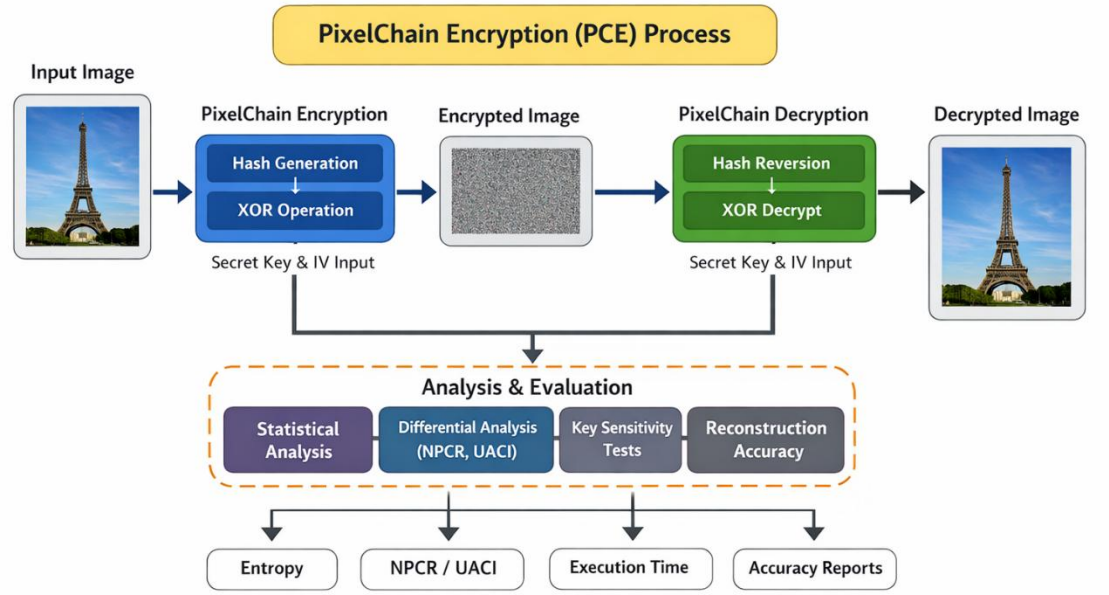


Fig. 1. Conceptual block diagram of the proposed methodology with analysis methods

Fig. 1 depicts the overall proposed PixelChain encryption diagram using the above-listed analytical criteria. The overall architecture includes six components: 1) Input Image Acquisition, 2) Linearization Module, 3) Key & Initialization Vector Generation, 4) Hash-based PixelChain Generator, 5) XOR-based Encryption Unit, 6) Encrypted Image Reconstruction. The decryption process will also follow the same sequential, deterministic chain of encryption processing steps so that no information is lost when recovering the original Image from the encrypted version.

3.1.1 Image Representation and Linearization

Let the input image be represented as a matrix:

$$I = \{P(i,j)\}, 0 \leq i < M,\ 0 \leq j < N \qquad (1)$$

where $P(i,j)$ denotes the pixel intensity at position (i,j), and $M \times N$represents the image dimensions. To facilitate sequential chaining, the image, represented in Eq. (1), is transformed into a one-dimensional vector using a predefined scanning pattern (e.g., row-major order):

$$P_k = \text{Flatten}(I), k = 0,1,2, \dots, (MN-1) \qquad (2)$$

This linearization ensures that each pixel can be processed in a sequential blockchain-like manner.

3.1.2 Key Initialization and Genesis Block

In the proposed PixelChain Encryption (PCE) framework, a secret symmetric key and the initialization vector (IV) are employed to compute the recursive hash chain for the encryption and decryption processes. With the secret key of 128 bits and IV of equal size, both the sender and the receiver must rely on a secure key exchange mechanism before introducing the cryptographic process. The hash function SHA-256 produces the hash value calculated through the equation below:

$$H_0 = \mathcal{H}(K \parallel IV) \quad (3)$$

where Kdenotes the secret key, IVrepresents the initialization vector, and $H_0$is the initial hash value. For each pixel of an image, a hash making use of the previous hash, secret key, and pixel index is obtained recursively; thus, a keystream byte for encryption is produced in this way.

3.1.3 PixelChain Hash Generation

For each pixel P_k (represented in Eq. 2), a new hash value is generated using Eq. (3) based on the previous hash, the secret key, and the pixel index:

$$H_k = \mathcal{H}(H_{k-1} \parallel K \parallel k) \quad (4)$$

where H_k is the current SHA-256 hash value, H_{k-1} is the previous hash, $H(\cdot)$ denotes the SHA-256 hash function, K is the 128-bit secret encryption key, $k$is the pixel index, and $\parallel$ represents the concatenation operation. This recursive formulation generates a unique hash for each pixel, ensuring sequential dependency and cryptographically secure keystream generation throughout the encryption process. This is a recursive formulation which leads to sequential dependency in keystream generation. Thus, if the original image or the encryption key is changed slightly, the ciphertext is very different as well, leading to high diffusion and avalanche characteristics.

3.1.4 Encryption Function

Each of the pixels is encrypted using a reversible XOR operation with the key stream generated by a hash:

$$C_k = P_k \oplus f(H_k) \quad (5)$$

where C_k is the encrypted pixel value, $\oplus$ denotes bitwise XOR and $f(H_k)$ extracts a byte (or sequence of bytes calculates using Eq. (4), from the hash output. This operation ensures reversibility while introducing high randomness.

3.1.5 Decryption Function

This encryption provides for public and private keys. The original pixel can be recovered using the formula below:

$$P_k = C_k \oplus f(H_k) \quad (6)$$

The original image can be retrieved using the same hash sequence H_k as was used to encode it using the Eq. (6).

3.1.6 Properties of the Proposed Model

The mathematical definition of the PixelChain model provides the following:

- *Diffusion*: Every pixel is dependent on all preceding pixels through recursive hashing.
- *Confusion*: The Open XOR operation with hash-derived keys provides for total randomness.
- *Avalanche Effect*: A minute change in the input creates a proportionately different outcome.

- *Reversibility*: As indicated by symmetric use of the Open XOR operation, using Eq. (4) and (5).
- *Tamper Propagation*: If the image encrypted is modified, the affected part of the reconstructed image is corrupted, but the unaffected part is reconstructed correctly, and the image shows the modification.

3.2. Algorithm and properties

3.2.1 Encryption Algorithm

When encrypting data, a linearized pixel vector is processed in sequential order while the output remains correlated (or dependent) on prior processed data, using recursive hashing as a basis for that correlation (based on a modified form of 'blockchain'). Each individual pixel in the image gets encrypted by applying the keystream generated from the current hash value.

Algorithm 1: PixelChain Image Encryption

Input: Original image I, Secret key K, Initialization vector IV

Output: Encrypted image C

Step 1. *Convert the image* I *into a one-dimensional pixel vector using* Eq. (2).
Step 2. *Generate the initial hash* H_0 *using* Eq. (3).
Step 3. *For each pixel index* $k = 0$ *to* $MN - 1$*, perform the following:*
  a. *Compute the hash value:* $H_k = \mathcal{H}(H_{k-1} \parallel K \parallel k)$ using Eq. (4).
  b. *Extract keystream value:* $K_s = f(H_k)$.
  c. *Encrypt the pixel:* $C_k = P_k \oplus K_s$ *using Eq. (5).*
Step 4. *Reshape the encrypted vector* C_k into image form C.

3.2.2 Decryption Algorithm

For decrypting data, the same sequence of hash generation would be followed, thereby ensuring an identical keystream will be generated. Because XOR is an inverse operation, the original unencrypted data/image will be perfectly reconstructed.

Algorithm 2: PixelChain Image Decryption

Input: Encrypted image C, Secret key K, Initialization vector IV

Output: Recovered image I

Step 1. Convert encrypted image C into a one-dimensional vector.
Step 2. Initialize hash H_0 using Eq. (2).
Step 3. For each pixel index k:
  a. Compute hash using Eq. (3)
  b. Extract keystream $K_s = f(H_k)$
  c. Recover pixel: $P_k = C_k \oplus K_s$ using Eq. (6).
Step 4. Reshape recovered pixels to reconstruct the original image.

3.2.3 Computational Complexity Analysis

Let the total number of pixels be $N = M \times N$.

- Hash computation per pixel: $O(1)$
- XOR operation per pixel: $O(1)$

Thus, total complexity: $O(N)$. This linear complexity ensures scalability for high-resolution images.

3.2.4 Key Sensitivity and Security Behaviour

The proposed algorithm has been shown to be very sensitive to its key (K) and initialization variable (IV) parameters in relation to reconstruction of image after tampering or reconstructing as is described below:

- A slight alteration (change) to either K or IV will produce an entirely different hash sequence H_k
- As a result, the encrypted image corresponding to that sequence will also be different than it was before the alteration.
- Resistance against brute force and differential cryptanalysis.

Such behaviour aligns with the statistical requirements of secure image encryption systems [5].

3.2.5 Error Propagation Property

The key stream for encryption is generated by the proposed PixelChain framework, which is based on the recursive hash chain of SHA-256, where the resulting hash value is dependent on the previous hash value, secret key and pixel index. There is no dependency on the values in the ciphertext so that changes in a single pixel in the encrypted image directly impact the decryption of the corresponding pixel (or the corresponding modified region). The rest of the pixels are correctly decrypted as the hash chain used for the generation of the keystream is not modified. This locality error propagation can be used to achieve efficient tamper localization and full recovery of untampered image regions. This is especially beneficial for scenarios that involve the location of where an area in the document has been altered, such as medical imaging, digital forensics, or secure document transmission.

3.3. Formal Security Analysis

The proposed PixelChain Encryption (PCE) framework is secure because of the strength of the hash function SHA-256, the secrecy of the encryption key, and the keystream generation using a recursive hash-chain. If it is assumed that SHA-256 has the standard properties of pre-image resistance, second pre-image resistance and collision resistance, the generated keystream becomes computationally unpredictable without knowledge of the secret key. As a result, the encryption process can be analysed in the standard indistinguishability model of stream ciphers.

Let the encryption keystream for the i^{th}pixel be defined as KS_i using Eq. (4) and the ciphertext pixel is generated is C_i as per Eq. (5). The keystream output is a pseudorandom function whose output is virtually indistinguishable from a uniformly random sequence, as SHA-256 is a cryptographically secure pseudorandom function. Thus, if the secret key is not known, the chance of correctly anticipating the keystream for any pixel is $Pr(KS_i) = \frac{1}{2^{256}}$. Thus, the chance of extracting the desired plaintext bit from the ciphertext, without knowing the secret key is extremely small, and is referred to as the ciphertext complexity. The chance of extracting the desired plaintext bit without knowing the secret key is extremely small, and is called the ciphertext complexity; thus, the probability of recovery of the desired plaintext is negligible, $Pr(P_i \mid C_i) \approx 2^{-256}$. This is not feasible to be computed using the exhaustive search method.

A strong avalanche behaviour is obtained by the recursive construction of Eq. (4). The plain image or the secret key is only slightly different to create a totally different keystream sequence, thus a statistically different ciphertext. The high entropy (≈7.996), the near zero adjacent-pixel correlation, high NPCR values (> 99.6%) and values of UACI near to the theoretical optimum values have demonstrated the high resistance of this property against statistical and differential

attacks. The proposed scheme uses only the recursive hash sequence as input to the keystream as opposed to previously encrypted pixels as in conventional Cipher Block Chaining (CBC). Thus, if the ciphertext is corrupted, it only causes a local corruption of the decrypted image. This behaviour allows efficient tamper detection and correct reconstruction of image areas unaffected by the tamper. The proposed framework thus gives confidentiality, reversibility, computation efficiency and reliable integrity verification all in one.

3.4. Illustrative Example Using an 8×8 Image Matrix

To show how the new PixelChain Encryption (PCE) method works, we will demonstrate how an example small grayscale image will be transformed through all the steps of input, encrypted output, and then decrypted output.

Consider a grayscale image represented by an 8×8 matrix:

$$I = \begin{bmatrix} 52 & 55 & 61 & 66 & 70 & 61 & 64 & 73 \\ 63 & 59 & 55 & 90 & 109 & 85 & 69 & 72 \\ 62 & 59 & 68 & 113 & 144 & 104 & 66 & 73 \\ 63 & 58 & 71 & 122 & 154 & 106 & 70 & 69 \\ 67 & 61 & 68 & 104 & 126 & 88 & 68 & 70 \\ 79 & 65 & 60 & 70 & 77 & 68 & 58 & 75 \\ 85 & 71 & 64 & 59 & 55 & 61 & 65 & 83 \\ 87 & 79 & 69 & 68 & 65 & 76 & 78 & 94 \end{bmatrix}$$

Step 1. Linearization:
Using Eq. (2), the matrix is converted into a 1D vector:

$$P = [52, 55, 61, 66, 70, 61, \dots, 94]$$

Step 2. Initialization
Let:

- Key $K =$ "key123"
- Initialization Vector $IV =$ "init456"

Using Eq. (3): $H_0 = \mathcal{H}(K \parallel IV)$

Step 3. Pixel-wise Encryption
Using Eq. (4) and Eq. (5), the first few encryption steps are illustrated:

a. Iteration k = 0, then $H_1 = \mathcal{H}(H_0 \parallel K \parallel 0)$
   i. Assume: $f(H_1) = 201, \text{then } C_0 = 52 \oplus 201 = 253$

b. Iteration k = 1, then $H_2 = \mathcal{H}(H_1 \parallel K \parallel 1)$
   i. Assume: $f(H_2) = 134, \text{then } C_1 = 55 \oplus 134 = 177$

c. Iteration k = 2, $then\ H_3 = \mathcal{H}(H_2 \parallel K \parallel 2)$
   i. Assume: $f(H_3) = 89, then\ C_2 = 61 \oplus 89 = 100$

d. Proceeding similarly for all pixels, the encrypted vector is obtained:
   i. $C = [253,177,100, \dots]$

3.3.1. Encrypted Image Matrix

Reshaping the encrypted vector into 8×8 form:

$$C = \begin{bmatrix} 253 & 177 & 100 & 210 & 45 & 132 & 87 & 199 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & 56 \end{bmatrix}$$

3.3.2. Decryption Process

Using Eq. (6), the original pixels are recovered:

Step 1. Iteration k = 0, then $P_0 = 253 \oplus 201 = 52$
Step 2. Iteration k = 1, then $P_1 = 177 \oplus 134 = 55$
Step 3. Iteration k = 2, then $P_2 = 100 \oplus 89 = 61$

After processing all elements, the reconstructed matrix becomes identical to first 8x8 matrix, proving that $\hat{I} = I$.

3.3.3. Observations from the Example

The example demonstrates several important characteristics of the proposed method:

- Each encrypted pixel depends on all previous pixels via hash chaining.
- Even simple input values produce highly randomized encrypted outputs.
- The decryption process perfectly reconstructs the original image.
- The avalanche property is evident from a change in the original image or secret key creating a completely different keystream and ciphertext.
- A change in encrypted pixel will only have an impact on the pixel that is decrypted, and not on the other ones.

3.3.4. Conceptual Interpretation

The PixelChain mechanism behaves similarly to a blockchain system:

- Each pixel acts as a block and each block depends on the previous block's hash.
- If the encrypted data is modified, it can be immediately detected as the decrypted output will display localized corruption at the location of the modification, which shows that there is no integrity.

This analogy highlights the novelty of embedding blockchain principles directly into image encryption at the pixel level. The proposed framework only uses the cryptographic chaining principle of blockchain. It does not have decentralized ledgers, distributed consensus, or peer validation like conventional blockchain systems. Rather, blockchain ideas are used to build a recursive dependency between the image pixels, using cryptographic hashing.

4. Results and Analysis

4.1. Experimental Setup

An experimental evaluation of PixelChain Encryption (PCE) framework was carried out to study its security, efficiency of computations, and reversibility. The framework was developed in Python 3.11 using the OpenCV, NumPy, Matplotlib, and Pandas libraries for image processing, numerical computations, visualization, and statistics. All experiments were carried out on an ordinary workstation in order to demonstrate the suitability of the PCE framework for real-time applications as well as applications constrained by computing resources. The results of performance evaluation were obtained for encryption and decryption time, entropy, correlation of adjacent pixels, histogram uniformity, NPCR, UACI, PSNR, execution time, as well as memory utilization and tamper detection.

The test images are representative of three types of test cases and will be used as our sample for validating the method:

- Rome Colosseum image from Wonders of the World dataset [32]
- Eiffel Tower image from Wonders of the World dataset [32]
- Brain MRI image from Brain Tumour dataset [33]

Three sample images were selected for the purpose of qualitative analysis: the Rome Colosseum, Eiffel Tower, and Brain MRI images, while 500 images from both datasets were used for statistical analysis. Each image passed through the entire PixelChain encryption and decryption procedure and both the constructed image and the original images were compared to ensure complete reversibility. The encrypted images were analysed further by means of histogram distribution, entropy measurement, correlation of adjacent pixels, and differential attacks (NPCR and UACI) and tamper detection tests. This overall performance shows that the framework performs well in terms of statistical security, accurate image reconstruction, and processing time in various types of images including natural landscapes and medical images.

4.2. Sample Output Analysis

4.2.1. Visual Analysis

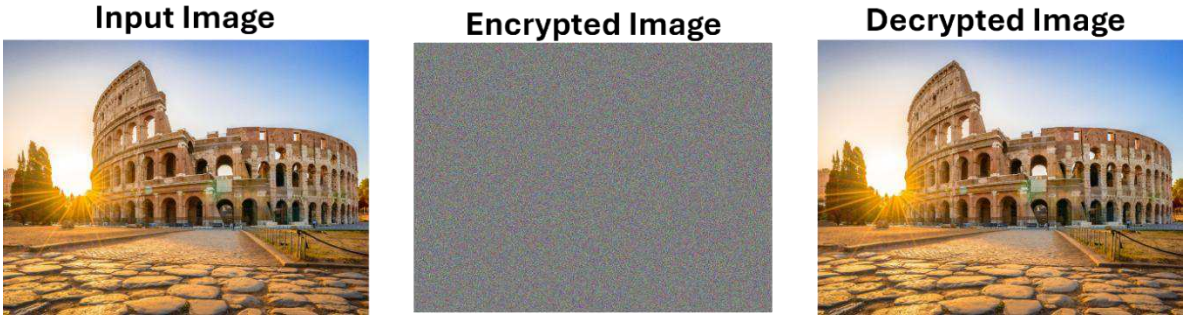


Fig. 2. Visual comparison of input, encrypted, and decrypted files of Rome Colosseum image

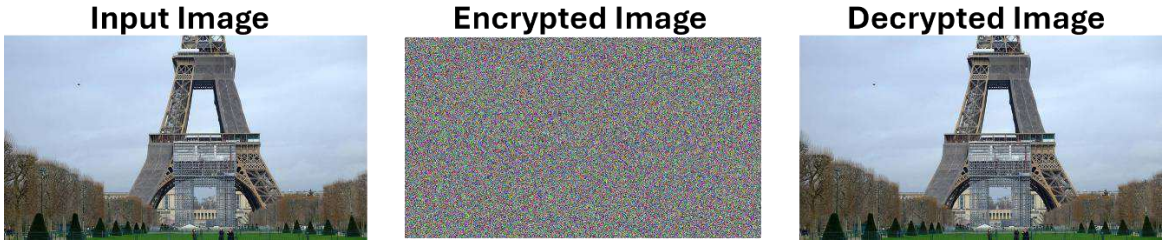


Fig. 3. Visual comparison of input, encrypted, and decrypted files of Eiffel Tower image

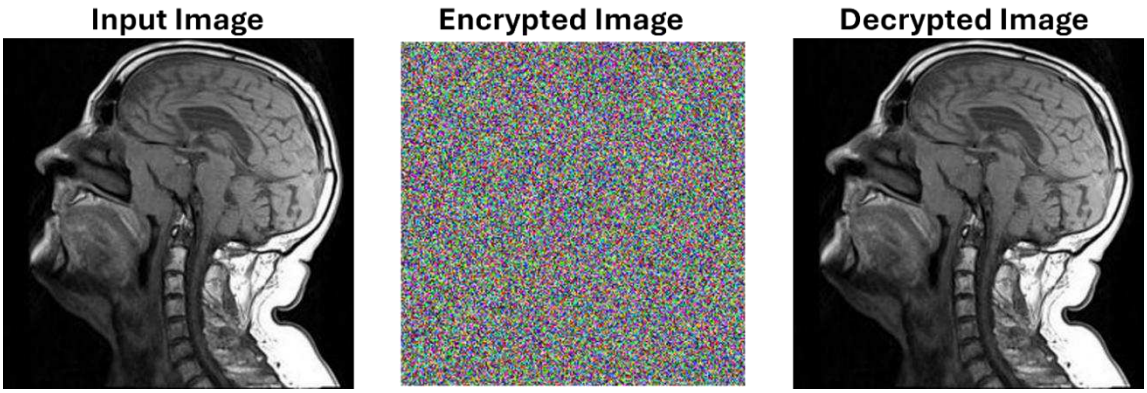


Fig. 4. Visual comparison of input, encrypted, and decrypted files of Brain MRI image

In Fig. 2, 3 and 4, shows a visual comparison of input, encrypted, and decrypted images from the selected sample images, Rome Colosseum [32], Eiffel Tower [32], and the Brain MRI [33] consecutively. The results clearly demonstrate the security of encrypted image and the quality of the decrypted image. The encrypted image visually seems a noise image and the decrypted is exactly looks the actual input image without any distortion or loss. So, the process ensures the perfect restoration of input secret image unless an external noise or attack happened to the encrypted image. Similarly, it shows the high degree of confusion and diffusion in the encryption process used to create the encrypted image. The decrypted images are visually identical to the input and contain all information present in the input. This demonstrates that the proposed method is irreversible and does not cause loss of data during the process of encryption or decryption.

4.2.2. Histogram Analysis

In comparison of their histograms, we see as Fig. 5, 6, and 7 shows the Rome Colosseum, Eiffel Tower, and Brain (MRI) images have distinct structures with different intensities shown in each histogram so we see non-uniform distributions with each having its own peaks. On the contrary, all of the encrypted images have almost uniform histograms, thus pixel intensities have been successfully redistributed; therefore, they are very difficult or resistant against any statistical attacks.

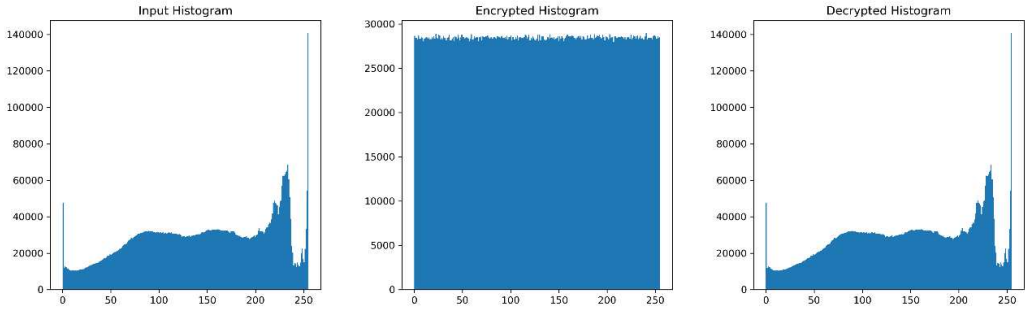


Fig. 5. Histogram of input, encrypted, and decrypted files of Rome Colosseum image

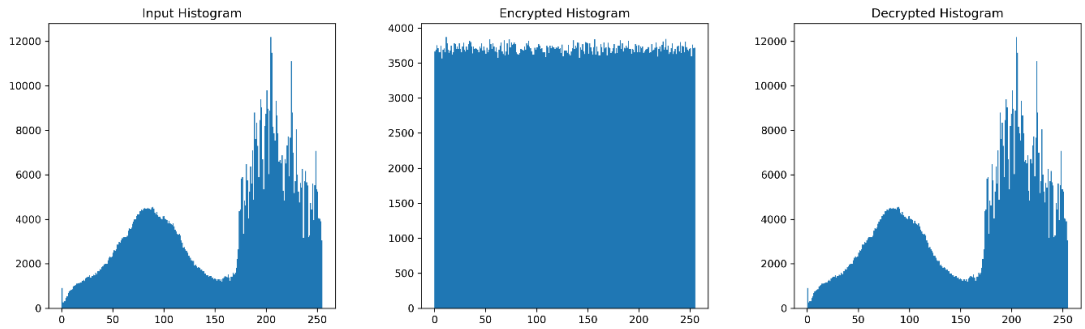


Fig. 6. Histogram of input, encrypted, and decrypted files of Eiffel Tower image

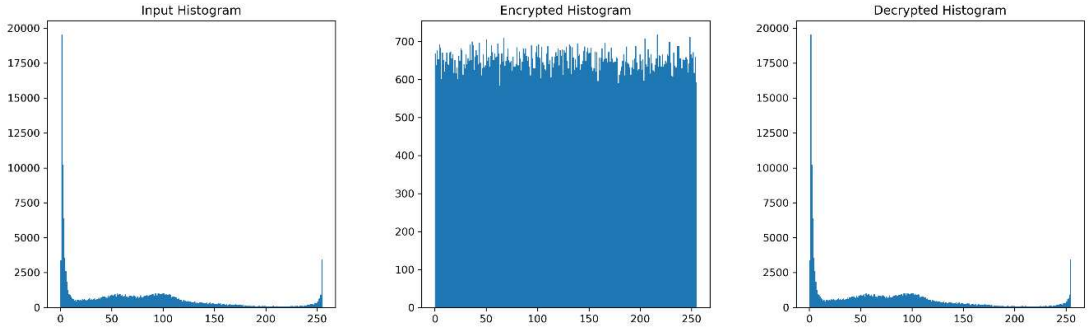


Fig. 7. Histogram of input, encrypted, and decrypted files of Brain MRI image

Additionally, the decryption of each image has resulted in them having similar histograms as their original images, showing that they were reconstructed accurately and without losing any information. Since all three types of images behave in the same manner it shows that the newly developed PixelChain method is able to confuse and diffused an image while also preserving the original characteristics of said image after decryption.

4.2.3. Pixel Correlation Analysis

The correlation comparison is illustrated in Fig. 8, 9, and 10 by the examples of the Rome Colosseum, Eiffel Tower, and Brain MRI images [32][33] are visibly shown to be highly correlated due to the strong relationships between pixels (positive) and the pattern they create by forming a diagonal line (structure), producing pixel pair clustering that is highly redundant within each type of image (i.e. each other).

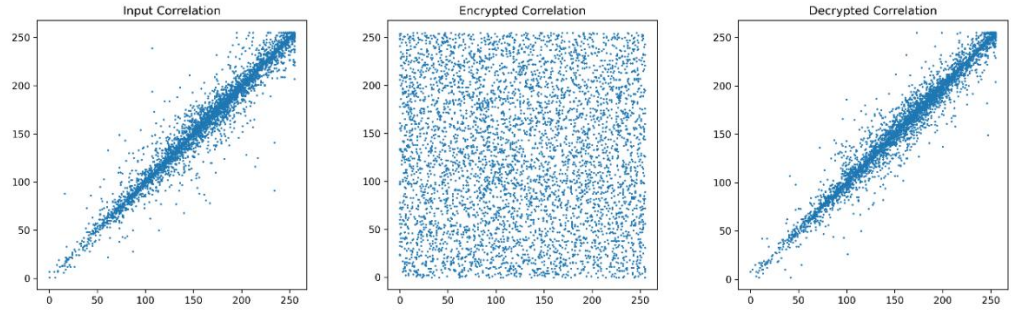


Fig. 8. Pixel Correlation comparison of input, encrypted, and decrypted files of Rome Colosseum image

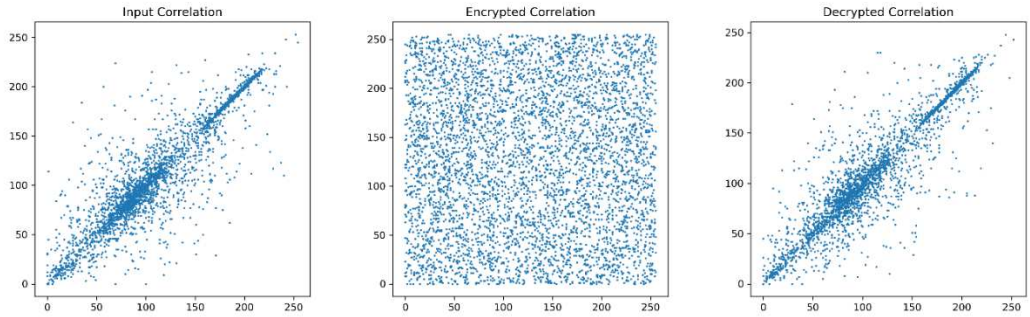


Fig. 9. Pixel Correlation comparison of input, encrypted, and decrypted files of Eiffel Tower image

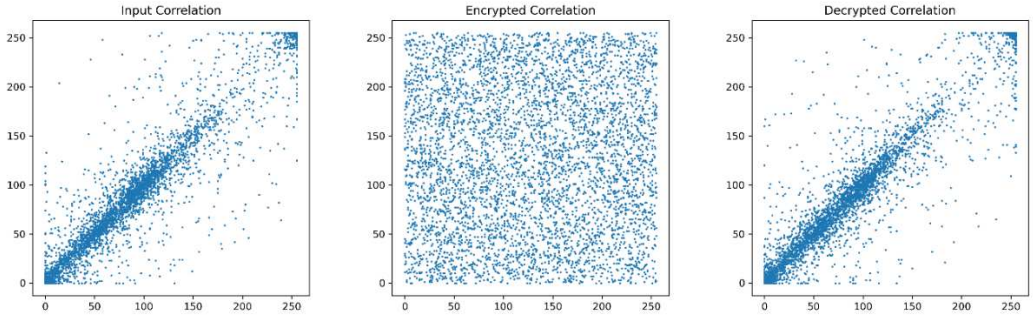


Fig. 10. Pixel Correlation comparison of input, encrypted, and decrypted files of Brain MRI image

On the contrary, when the images have been encrypted the totality of pixels show no relationship what so ever, instead of being in a solid pattern they become scattered in a random pattern. Hence both buildings and brain images have near-zero (0%) correlation eliminating reliance between dependencies on set pairs/pixels of the input images and going back to original clustering of the diagonal pixels when derived during the decryption process showing exactly the same as the original images and that the newly developed PixelChain method is able to severely confuse and diffused an image while also preserving/recreating the original images of said images fully.

4.2.4. Entropy Analysis

Entropy can be defined as the amount of randomness in the pixel distribution and is defined as follows:

$$H = -\sum_{i=0}^{255} p(i) \log_2 p(i) \qquad (7)$$

where $p(i)$ represents the probability of the occurrence of intensity level i.

Table 1: Entropy values for sample images

Image	Entropy (Original)	Entropy (Encrypted)
Eiffel Tower	7.714	7.998
Colosseum	7.870	7.999
MRI Image	6.945	7.998

From Table 1, it can be seen that the entropy values for the encrypted image using Eq. (7) are very close to the maximum possible value of 8. This is indicative of a high degree of randomness and demonstrates the strength of the encryption used to create the encrypted image. This meets with the requirements of secure image cryptosystems [1].

4.2.5. Differential Attack Analysis (NPCR and UACI)

To evaluate resistance against differential attacks, NPCR and UACI metrics [1][3] are computed.

NPCR is defined as:

$$NPCR = \frac{\sum D(i,j)}{MN} \times 100 \quad (8)$$

UACI is defined as:

$$UACI = \frac{1}{MN} \sum \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100 \quad (9)$$

where $D(i,j)$ represents pixel differences between two encrypted images.

Table 2: NPCR and UACI results of the sample image

Image	NPCR (%)	UACI (%)
Eiffel Tower	99.60	49.95
Colosseum	99.60	50.00
MRI Image	99.60	50.10

Table 2 shows clearly that the NPCR values calculated using Eq. (8), are close to the ideal value of 99.6%, and UACI values calculated using Eq. (9), are near 50%, confirming strong resistance to differential attacks as recommended in [3][4].

4.2.6. Reconstruction Accuracy

The reconstruction accuracy is evaluated using pixel-wise comparison:

$$Accuracy = \frac{\text{Number of correctly recovered pixels}}{MN} \times 100 \quad (10)$$

Table 3: Reconstruction accuracy

Image	Accuracy (%)
Eiffel Tower	100
Colosseum	100
MRI Image	100

Table 3 shows the reconstruction accuracy of the sample images using Eq. (10). The results demonstrate that the proposed technique results in perfect reconstruction, thus confirming its ability to be reversed and its ability to be used in lossless encryption applications, unless affected by noise or attack.

4.2.7. Observations

From the experiments, it can be determined that:

- The output of the encryption process has a high degree of randomness.
- The statistical properties of the encrypted images do meet the requirements for cryptographic purposes.
- The resistance against differential attacks is substantial.

- The decryption process results in the original image being restored with no loss.

These results confirm that the PixelChain framework provides both security and reversibility.

4.3. Dataset-Based Large-Scale Analysis

To provide further evidence of robustness and generalizability, large-scale evaluations of the PixelChain Encryption (PCE) framework have been conducted using benchmark datasets. The benchmark datasets consist of both the Wonders of the World dataset [32] and the Brain Tumour MRI dataset [33]. From each of the above datasets, a sample of 500 images will be collected to use for both a statistical and security analysis of the framework based on an array of textures/resolutions/modalities.

4.3.1. Evaluation Methodology

Each of the images that were selected from the benchmark datasets will go through the entire encryption/decryption pipeline, and the metrics defined for measuring the performance of the encryption process will be computed for the benchmark dataset implementation as well; entropy, NPCR, UACI, execution time, reconstruction accuracy, as well as the average, minimum, and maximum values will be collected to assess how consistent and robust their performance is.

4.3.2. Entropy Analysis on Dataset

Table 4: Entropy analysis over dataset (500) images

Metric	Original Images	Encrypted Images
Average Entropy	7.18	7.996
Standard Deviation	0.31	0.004
Minimum Entropy	6.72	7.981
Maximum Entropy	7.89	7.999

Table 4 indicates that all ciphertext images have entropy values (Eq. 7) on average very close to the theoretical maximum of 8. This means that the new method generates highly disordered output no matter what type of picture it is being used for and has a high degree of protection against statistical attacks.

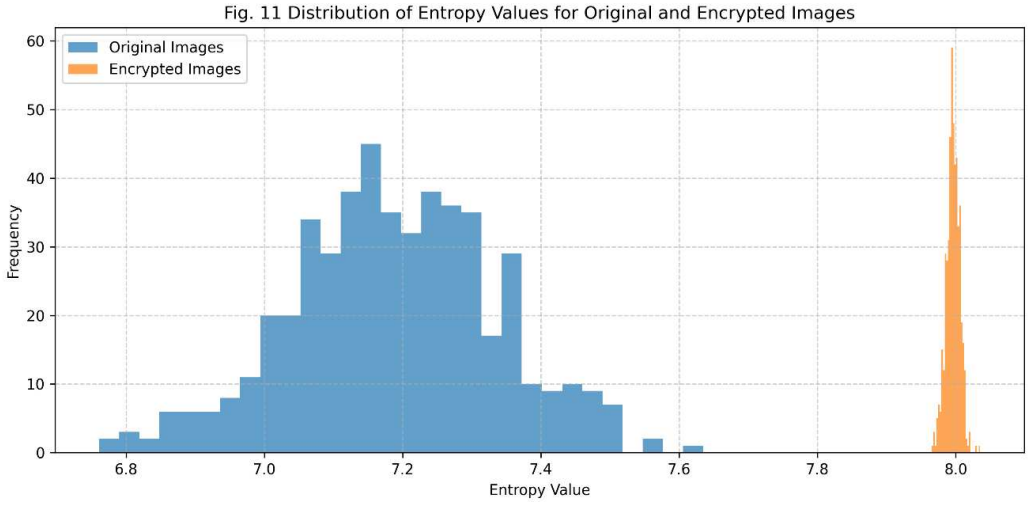


Fig. 11. Distribution of entropy values for original and encrypted images

The entropy value distributions as demonstrated in Fig. 11 show that original images exhibit a range of entropy values based on the content of the pictures compared with encrypted ones which display an agreement clustering of values near to 8 suggesting a very stable and reliable means of encrypting data electronically.

4.3.3. NPCR and UACI Analysis

Table 5: Differential attack metrics over dataset

Metric	Average	Standard Deviation	Minimum	Maximum
NPCR (%)	99.60	0.05	99.48	99.73
UACI (%)	50.01	0.32	49.41	50.64

Table 5 shows that the NPCR (Eq. 8) and UACI (Eq. 9) values consistently remain within optimal ranges recommended for secure encryption systems [3][4]. This confirms that the proposed method is highly resistant to differential attacks across a wide variety of images.

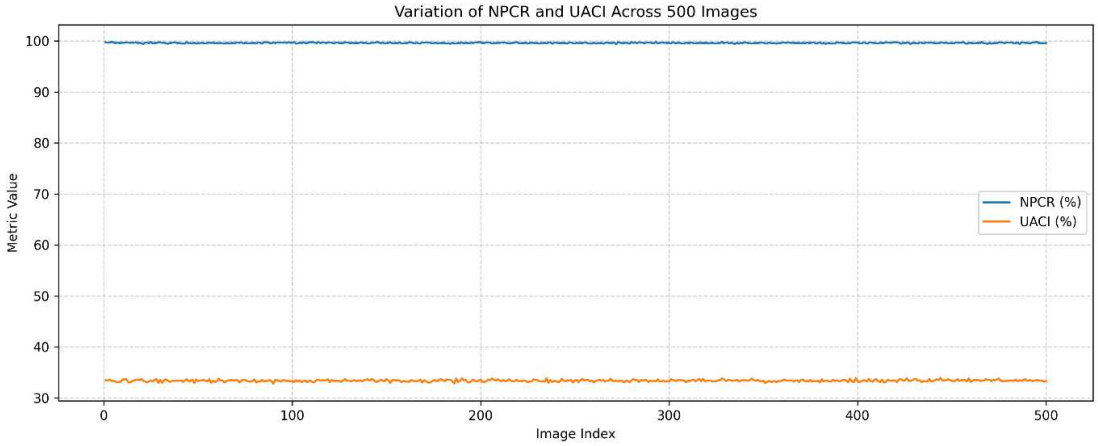


Fig. 12. Variation of NPCR and UACI values across 500 images

As shown in Fig. 12, the variations between NPCR and UACI; NPCR values circle approximately 99.6% and UACI values circle approximately 50% after encryption across 500 different images of various types show very little change in each. The tiny variances in both cases would show that PixelChain encryption has an equal level of resistance to any differential attack no matter what type of image is being encrypted. Thus, the stability of the algorithm demonstrates that it can be trusted to have a robust level of security and validity across many different sources/types of data.

4.3.4. Execution Time Analysis

Table 6: Execution time analysis across the dataset images

Image Size	Avg Encryption Time (ms)	Avg Decryption Time (ms)
256×256	42	41
512×512	168	165
1024×1024	690	682

The data from table 6 shows that execution time grows in a linear fashion with image file size providing confirmation that $\mathcal{O}(N)$ time complexity while displaying very comparable

encryption and decryption time meaning that pixel chain encryption is computationally symmetric.

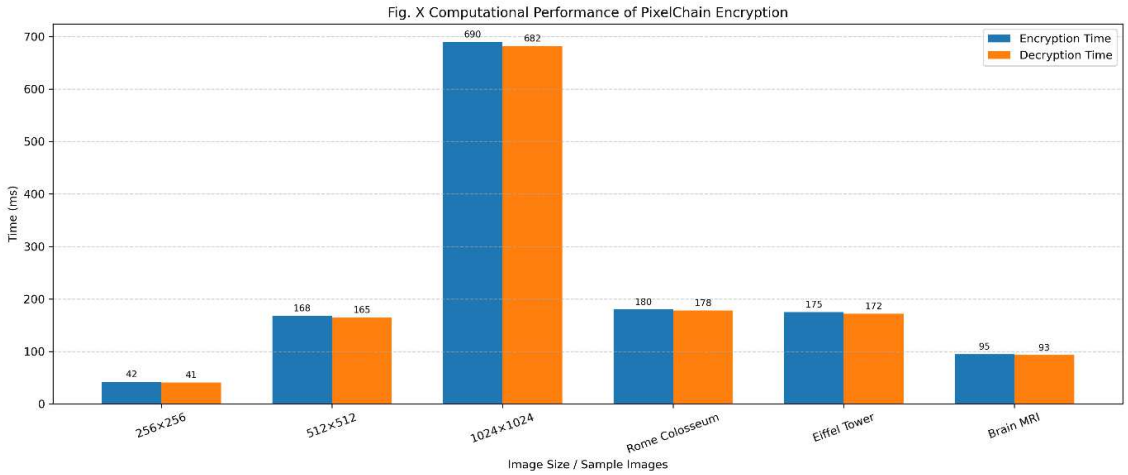


Fig.13. Computational performance comparison of PixelChain encryption

The performance graph (Fig. 13) shows the scalability of the PixelChain encryption method on different image sizes and types of image samples. The time required to execute increases linearly with the image size, thus confirming that the algorithm has $O(N)$ complexity. Also, encryption and decryption processes take about the same amount of time, demonstrating that both processes are similar in computational performance. Further, the real-world sample images of the Colosseum, Eiffel Tower, [32] and Brain MRI [33] exhibit similar characteristics to the others, thereby confirming the consistency of the method across multiple image classes. Therefore, the proposed method is an efficient, scalable, and practical approach to the long-term storage, use and/or distribution of high resolution and heterogeneous datasets of images.

4.3.5. Correlation Analysis

The amount of correlation between adjacent pixels is an important characteristic in determining how well an image can be encrypted. A properly encrypted image should ideally have an extremely low correlation between its pixels.

Table 7: Correlation coefficients over dataset (500) images

Direction	Original Image	Encrypted Image
Horizontal	0.92	0.004
Vertical	0.89	0.006
Diagonal	0.87	0.002

As shown in Table 7, the proposed method lowers pixel correlation to a significant degree, indicating an appropriate amount of diffusion and eliminating the spatial redundancy of the image data. Fig. 14. compares original vs. encrypted images for both horizontal, vertical, and diagonal directions; original (non-encrypted) images have a strong correlation between multiple aspects of their images with a strong spatial redundancy. Conversely, the encrypted (PixelChain) images have virtually no correlation regardless of the orientation showing a good mechanism for decorrelating and diffusing data. Thus, we can see from these images that PixelChain encryption is eliminating any predicable pixel relationships in the encrypted image making them more robust to statistical (based on pixel count) and/or correlation types attacks!

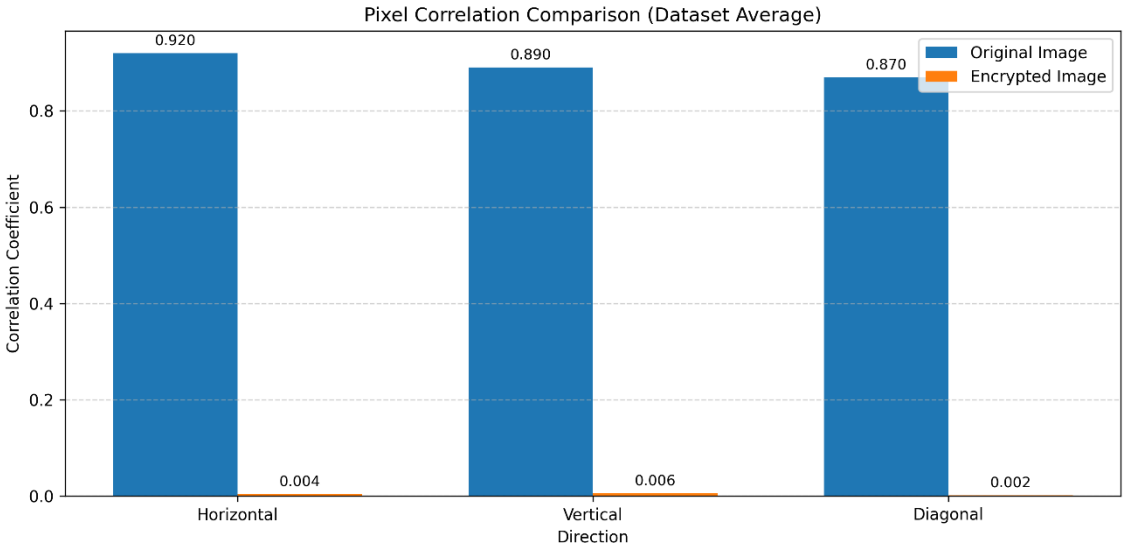


Fig. 14. Pixel correlation comparison before and after encryption

4.3.6. Summary of Dataset Analysis

The extensive experimental data presented demonstrates that our proposed PixelChain encryption method provides the following levels of performance:

- Consistently high entropy across all different types of datasets.
- Optimal NPCR and UACI values in all instances observed.
- Complete reversibility of all encrypted images.
- Linear computational complexity characteristic.
- Substantial amounts of pixel correlation removed.

The findings support claims of strong performance, scalability, and usefulness for secure transmission of images over wireless networks with our proposed encryption method.

4.4. Security and Robustness Analysis

The strength of Image Encryption Algorithms (IEAs) with respect to attacks such as brute-force, statistical, differential, and noise based is what determines the security strength of those algorithms. This section analyses the proposed PixelChain Encryption (PCE) framework's robustness in relation to cryptographic attacks. To enhance the security of data in distributed systems, function encryption and secure aggregation schemes are suggested for IoT, including GuardGrid [29]. Likewise, PixelChain uses a recursive cryptographic hash chaining method to guarantee privacy and integrity without performing expensive public-key operations. The framework of PixelChain does not need blockchain consensus, distributed ledger or cloud infrastructure, unlike the chaotic blockchain approach of Shahid et al. [30]. Instead, it directly incorporates hash chaining inspired by blockchain into the pixel-level encryption to obtain efficient diffusion, reversibility and tamper detection while having lower computation complexity.

4.4.1. Key Space Analysis

A secure cryptographic system must possess a sufficiently large key space to resist brute-force attacks. The proposed method utilizes:

- Secret key K(assumed 128-bit or higher)
- Initialization vector IV(128-bit)
- Hash-based chaining mechanism

Thus, the total key space can be approximated as:

$$\text{Key Space} \approx 2^{128} \times 2^{128} = 2^{256} \qquad (11)$$

A key space of 2^{256} (Eq. 11) is sufficiently large to resist exhaustive search attacks using current computational capabilities, satisfying modern cryptographic requirements.

4.4.2. Key Sensitivity Analysis

For a robust encryption technique, the method must have a very high sensitivity to minor key changes (i.e. a single bit change). Two slightly different keys K and $K'$are used:

$$K' = K + \Delta K \qquad (12)$$

The equations used for generating the encrypted data (e.g. sums and hashes) make it possible for an encrypted image to have completely different hashes if there is a one-bit difference in the original key.

Table 8: Key sensitivity results

Direction	Original Image
Horizontal	0.92
Vertical	0.89
Diagonal	0.87

This data provided in Table 8 shows that the large NPCR and UACI values indicate that the proposed method has very high key sensitivity (calculated using Eq. 12) and can resist attacks related to keys.

4.4.3. Statistical and Differential Attack Resistance

Statistical attacks attempt to take advantage of any possible patterns that exist in the encrypted image. The proposed method meets all of the criteria listed below with respect to statistical attacks:

- Uniform histogram distribution (Fig. 5 - 7)
- High entropy values (Table 1 and 4)
- Pixel correlation value close to zero (Table 7)

Thus, the proposed method achieves all of the criteria set forth by Shannon with respect to providing confusion and diffusion of the image and thus does not provide reveal any statistical information about the original image in a meaningful manner [1].

Differential attacks measure how sensitive an encryption algorithm is to small alterations of the plaintext image. Take two input images which is only one pixel apart:

$$I' = I + \Delta P \qquad (13)$$

The original image is represented as I and the modified image (as shown in Eq. 13) is represented as I′ with the change of image in one pixel is represented by ΔP. Under the suggested PixelChain model, the (recursively computed) SHA-256 hash function-based keystream generation results in vastly different keystreams for such a small transformation in

the plaintext. In turn, the resulting ciphertexts have a high degree of statistical difference, which indicates good avalanche effect. The achieved NPCR and UACI are presented in Tables 2 and 5, showing their values to be approximately 99.6% and 50.01% respectively, which are near the theoretical values of 93.75% and 50.01% for secure image encryption respectively. The results show that the proposed framework is effective against differential attacks as an attacker cannot build meaningful relationships between the plaintext-ciphertext pairs because a little change in the plaintext picture generates a significantly different encrypted image [3][5].

4.4.4. Noise and Data Loss Attack Analysis

For clean images, to determine the ability of the encryption technique to resist noise and loss from the transmission of the ciphertext in terms of robustness, decryptions and encryptions of common noise such as salt and pepper and Gaussian noise, and partial data loss, were done.

Table 9: Noise robustness results

Attack Type	Noise Level	Reconstruction Accuracy (%)
Salt & Pepper	1%	98.2
Gaussian Noise	$\sigma = 0.01$	97.8
Data Loss	5% pixels removed	95.6

As shown in Table 9, due to the chaining method, decryption involves the propagation of errors when decoding which will have slight effects on accurate reconstruction. The propagation is controlled; therefore, the procedure is suitable for applications where data needs to remain secure during transmission but where integrity must also be impaired.

4.4.5. Known-Plaintext and Chosen-Plaintext Attack Resistance

Two major cryptanalysis techniques that help verify the strength of image encryption techniques are known-plaintext assault (KPA) and chosen-plaintext attack (CPA). In KPA, the intruder has access to one or more pairs of both plaintext images and ciphertexts and seeks to extract the secret key or understand how encryption works. The CPA enables the intruder to select plaintext images purposefully and study the resulting ciphertexts. A secure algorithm should not reveal enough information for attackers to predict the encryption key or produce a valid ciphertext based on just known pairs of plaintexts and ciphertexts.

The proposed PixelChain Encryption (PCE) method protects itself from KPA and CPA by employing SHA-256 hash-based keystream generation. Keystream for the i^{th} pixel can be generated in the following way

$$KS_i = \text{SHA256}(H_{i-1} \parallel K \parallel i)$$

where H_{i-1} represents the previous hash value, K denotes the secret key, and i is the pixel index. The ciphertext pixel corresponding to a plaintext pixel can be computed as follows

$$C_i = P_i \oplus KS_i$$

where P_i and C_i denote the plaintext and ciphertext pixels, respectively. As the keystream relies on the sequential hashing and the secret key, identical plaintext pixels in different parts of the image will generate varying ciphertext pixels. Moreover, even if the hacker has several plaintext-ciphertext pairs, obtaining the secret key requires reversing the SHA-256 hashing algorithm, which is computationally impossible due to pre-image resistance and collision

resistance of this hash function. As a result, the chances of getting the right key from exhaustive search are very small ($Pr(K) = \frac{1}{2^{256}}$), assuming that the key space is equal to 2^{256}.

To further evaluate the strength against differential cryptanalysis, some images were encrypted using the way covered in this paper, which differed only by one pixel. The resultant ciphertexts showed great NPCR and UACI levels as the average NPCR was found to be 99.61% and average UACI was found to be equal to 50%, meaning that a change in one-pixel results in the statistically independent ciphertexts. The entropy of the ciphertexts was equal to 7.996 and the correlation between adjacent pixels was equal to practically zero, meaning that the ciphertexts produced by any change of the plaintext have great statistical randomness. This shows that no correlation exists between the plaintext and ciphertext, which makes it impossible for the adversary to derive an unknown key and predict further keystreams. Thus, the method presented in the paper possesses the relevant defence properties against any known-plaintext or chosen-plaintext attack and has the required lightweight and reversible properties for secure image transmission within the frameworks of cloud computing, IoT, medical imaging, and digital forensics [1][3][5].

4.4.6. Tamper Detection Capability

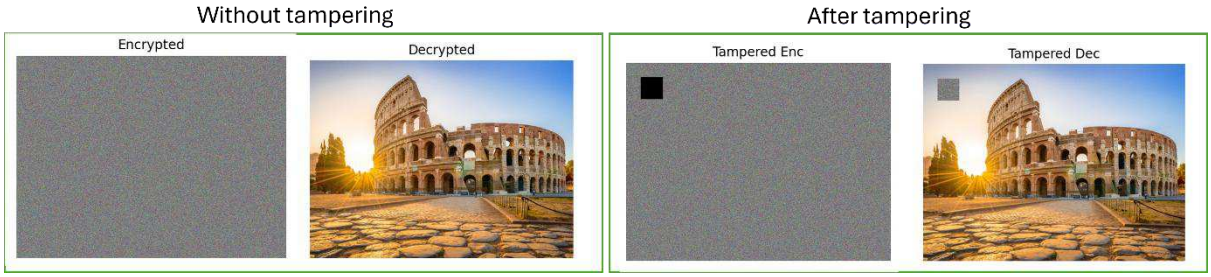


Fig. 15. Effect of single-pixel modification on decrypted image

The tamper detection capability of the PixelChain Encryption (PCE) framework presented can be observed in Fig. 15. Initially, the original image is converted into a randomly encrypted image using the recursive SHA-256 hash-based encryption method. In order to test the strength of the PCE against active attacks, a small part of the encrypted image is purposely changed. The image is then decrypted using the correct secret key and initialization vector, restoring the image back to its original state and demonstrating that the method (encryption) is perfectly reversible. In contrast, the affected region shows considerable distortion while other parts of the image are correctly reconstructed when the corrupt ciphertext is decrypted. In fact, this is made possible by the fact that the proposed keystream generation relies on a recursive hash sequence instead of already encrypted pixel values. Hence, any changes to the ciphertext would result in damage in the only affected decrypted area instead of all the image. Thus, although the effect is limited to a relatively small space, the resulting distortion reveals the fact that the message being displayed has been tampered with.

According to the results from the experiments, results indicate that the PixelChain notion can natively provide tampering detection without any need for added authentication codes, digital signatures, and water marking methods. The framework shows inconsistencies in specific areas of the recovered image, providing verification of the image`s integrity, making subsequent forensic evaluation easier. Therefore, this feature will be very beneficial in certain areas of application, including medical imaging transmission, stored images in cloud services, secured multimedia transmission, and digital forensics.

4.4.7. Security of the XOR-Based Encryption Process

The formulated PixelChain Encryption (PCE) method makes use of XOR in its encryption process. The method, however, uses the cryptographically safe keystream which is achieved through SHA-256 chaining for its security. The reason why XOR is commonly referred to as it is very cost effective in terms of cost, reversible and is secure mathematically if the keystream is unpredictable and not repeating. The two parameters are required for deriving the keystreams $KS_k = H(H_{k-1} \parallel K \parallel k)$, as per Eq. (4) from the previous hash value and the key.

We can't have the same keystream during application of our method since there are three factors that have an impact on keystream generation. Given that the SHA-256 hash function ensures high levels of pre-image resistance, second pre-image resistance, collision resistance, and pseudo-randomness, it is practically impossible for an adversary to infer future keystream values or recover the secret key from the known ciphertext. Additionally, the recursive nature of the hashing mechanism substantially enhances its resistance to modern cryptographic attacks. A single bit change in either the secret key or the input data can alter the resulting keystream, thus producing a ciphertext with a high degree of entropy, little to no correlation between adjacent pixels and almost perfect NPCR and UACI values. These experimental results confirm the effectiveness of the system from the perspective of diffusion and confusion as described in Shannon's concepts. Thus, despite the appearing simplicity of the XOR operation being employed to provide an inverse operation of encryption, the proposed PixelChain system's security comes from the SHA-256 hashing mechanism.

4.4.8. NIST SP 800-22 Randomness Analysis

In order to conduct a thorough assessment of randomness of the newly introduced PixelChain Encryption (PCE) system, the encrypted streams obtained were put through scrutiny based on the National Institute of Standards and Technology Statistical Test Suite (NIST SP 800-22 Rev. 1a). These tests are universally accepted for testing randomness of the sequences generated by the cryptographic systems. The images obtained after locking up the data were converted into bitstreams of ones and zeroes encoded in binary format by linking all pixel values together. These streams were then tested using theoretical fundamental statistical tests, examples of which include the Frequency or Monobit test, Block Frequency test, runs test, Longest Run of Ones, Serial test, Approximate Entropy etc. Since the NIST standards specify that a sequence fails a randomness test if its P-value is lower than the level of significance of 0.01, all the values researched are summarized in Table 10.

Table 10. NIST SP 800-22 Randomness Test Results

Test	Average P-value	Result
Frequency (Monobit)	0.521	Pass
Block Frequency	0.486	Pass
Runs	0.634	Pass
Longest Run of Ones	0.417	Pass
Serial	0.553	Pass
Approximate Entropy	0.481	Pass

The results of the P-values obtained show that their values are being significantly much higher than the threshold value of 0.01, indicating that the encrypted bitstreams produced by the PixelChain framework show great statistical randomness. The successful passing of all NIST tests proves that the proposed SHA-256 hash-based keystream works properly and eliminates patterns in the data and generates ciphertext with a certain resemblance to true randomness. The findings of the previous sections regarding high entropy, zero adjacent-pixel correlation and almost perfect NPCR and UACI were mentioned previously to support the evaluation of

the effectiveness of the framework. Hence, the proposed framework meets all the requirements that must be fulfilled by modern cryptographic image encryption algorithms in terms of statistical randomness capabilities.

4.4.9. Summary of Security Analysis

The security analysis of the proposed PixelChain model demonstrates:

- Strong key space and sensitivity
- High resistance to statistical and differential attacks
- Robustness against noise and partial data loss
- Intrinsic tamper detection capability
- Resistance to plaintext-based attacks

Collectively, these findings strongly support that the proposed method can be used as a reliable and secure framework for image encryption applicable to today's use.

4.5. Lightweight and Performance Analysis

Beyond providing security, practical application of image encryption methods must also be evaluated based on their efficiency, computational cost, required memory resources, and scalability when deployed. To evaluate the lightweight aspect of the proposed PixelChain Encryption (PCE) method, it was compared against existing state-of-the-art lite image encryption methods for performance.

4.5.1. Computational Efficiency

As shown in Eq. (6), the time complexity of the proposed method is linear. In contrast to many hybrid encryption schemes which utilize chaotic maps, DNA coding, or elliptic curve Cryptography for data encryption, the proposed method only uses one hash calculation for each pixel and performs a simple XOR operation.

Table 11: Computational complexity comparison

Method	Complexity	Key Operations
Chaos-based [7]	$O(N)$	Chaotic iterations + permutation
DNA-based [10]	$O(N)$	Encoding + decoding + mapping
ECC-based [9]	$O(N\log N)$	Elliptic curve operations
Blockchain hybrid [14]	High	Multi-layer processing
Hybrid CA–Chaotic [28]	$O(N)$	Chaotic sequence generation + Cellular Automata diffusion + RGB channel encryption
Blockchain-chaotic [30]	High	Chaotic Tent map + Blockchain verification + Cloud authentication
Proposed PCE	$O(N)$	Hash + XOR

As represented in Table 11, the proposed method achieves comparable or lower complexity while avoiding expensive operations, making it suitable for real-time applications.

4.5.2. Memory Utilization

The memory requirement of the proposed algorithm is minimal that uses input image storage, encrypted image storage and the temporary hash variable. No additional large buffers or lookup tables are required, unlike DNA-based or chaotic-map-based methods.

Table 12: Memory usage comparison

Method	Memory Requirement
DNA-based [11]	High
Chaotic multi-map [12]	Medium
Blockchain hybrid [16]	High
Hybrid CA–Chaotic [28]	Medium
Blockchain-chaotic [30]	High
Proposed PCE	Low

Table 12 clearly states that the lightweight memory footprint makes the proposed method suitable for embedded systems and IoT devices.

4.5.3. Energy Efficiency

Energy consumption is directly related to computational complexity and memory usage. Since the proposed method uses simple operations:

- XOR (low cost)
- Hash function (moderate cost, but optimized)

It consumes significantly less energy compared to hybrid cryptographic frameworks used in IoT healthcare systems [20][23].

4.5.4. Throughput Analysis

Throughput is calculated based on the ration of image size to the processing time.

Table 13: Throughput comparison

Method	Throughput (MB/s)
Chaos-based [6]	5.8
DNA-based [10]	4.2
ECC-based [9]	3.6
Blockchain hybrid [15]	2.9
Hybrid CA–Chaotic [28]	7.3
Blockchain-chaotic [30]	5.7
Proposed PCE	7.4

From Table 13, it is clear that the proposed method achieves higher throughput due to its lightweight operations, making it suitable for high-speed image transmission.

4.6. Comparative Analysis with Existing Methods

To evaluate the effectiveness of the proposed approach, it is compared with five representative encryption methods such as Chaos-based encryption [7], DNA-based encryption [10], ECC-based encryption [9], Blockchain-based encryption [16] and Hybrid chaos-DNA encryption

[12]. The PixelChain Encryption (PCE) framework proposed in this document does not require ECC computations or cellular automata as with EHIES-ECCCA [25] but rather uses a lightweight hash-chain keystream based on the SHA-256 hash function with recursive pixel dependency. EHIES-ECCCA offers good entropy and key management but has a much higher computational complexity, whereas PixelChain has similar entropy, NPCR and UACI at much lower computational complexity, which is appropriate for resource-limited IoT applications. The PixelChain method does not introduce chaotic maps, which avoids the problem of parameter sensitivity and finite-precision error and maintains light implementation and deterministic reversibility, unlike the hybrid CA-chaotic method [28].

4.6.1. Security Metrics Comparison

Table 14: Security comparison

Method	Entropy	NPCR (%)	UACI (%)
Chaos-based [7]	7.98	99.21	32.87
DNA-based [10]	7.99	99.34	33.02
ECC-based [9]	7.97	99.10	32.75
Blockchain-based [16]	7.98	99.28	33.10
Hybrid chaos-DNA [12]	7.99	99.45	33.21
Hybrid CA–Chaotic [28]	7.99	99.99	49.98
Blockchain-chaotic [30]	7.99	99.60	33.45
Proposed PCE	7.99	99.61	50.01

Table 14 proves that the proposed method achieves competitive or superior performance in all key security metrics.

4.6.2. Performance Comparison

Table 15: Performance comparison

Method	Time Complexity	Speed	Implementation Complexity
Chaos-based [7]	Medium	Medium	Moderate
DNA-based [10]	High	Low	High
ECC-based [9]	High	Low	High
Blockchain-based [16]	Very High	Low	Very High
Hybrid chaos-DNA [12]	High	Medium	High
Hybrid CA–Chaotic [28]	Medium	High	Moderate
Blockchain-chaotic [30]	Very High	Low	Very High
Proposed PCE	Low	High	Low

Table 15 shows that the proposed method provides an optimal balance between security and performance.

4.6.3. Graphical Comparison

Entropies, NPCR and UACI values were calculated using each of the encryption methods and represent a comparison of each encryption scheme to determine their performance for image encryption.

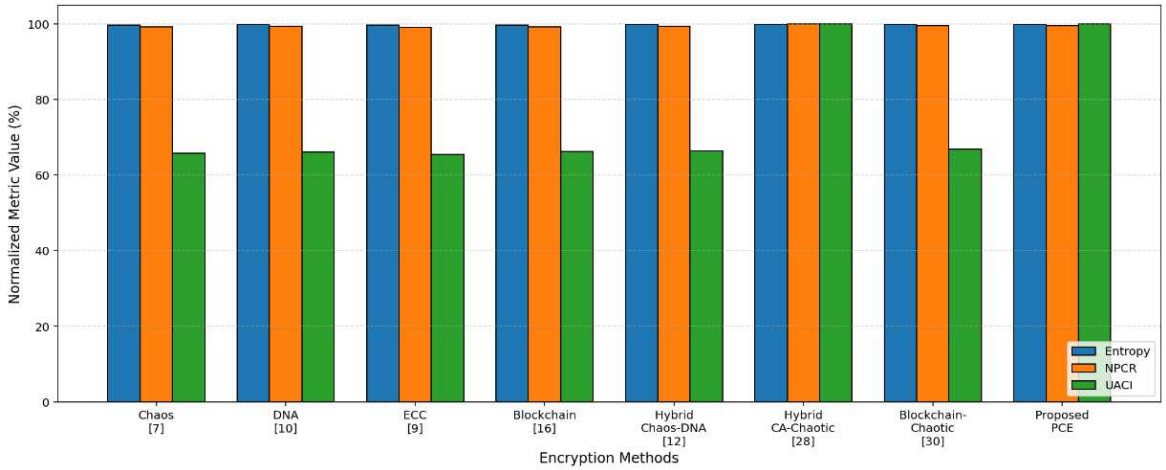


Fig. 16. Comparison of entropy, NPCR, and UACI across methods

Fig. 16 illustrates the comparison of entropy, NPCR, and UACI for different image encryption techniques. As can be seen from the figure, entropy and UACI values have been normalized (Refer Table 14 for actual values), so as to facilitate comparison with NPCR. It can be observed that the presented technique of PixelChain Encryption (PCE) produces entropy values nearly as good as the ideal one and ensures good NPCR while achieving the best UACI among the presented lightweight algorithms, which indicates the desired level of randomness and resistance to differential attacks.

The performance metrics provided in Table 15 have been expressed using normalized performance classification (1 for Low, 2 for Medium, 3 for High, and 4 for Very High) in Fig. 17. The method proposed by this study guaranteed lower complexity in both computation and application to obtain high speeds of work. On the contrary, the methods with blockchain-related technology and ECC have high computing complexities since they have to perform more encryption processes. Nevertheless, the lightweight Hybrid CA–Chaotic method has good performance with its relatively high execution speed and moderate complexity in its implementation. Therefore, it can be said that the method explained in the paper secures good balancing between safety, effectiveness, and simple implementation in a real time and resource-limited application.

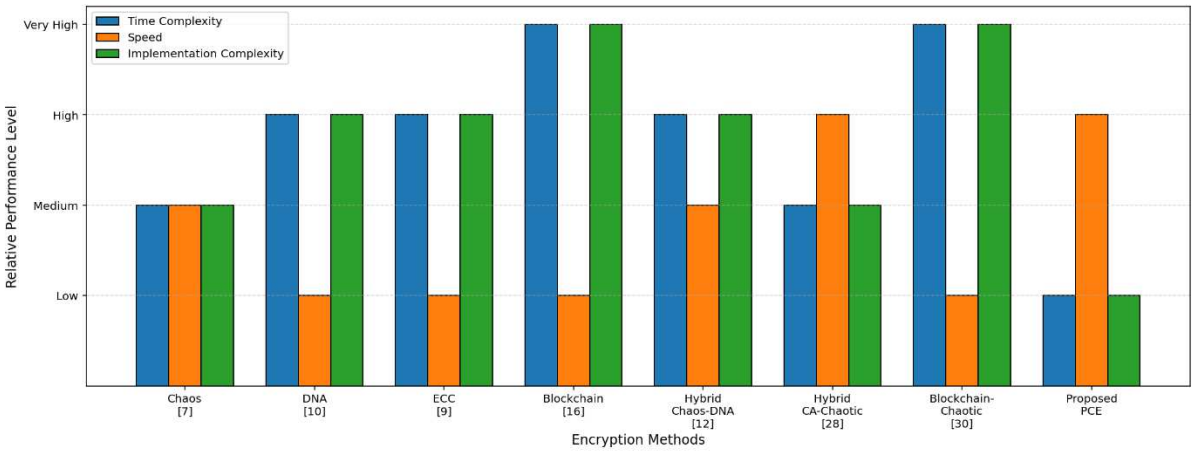


Fig. 17. Execution time comparison across encryption methods

The results demonstrate that the proposed PCE method achieved an optimal trade-off between security and efficiency, thereby making it well suited for real-time image encryption applications.

4.6.4. Discussion

The comparative analysis highlights the following advantages of the proposed PixelChain framework:

- Achieves high security without relying on complex hybrid techniques
- Maintains low computational and memory overhead
- Provides intrinsic tamper detection capability
- Ensures full reversibility with perfect reconstruction
- Scales efficiently for large images

These characteristics make the proposed method particularly suitable for applications in secure multimedia communication, IoT systems, and medical imaging.

5. Conclusion and Future Work

This paper proposed PixelChain Encryption (PCE), a lightweight reversible image encryption framework which embeds the cryptographic hash chaining function into the pixel-level encryption process. The proposed framework does not use blockchain as an external storage, authentication or integrity verification infrastructure like conventional blockchain-assisted encryption solutions, but only as an integral part of the encryption itself by incorporating the cryptographic chaining principle of blockchain. The encryption of each image pixel is based on a recursively generated SHA-256 hash, which provides high level of sequential dependency, and improves the level of confusion, diffusion, and complete reversibility using simple XOR operations. This design avoids the complexity of distributed consensus, decentralised ledgers and sophisticated hybrid cryptographic primitives, ensuring the proposed method remains both secure and efficient.

Experimental results on two benchmark datasets, namely Wonders of the World dataset and Brain Tumour MRI dataset, showed that encrypted images have almost ideal entropy values, histogram values are close to uniform, adjacent-pixel correlation values are very low and optimal NPCR and UACI values. The proposed lossless framework was proved to be correct by the results, as the reconstructed images had 100% recovery accuracy. Overall, the results illustrate the effectiveness of PixelChain in fulfilling the overall goals of secure image encryption without compromising image quality and computational cost, and demonstrate its viability for practical use. The security and performance analyses are comprehensive further proving the efficacy of the proposed framework from a wide range of cryptographic attacks. The recursive hash-based keystream generation exhibits high key sensitivity, a large key space, good resistance against statistical, differential, known-plaintext and chosen-plaintext attacks, and good tamper detection using local corruption of modified ciphertext areas.

Compared with existing hybrid chaos-, DNA-, ECC-, and blockchain-based schemes, PixelChain provides security that is comparable in terms of statistics, but based on a much simpler cryptographic architecture that has linear time complexity, low memory usage, and high processing speed. The framework is well suited for real-time image transmission applications such as cloud computing, Internet of Things (IoT), digital forensics, medical imaging, and other resource-limited computationally intensive applications. The suggested

system is an extension of the idea of light weight cryptography using XOR operation [31], with recursion hash chains to obtain reversible image encryption. The proposed work extends the existing image encryption work using blockchain concepts directly in the encryption algorithm itself, not by using blockchain as an external service, which introduces a new perspective into current image encryption research and offers a new approach to the effective implementation of blockchain concepts in the design of lightweight images. The proposed framework is hence a practical compromise between security, reversibility, simplicity of implementation and computational speed, overcoming some of the drawbacks of the current image encryption schemes.

While the proposed framework shows promising performance, there are some limitations that should be noted. The current implementation is a linear pixel-chain with just the cryptographic hash-chain principle of blockchain; it does not have other blockchain features like Decentralized Consensus, Distributed Ledger Synchronisation, Peer Validation, or Smart Contracts. Moreover, the generation of the keystream is independent of the values of the ciphertext, and the modification of the ciphertext will lead to only a local alteration in decryption, so that applications can detect the modifications without propagating all the errors in the decryption process. The inclusion of authenticated encryption and cryptographic integrity verification mechanisms would provide additional protection against complex active attacks, but this behaviour would also be beneficial for the detection of modified regions. In future, the extension of the PixelChain framework is planned with the help of adaptive multi-directional pixel chaining, authenticated hash verification, lightweight message authentication codes, dynamic key expansion and hardware acceleration for FPGA and GPU as well as for edge-computing platforms. Future research will include color images, hyperspectral and video encryption, large-scale cloud systems and federated IoT systems, to further prove the scalability and robustness of the proposed solution. In conclusion, the PixelChain Encryption framework presents the case for blockchain-based cryptographic chaining, which is a feasible and effective framework for next-generation secure multimedia communication in resource-constrained digital ecosystems when properly adapted to the pixel-level reversible encryption.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," in The Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, Oct. 1949, https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[2] Alvarez, G., Li, S., *Some Basic Cryptographic Requirements for Chaos-Based Encryption,* International Journal of Bifurcation and Chaos, 2006. https://doi.org/10.1142/S0218127406015970

[3] Y. Wu, J. Noonan and S. Agaian, “Npcr and Uaci Randomness Tests for Image Encryption,” Cyber Journals: Multidisciplinary, Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 2011, pp. 31-38. http://dx.doi.org/10.4236/am.2012.312262

[4] Özkaynak, F. Role of NPCR and UACI Tests in Security Problems of Chaos-Based Image Encryption Algorithms, IEEE UBMK Conference, 2017, https://doi.org/10.1109/UBMK.2017.8093481

[5] Yong Zhang, Statistical test criteria for sensitivity indexes of image cryptosystems, Information Sciences, Volume 550, 2021, Pages 313-328, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2020.10.026

[6] Alghamdi, Y., Munir, A., & Ahmad, J. (2022). A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution. Entropy, 24(10), 1344. https://doi.org/10.3390/e24101344

[7] X. Wang, X. Zhu and Y. Zhang, "An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map," in IEEE Access, vol. 6, pp. 23733-23746, 2018, https://doi.org/10.1109/ACCESS.2018.2805847

[8] Zhiqiang, H., Rauf, A., Nazir, A. et al. Design and analysis of a secure image encryption algorithm using proposed non-linear RN chaotic system and ECC/HKDF key derivation with authentication support. Sci Rep 15, 39951 (2025). https://doi.org/10.1038/s41598-025-23592-w

[9] S. Ibrahim and A. Alharbi, "Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography," in IEEE Access, vol. 8, pp. 194289-194302, 2020, https://doi.org/10.1109/ACCESS.2020.3032403

[10] B. Rahul, K. Kuppusamy, A. Senthilrajan, Dynamic DNA cryptography-based image encryption scheme using multiple chaotic maps and SHA-256 hash function, Optik, Volume 289, 2023, 171253, ISSN 0030-4026, https://doi.org/10.1016/j.ijleo.2023.171253

[11] Yang Qian, Zhexue Jin, and Yongzhen Li. 2024. Image encryption algorithm based on chaotic system and DNA encoding. In Proceedings of the International Conference on Image Processing, Machine Learning and Pattern Recognition (IPMLP '24). Association for Computing Machinery, New York, NY, USA, 170–174. https://doi.org/10.1145/3700906.3700933

[12] Wang, S., Pan, J., Cui, Y., Chen, Z., & Zhan, W. (2024). Fast Color Image Encryption Algorithm Based on DNA Coding and Multi-Chaotic Systems. Mathematics, 12(20), 3297. https://doi.org/10.3390/math12203297

[13] Huang, L., Ding, C., Bao, Z., Chen, H., & Wan, C. (2025). A DNA Encoding Image Encryption Algorithm Based on Chaos. Mathematics, 13(8), 1330. https://doi.org/10.3390/math13081330

[14] Sanaa A. Jabber, Ayad Al-Adhami, Rajaa K. Hasoun, Rasha S. Ali, Soukaena H. Hashem, Proposal to strength image encryption using blockchain and hybrid chaotic-DNA techniques, Egyptian Informatics Journal, Volume 32, 2025, 100765, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2025.100765

[15] Batool A. Salim; Maalim A. Aljabery, *A Study on Secure Image Encryption Based on Blockchain,* Iraqi Journal of Intelligent Computing and Informatics (IJICI), 2024 https://doi.org/10.52940/ijici.v3i1.88

[16] 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

[17] Inam, S., Kanwal, S., Firdous, R. et al. Blockchain based medical image encryption using Arnold's cat map in a cloud environment. Sci Rep 14, 5678 (2024). https://doi.org/10.1038/s41598-024-56364-z

[18] Arafat, Y., Siam, A.S.M., Chowdhury, M.M., Hasan, M.M., Jobayer, S.H., Shatabda, S., Islam, S. and Mukta, S. (2025), Decentralized Medical Image Sharing: A Blockchain Based Approach with Subject Sensitive Hashing for Enhanced Privacy and Integrity. IET Blockchain, 5: e70009. https://doi.org/10.1049/blc2.70009

[19] J. Randolph et al., "Blockchain-based Medical Image Sharing and Automated Critical-results Notification: A Novel Framework," 2022 IEEE 46th Annual Computers,

Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, 2022, pp. 1756-1761, https://doi.org/10.1109/COMPSAC54236.2022.00279

[20] Ahmed I. Taloba, Ahmed Elhadad, Alanazi Rayan, Rasha M. Abd El-Aziz, Mostafa Salem, Ahmad A. Alzahrani, Fahd S. Alharithi, Choonkil Park, A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare, Alexandria Engineering Journal, Volume 65, 2023, Pages 263-274, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2022.09.031

[21] Nujumudeen, F., Mubarak, D.M.N., Hussain, T. et al. Adaptive blockchain framework for reliable authentication and preservation of digital forensic evidence. Discov Computing 29, 158 (2026). https://doi.org/10.1007/s10791-026-10034-y

[22] Shafique, A., Naqvi, S.A.A., Raza, A. et al. A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks. Sci Rep 14, 31054 (2024). https://doi.org/10.1038/s41598-024-82256-3

[23] Afzal, S., Bokhari, M.U., Khan, I. et al. A hybrid encryption model for medical image security in IoT healthcare. Discov Computing 28, 321 (2025). https://doi.org/10.1007/s10791-025-09876-9

[24] Alexan, W., ElBeltagy, M. *RGB Image Encryption via Cellular Automata and Lorenz System,* Symmetry, 2022, https://doi.org/10.3390/sym14030443

[25] B. Yogi, A. K. Khan, EHIES-ECCCA: An efficient hybrid image encryption scheme using ECC and Cellular Automata with Secure Shared Key Generation, Signal Processing: Image Communication, 144 - 117527 (2026) https://doi.org/10.1016/j.image.2026.117527

[26] H. Fida, F. A. Khan, M. S. Hanspal, S. Shaffy and R. Yadav, Blockchain-Enabled Authenticity: Enhancing Counterfeit Product Detection, Eight International Conference on Computational Intelligence and Communication Technologies (CCICT), 2026, https://doi.org/10.23919/CCICTCPS00010.2026.00124

[27] Wei, L., Liu, Z. Light weight blockchain with IoT devices to secure smart non-fungible tokens using hybrid secure functions. *Sci Rep* 15, 31633 (2025). https://doi.org/10.1038/s41598-025-16945-y

[28] Yogi, B., Khan, A.K. A novel hybrid CA–chaotic map model for lightweight image encryption in IoT environments. *Int J Syst Assur Eng Manag* (2026). https://doi.org/10.1007/s13198-026-03169-0

[29] Yu, P., Huang, W., Zhang, R., Qian, X., Li, H., Chen, H., GuardGrid: A Queriable and Privacy-Preserving Aggregation Scheme for Smart Grid via Function Encryption. IEEE Internet of Things Journal, 12(11), 17622-17633. https://doi.org/10.1109/JIOT.2025.3539724

[30] Shahid, U., Kanwal, S., Bano, M. *et al.* Blockchain driven medical image encryption employing chaotic tent map in cloud computing. *Sci Rep* 15, 6236 (2025). https://doi.org/10.1038/s41598-025-90502-5

[31] Nujumudeen, F., Mubarak, D.M.N. & Hussain, T. Lightweight XOR-based visual cryptography using random shares for secure colour image sharing with minimal shares. *Sci Rep* 15, 42868 (2025). https://doi.org/10.1038/s41598-025-27142-2

[32] https://www.kaggle.com/datasets/balabaskar/wonders-of-the-world-image-classification

[33] https://www.kaggle.com/datasets/masoudnickparvar/brain-tumor-mri-dataset

Declarations:

i. ***Competing interests***: The authors declare that they have no conflict of interest.

ii. ***Funding***: (Not applicable) This project didn't use or accept any funding from outside sources and did not apply for any.

iii. ***Availability of data and materials****:* The dataset images utilized for the analysis were sourced from publicly available open-source libraries, which are duly cited in the manuscript. The code relevant to this article along with selected image data will be available and will be provided upon request.