Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.065356

ARTICLE

Secure Medical Image Transmission Using Chaotic Encryption and Blockchain-Based Integrity Verification

Rim Amdouni[1,2,*], **Mahdi Madani**[3], **Mohamed Ali Hajjaji**[1,4], **El Bay Bourennane**[3] **and Mohamed Atri**[5]

[1]Research Laboratory in Algebra Numbers Theory and Intelligent Systems (RLANTIS), University of Monastir, Monastir, 5000, Tunisia
[2]Faculty of Sciences of Monastir, University of Monastir, Monastir, 5000, Tunisia
[3]Laboratoire ImViA (EA 7535) 9, DIJON CEDEX, Avenue Alain Savary, BP 47870, 21078, France
[4]Higher Institute of Applied Sciences and Technology, Sousse University, Sousse, 4003, Tunisia
[5]Computer Engineering Department, College of Computer Science, King Khalid University, Abha, 62421, Saudi Arabia

*Corresponding Author: Rim Amdouni. Email: rimamdouni0@gmail.com

Received: 10 March 2025; Accepted: 05 June 2025; Published: 30 July 2025

ABSTRACT: Ensuring the integrity and confidentiality of patient medical information is a critical priority in the healthcare sector. In the context of security, this paper proposes a novel encryption algorithm that integrates Blockchain technology, aiming to improve the security and privacy of transmitted data. The proposed encryption algorithm is a block-cipher image encryption scheme based on different chaotic maps: The logistic Map, the Tent Map, and the Henon Map used to generate three encryption keys. The proposed block-cipher system employs the Hilbert curve to perform permutation while a generated chaos-based S-Box is used to perform substitution. Furthermore, the integration of a Blockchain-based solution for securing data transmission and communication between nodes and authenticating the encrypted medical image's authenticity adds a layer of security to our proposed method. Our proposed cryptosystem is divided into two principal modules presented as a pseudo-random number generator (PRNG) used for key generation and an encryption and decryption system based on the properties of confusion and diffusion. The security analysis and experimental tests for the proposed algorithm show that the average value of the information entropy of the encrypted images is 7.9993, the Number of Pixels Change Rate (NPCR) values are over 99.5% and the Unified Average Changing Intensity (UACI) values are greater than 33%. These results prove the strength of our proposed approach, demonstrating that it can significantly enhance the security of encrypted images.

KEYWORDS: Medical image encryption; chaotic maps; blockchain; substitution-Box; security; integrity

1 Introduction

The rapid advancement of the Internet of Things (IoT) has changed how we interact with smart devices, affecting many aspects of our daily lives. This concept facilitates interconnectedness and data exchange among millions of smart devices. It can be conceptualized as a network of physical devices capable of capturing and sharing various types of information in any location, time, medium, or context [1]. With advancements in technologies such as IoT, the healthcare sector is experiencing rapid growth. The primary objective of integrating IoT into healthcare facilities is to enable remote accessibility, facilitating seamless communication between doctors and patients via the Internet, particularly in emergency situations. Advancements in camera technology have brought IoT to a new dimension, but security remains an issue. The centralized storage of sensitive health data might expose personal information to unauthorized access.

Moreover, the prevalent IoT architecture heavily relies on centralization, entrusting a single entity with the administration of healthcare data, thereby introducing a single point of failure. Implementing a Blockchain network stands out as one of the most effective approaches, given its role as a distributed database in this scenario. It is suggested that it can serve as a secure and efficient foundation for numerous IoT applications. It offers crucial features including privacy protection, immutability, and decentralization, which greatly enhance the security of data sharing [2–6]. Many existing works rely primarily on the security attribute of Blockchain [7–11]. The authors in [12] address the processing of multimedia data in the context of healthcare systems and present a secure framework for healthcare. leveraging blockchain technology to ensure confidentiality and transparency between patients and intermediaries. Specifically, they proposed a security framework for healthcare utilizing blockchain techniques, where each data is hashed to establish secure chains of records stored across all patient networks. The paper [13] suggested a Blockchain model framework for securing reported patient status health data thereby guaranteeing the security of health data. The method is a (BSDMF): Blockchain-assisted Secure Data Management Framework tailored for health information within the Internet of Medical Things (IoMT). The framework aims to facilitate the exchange of patient data while improving security, scalability, and data accessibility in healthcare environments. It provides secure data management among embedded medical devices, cloud servers, and personal servers. Leveraging the security framework based on IoMT, the authors employed BC technology to guarantee the security of data transmission and effective data management across interconnected nodes. Azbeg et al. [14] introduced BlockMedCare, a secure healthcare system integrating IoT medical devices with BC and IPFS technologies. This solution is constructed with the objective of efficiently collecting and sharing patient data with medical teams, ensuring a high level of security for storing and sharing sensitive information. The system is divided into three key parts. The first part is devoted to data collection, utilizing IoT healthcare devices to ensure accurate and reliable data acquisition. The second part is dedicated to securely sharing data, with blockchain technology ensuring the integrity and confidentiality of shared information. Lastly, the third part handles data storage, utilizing IPFS for efficient and decentralized storage of patient data. Therefore, by primarily leveraging the security attribute of Blockchain, some works may not suffice for certain use cases. However, there has been a lack of extensive research conducted regarding security and privacy within the domain of IoT in healthcare.

Some research efforts have been dedicated to the security domain [15–19]. To ensure security and privacy for telehealth services, Anand et al. [20] proposed a sophisticated technique to enhance the security of medical images in telemedicine by leveraging discrete wavelet transform (DWT) and singular value decomposition (SVD) for watermarking. The method excels in providing enhanced security, robust resistance to various signal processing attacks, and high imperceptibility, which are crucial for ensuring the integrity and confidentiality of medical data. Despite its strengths, the method's complexity can lead to increased computational demands, potentially limiting its application in real-time environments or when scaling large datasets. Additionally, while robust, the approach may not guarantee comprehensive defense against all novel attack vectors, emphasizing the need for continuous updates. The paper in [21] proposed a medical image encryption scheme combining DNA computing and chaotic maps to enhance security in telemedicine. The method ensures high entropy, low pixel correlation, and strong key sensitivity, making it resistant to brute-force, statistical, and differential attacks. It is computationally efficient and suitable for cloud-based healthcare applications. However, its high computational complexity may limit use in resource-constrained devices, and key management challenges could impact synchronization during decryption. Additionally, it lacks explicit countermeasures against quantum computing threats. Despite these limitations, the method provides robust encryption for securing medical images in modern telemedicine systems. In [22], the authors introduced a novel approach to medical image cryptography within the context of smart

IoT healthcare applications, utilizing a Neural Stacked Auto-Encoder (SAE) framework to leverage deep extracted features. The proposed cryptosystem employs the network SAE to generate two chaotic random matrices. They used the first matrix to create a comprehensive shuffling matrix, which alters the location of pixels within the digital input image. Subsequently, the medical image is shuffled using this matrix, resulting in a rearranged image where pixel values are altered based on their corresponding positions in the shuffling matrix. The second set of chaotic random matrices generates independent sequences, which remove the correlation among the shuffled cipher and original images. Each chaotic sequence used to further confuse the permuted medical image. In [23], authors proposed a cryptosystem for enciphering different types of medical images. A hybrid mechanism was created to scramble two plain images in a separate way using chaotic maps and combining them to improve the robustness and security of the cryptosystem. The first image undergoes diffusion and permutation through the Logistic-May map and the Henon map. The second image exhibits a scrambled arrangement of pixels using the Logistic-Sine system. Lastly, a non-linear formula that is based on Cramer's rule was used for fusing both ciphered images, resulting in two hybrid encrypted images.

Indeed, numerous security solutions have been proposed in the literature, among them encryption and blockchain technology stand out prominently [24–27]. In response to cybersecurity challenges, Doreen Hephzibah Miriam et al. [28] present a novel security enhancement approach involving blockchain-based data sharing within healthcare systems. It introduces the Lionized Golden Eagle-based Homomorphic Elapid Security (LGE-HES) algorithm. This algorithm combines the LGE and HES techniques. The HES technique relies on a confusion process, utilizing S-Box components in both the original and encrypted data. On the other hand, the LGE technique is employed for optimal key selection, aiming to select the most suitable private and public keys for transmission and reception within the blockchain network. Several issues arise in this work, including the overall key size and the computational complexity, which tend to be significant. The work in [29] introduced a Blockchain-based chaotic deep Generative Adversarial Network (GAN) encryption scheme. This scheme leverages blockchain technology to protect personal information and to authenticate the veracity of data. Medical images are ciphered using the chaotic deep GAN based on the principles of confusion, substitution, and diffusion before storing them in the cloud. This scheme generates secret keys that are specific to image with the objective of enhancing the system's ability against attacks. The data sender sends the ciphered data to the cloud server, signs the ID of the cipher image, and then stores it on the blockchain while the data user requests the data from the cloud and uses the signature to verify the encrypted image's authenticity. In the paper [30], the authors proposed a Blockchain-based Chaotic Arnold's Cat Map Encryption Scheme (BCAES). This scheme is used to encrypt the medical image utilizing Arnold's cat map encryption scheme. Subsequently, the ciphered image is transmitted to the Cloud Server, while the signature of the plain image is stored in the Blockchain. The signature is made using the SHA-256 hash function. The image encryption algorithm goes through three phases: confusion, using the henon, permutation, and lastly, a diffusion phase using a novel Arnold's cat map, which is XORed with the previous results. This work has used classical chaotic systems while these systems have some limitations including periodicity, vulnerability to phase space destruction, and low Lyapunov exponents. In the article [31], authors have proposed an image encryption model, named Multi-Chaotic Maps and Blockchain (MCBE). The encryption process was divided into two phases. The confusion phase: a random permutation is employed to scramble the original image pixels. The diffusion phase: a logistic map and tent map are applied row-wise and column-wise. Additionally, blockchain is integrated using the SHA-256 hash function, enhancing the model's efficiency and increasing security. Finally, the encrypted image data blocks are merged to form the entire encrypted image.

In this context, we introduce a novel encryption algorithm that integrates Blockchain technology, intending to enhance the security and privacy of data transmission.

The main purpose of our contribution is:

- Implementing an innovative block cipher encryption scheme for medical images based on chaos theory.
- Encrypting the medical images and generating digital signatures utilizing hash functions and storing them to authenticate the cipher image's authenticity.
- Proposing a blockchain-based solution that transmits the medical images into the network after encrypting them, and secure communication between the nodes.
- The remainder of this work is structured as follows. Section 2 presents the necessary background and preliminaries. Section 3 outlines the proposed methodology, followed by the proposed cryptosystem in Section 4. A description of the signature generation is discussed in Section 5. The results analysis is described in Section 6. In Section 7, a comparative study is discussed and finally, conclusions are drawn in Section 8.

2 Preliminaries

After outlining the introduction and organization of the paper, this section begins with an overview of some topics. This serves as a background and a preamble to the concepts utilized in the proposed method.

2.1 Chaotic Maps: Logistic Map (LM)

The LM is presented as a second-order polynomial map, characterized by its one-dimensional discrete-time nonlinear nature [32]. It serves as a thoroughly documented example of a discrete system demonstrating chaotic behaviour. It stands out as one of the simplest and most transparent systems showcasing the transition from order to chaos [33]. The LM is defined by the Eq. (1):

$$x_{n+1} = r\,x_n\,(1 - x_n) \tag{1}$$

With r presented as a control parameter in the range of [0, 4]. The generated chaotic sequence is presented by x_n with values ranging between 0 and 1. The logistic map shows chaotic behavior when the control parameter r varies between 3.57 and 4.

Fig. 1 displays the bifurcation diagram of the one-dimensional LM. The diagram reveals periodic windows appearing at fixed intervals. These periodic windows must be eliminated as their presence prevents the cipher image from behaving randomly, ultimately leading to an inefficient encryption process.

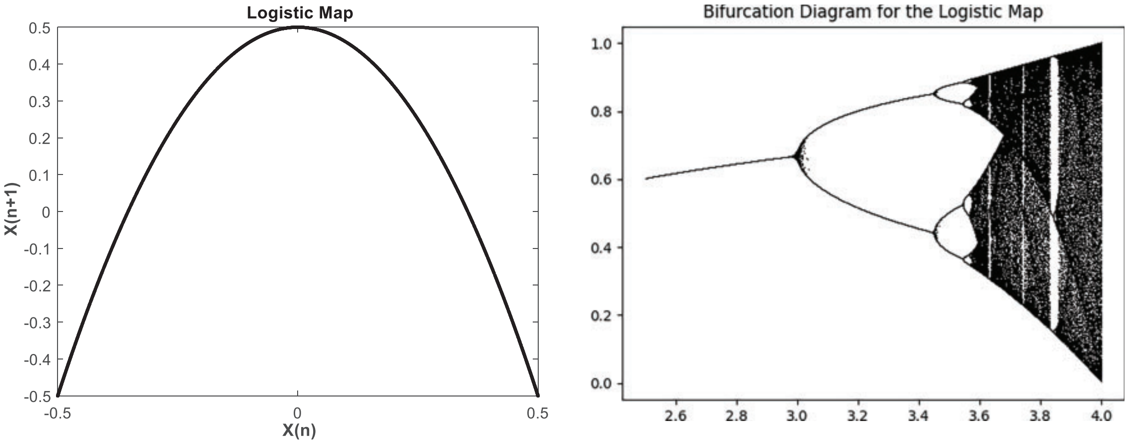


Figure 1: The Logistic Map function and Bifurcation diagram with r between 2.5 and 4

2.2 Chaotic Maps: Tent Map (TM)

The tent map stands out as one of the most straightforward 1-D, non-invertible, piecewise linear discrete maps showing chaotic dynamics [34]. The chaotic tent map equation is denoted by Eq. (2):

$$x_{i+1} = f\left(x_i, \mu\right) \tag{2}$$

where $f\left(x_i, \mu\right)$ is defined as:

$$f\left(x_i, \mu\right) = \begin{cases} \mu \times x_i & If\ x_i < 0.5, \\ \mu \times \left(1 - x_i\right) & If\ x_i \geq 0.5. \end{cases} \tag{3}$$

In which, $x_i \in (0, 1)$ for $i \geq 0$ is referred to as the state of the system. It should be noted that $\mu \in [0, 2]$ is the control parameter and x_0 is the initial value.

Fig. 2 illustrates the bifurcation diagram of the Tent map, highlighting its dynamic behavior and broad chaotic regime. The diagram clearly reveals the system's transition into chaos, with the bifurcation phenomenon indicating its inherently chaotic nature.

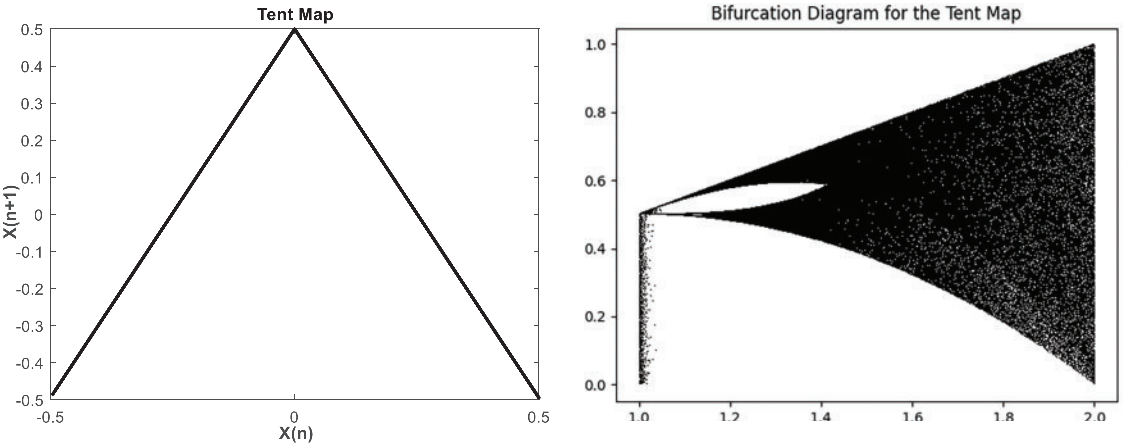


Figure 2: The Tent Map function and Bifurcation diagram with μ between 1 and 2

2.3 Chaotic Maps: Henon Map (HM)

The Henon map, which was first introduced by Michel Henon in 1976, is a straightforward 2D discrete chaotic system [35]. It serves as a discrete dynamic map demonstrating chaotic behavior, being highly sensitive to its initial conditions.

Mathematically, the Henon map is presented as follows:

$$\begin{aligned} x_{(n+1)} &= 1 - a x_n^2 + y_n \\ y_{(n+1)} &= b x_n \end{aligned} \tag{4}$$

The variables $\left(x_{(n)}, y_{(n)}\right) \in \mathbb{R}^2$ are presented as the state values of the system, while a and b serve as the control parameters. The Henon Map depends on these two parameters, which are explored across various numerical values. However, the system exhibits chaotic behavior specifically when $a = 1.4$ and $b = 0.3$. Fig. 3 illustrates the Henon map attractor on the (x, y) plane.

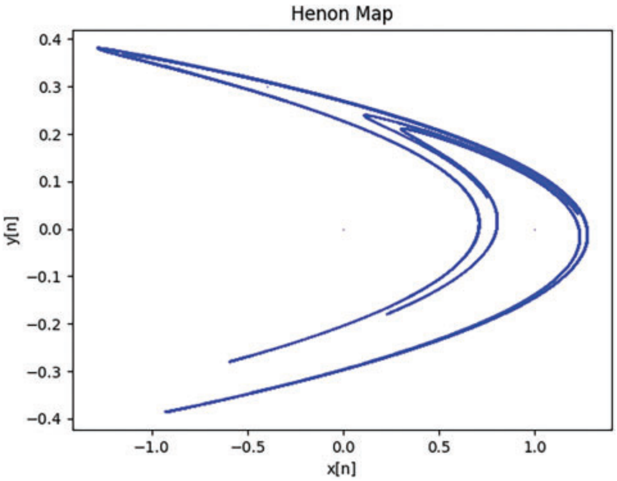


Figure 3: Diagram of henon map for $a = 1.4$ and $b = 0.3$

2.4 Scan Pattern Method

The Scan method is a two-dimensional spatial access technique designed to generate diverse scanning trajectories across a matrix of size M × M. It offers a systematic and efficient approach for constructing various scanning paths, which are particularly useful in image processing applications. In the context of image encryption, these scan patterns play a critical role in the pixel scrambling process, enhancing diffusion and security. Fig. 4 presents several commonly employed scan patterns that are frequently integrated into encryption schemes [36,37].

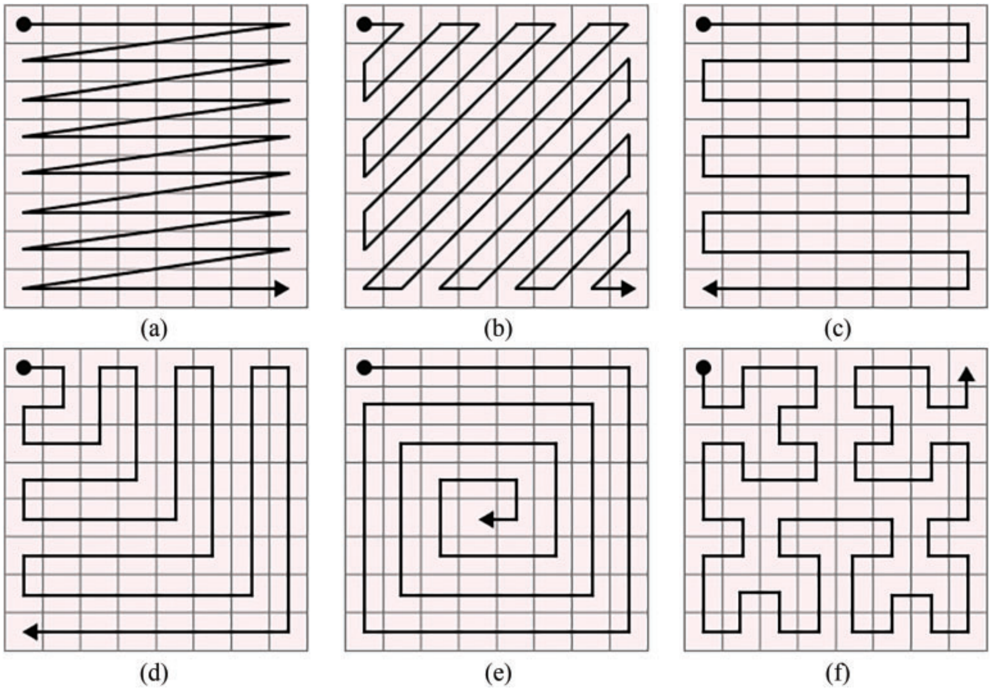


Figure 4: Different scan patterns

In this work, image scrambling is achieved utilizing the Hilbert curve, ensuring only pixel-level permutations. The primary reason for using the Hilbert curve is its easy to generate. Additionally, when applied to the image, it better utilizes the coherence of neighboring pixels compared to the traditional scan-line approach, resulting in greater image confusion. The Hilbert curve is a type of SCAN pattern that scans a 2 m × 2 m array of points as shown in Fig. 4f. The scan path can be constructed starting from the right-top (RT), left-top (LT), right-bottom (RB), or the left-bottom (LB) corners of the square grid. In the scan method, the Hilbert curve is employed to shuffle the pixel positions of the image, resulting in a scrambled image. Fig. 5a–d depicts the Hilbert curves of orders 1, 2, 3, and 4, respectively, corresponding to square grids of sizes 2 × 2, 4 × 4, 8 × 8, and 16 × 16.

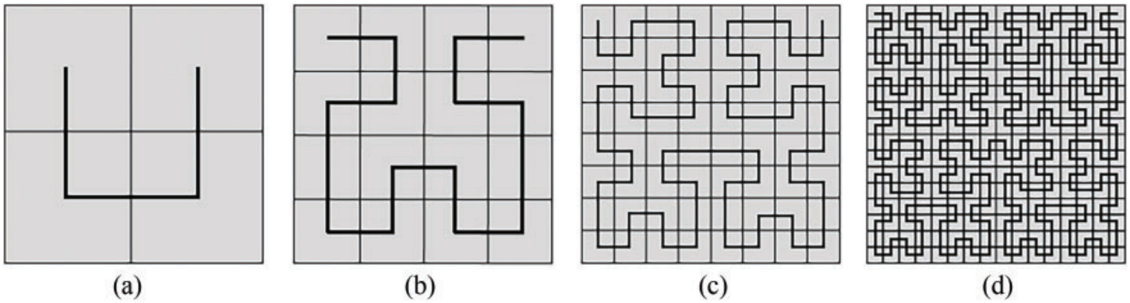


Figure 5: The Hilbert curves of orders 1, 2, 3, and 4 correspond to square grids of sizes 2 × 2, 4 × 4, 8 × 8, and 16 × 16, respectively

2.5 Blockchain Technology

Blockchain technology serves as a mechanism for storing and transmitting data, primarily aimed at facilitating transactions without the necessity of an intermediary, a concept known as decentralization [38]. The blockchain is a technology that enables decentralized and secure storage of data by utilizing blocks that are linked together. Its application extends to ensuring the security and transparency of data gathered by interconnected objects within IoT networks [39]. In Blockchain, information such as transactions is stored within the blocks of the blockchain. Each block serves as a grouping of the most recent transactions that await validation and undergo cryptographic processing [40]. A block is divided into two parts. The first part is the header containing identification information used to prove the block's authenticity and transactions it contains. The second part is the body that contains all recent transactions.

Fig. 6 illustrates an overview of the fundamental architecture of a blockchain. The header comprises the hash value of the previous block, the current block, and a timestamp. The body section encompasses transactions or data.

Blockchain technology relies on cryptography, employing encryption through advanced algorithms to protect data and ensure its integrity. This cryptography guarantees secure communication, even in scenarios where a malicious entity gains access to confidential data on a device. The cryptography primitives used in blockchain are hash functions, asymmetric encryption, and digital signatures.

A hash function is employed to transform data of variable size into fixed-size output data. It is applied to both transactions and blocks. Any modification made to the data will impact the hash of the data, thereby affecting the final hash because the mentioned function merges blocks. This function provides a double layer of protection to the data and renders blockchain blocks resistant to tampering and manipulation.

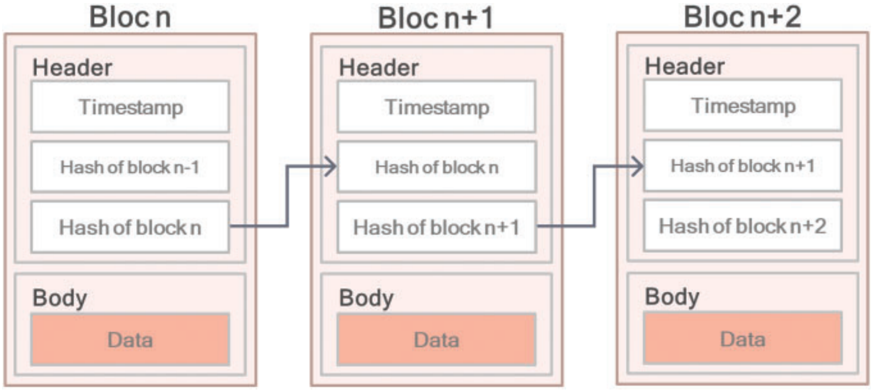


Figure 6: General structure of a blockchain

In asymmetric encryption, a key pair is necessary, comprising a private and a public key. The public one can be exchanged openly, whereas the private one has to remain exclusive to its owner, ensuring that it cannot be derived from the public key.

3 Methodology

The primary objective of this study is to develop a novel encryption framework that incorporates blockchain technology to enhance the security and privacy of data transmission, while ensuring the confidentiality and integrity of medical images. The integration of blockchain is motivated by its decentralized architecture, immutability, and ability to provide a tamper-proof and permanent record of information.

Fig. 7 shows the proposed architecture of a blockchain method used in healthcare systems and enhanced with encryption.

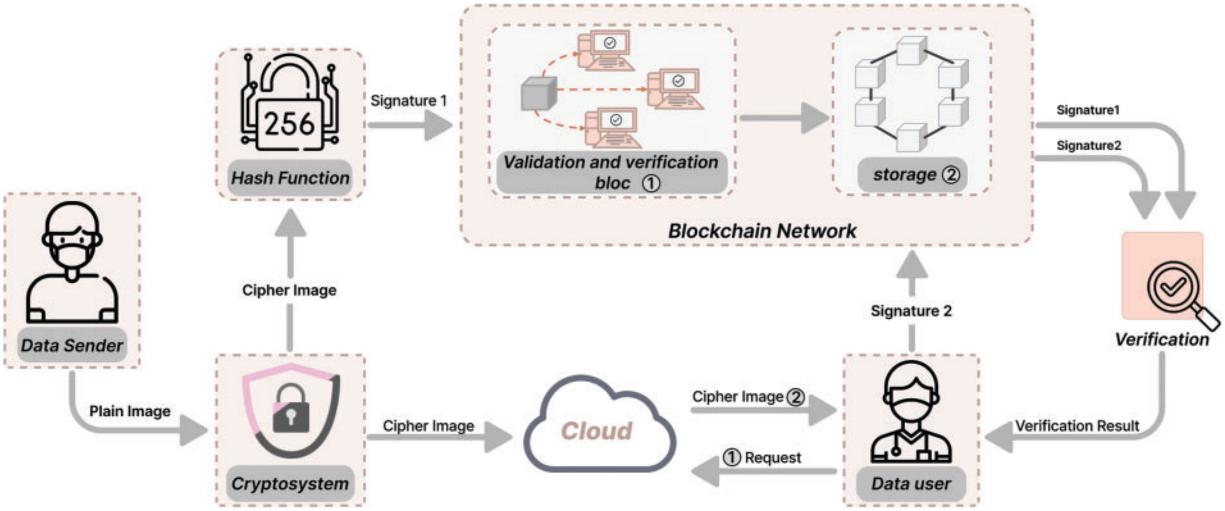


Figure 7: The proposed architecture of the blockchain method used in healthcare systems

Initially, the sender generates a digital signature of the medical image using the SHA-256 hash function and subsequently encrypts the image using the proposed encryption scheme. The resulting ciphertext is uploaded to a cloud server, while the corresponding digital signature is recorded on the blockchain. When a data user requests access to the medical image, the encrypted file is retrieved from the cloud and delivered to the user. Upon receipt, the user applies the decryption algorithm to recover the image. Prior to decryption, the user verifies the integrity and authenticity of the encrypted image by submitting it to the blockchain. The blockchain performs the verification using the stored signature and returns a confirmation message either "yes" or "no" indicating whether the image has maintained its authenticity. The key features of the proposed model are summarized as follows:

- **Data Sender (Patient):** Encrypts medical images with the proposed encryption algorithm, sends the obtained data to the Cloud Server, and then signs the ciphered image to finally store it in the Blockchain network.
- **Data User (Health Service):** Requests the data from the cloud server to obtain the ciphered image. In addition, the user verifies the authenticity of the cipher image by matching the cipher image's signature stored in the blockchain.
- **Cloud Server (CS):** Stores large amounts of medical image data and searches and sends the associated encrypted images due to the data user's request.
- **Blockchain:** Checks the stored signature when it receives a request from the data user to confirm the validity of the encrypted image. If the condition is true, the result is 1; else, the result is 0.
- **Encryption and Decryption Process:** Before transmission to the Cloud Server, the medical image undergoes encryption using our proposed encryption algorithm that is based on chaotic maps. The reverse process, which is for retrieving the medical image, is the decryption process.

4 Proposed Cryptosystem

This section presents the proposed algorithm for image encryption and decryption based on chaotic maps. The algorithm comprises two primary phases. In the first phase, three initial chaotic keys are employed to generate high-quality encryption keys using three distinct chaotic maps: the Logistic map, the Tent map, and the Henon map. The second phase involves the application of the cryptosystem, which leverages the principles of confusion and diffusion to ensure robust security. Fig. 8 illustrates the overall structure of the proposed encryption and decryption framework.

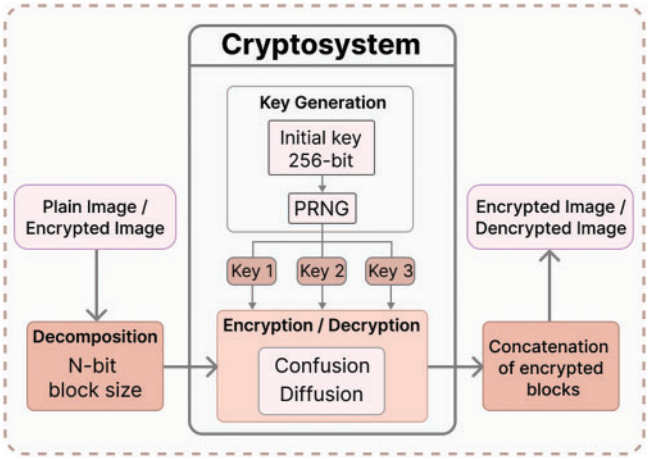


Figure 8: General view of the proposed cryptosystem

4.1 Key Generation

To enhance the robustness of keys against hackers, we have proposed a Pseudo-Random Number Generator (PRNG) that produces deterministic random number sequences based on various chaotic maps. In this paper, we have chosen three distinct chaos maps for analysis and design: the LM, the TM, and the HM. These maps exhibit strong chaotic characteristics, rendering their chaotic orbits highly unpredictable.

The PRNG necessitates initialization with an initial state to generate a set of numbers displaying robust random behavior. The input image's hash value was generated using SHA-256, producing a 256-bit (32-character) result. This hash value is then divided into four parts. To implement the confusion and diffusion processes, the three chaotic maps are utilized. Each 32 bits of hash value is employed to generate the initial conditions for each chaotic map. Fig. 9 illustrates the block diagram of the key generation procedure.

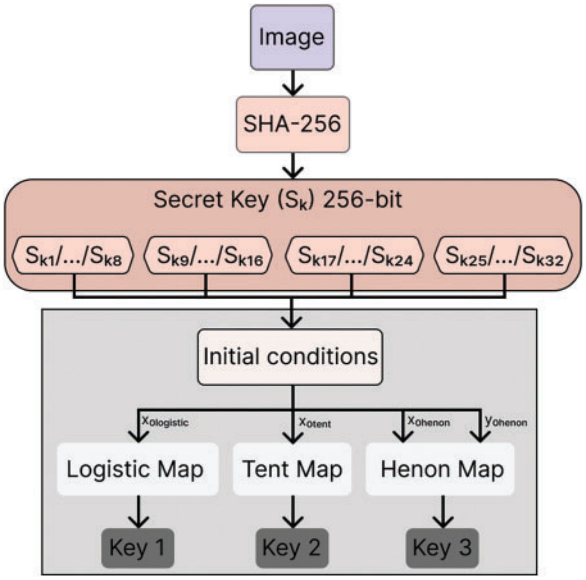


Figure 9: Key generation module used for feeding the encryption process

The generated sequence, referred to as the 256-bit secret key (S_k), is divided into 8-bit blocks (S_{ki}), allowing S_k to be expressed as described in the equation below. These new blocks (S_{ki}) will be utilized to create the initial map values.

$$S_k = S_{k1}|S_{k2}|S_{k3}|S_{k4}|\ldots|S_{k32} \tag{5}$$

$$x_{0\log istic} = x'_{0\log istic} + \frac{S_{k1} \oplus S_{k2} \oplus \ldots \oplus S_{k8}}{256} \tag{6}$$

$$x_{0tent} = x'_{0tent} + \frac{S_{k9} \oplus S_{k10} \oplus \ldots \oplus S_{k16}}{256} \tag{7}$$

$$x_{0henon} = x'_{0henon} + \frac{S_{k17} \oplus S_{k18} \oplus \ldots \oplus S_{k24}}{256} \tag{8}$$

$$y_{0henon} = y'_{0henon} + \frac{S_{k25} \oplus S_{k26} \oplus \ldots \oplus S_{k32}}{256} \tag{9}$$

4.2 Encryption Process

To illustrate the effectiveness and practical applicability of the proposed approach, a basic image encryption algorithm based on confusion and diffusion principles is developed. The input image I, with dimensions M × N × L, undergoes encryption, where L represents the number of channels, and M and N denote the image height and width, respectively. For grayscale images, the encryption is applied directly. In the case of color images, each of the three RGB channels; Red, Green, and Blue is encrypted independently. The resulting encrypted channels are then recombined to produce the final ciphertext image. Prior to encryption, each color component is divided into fixed-size blocks of 512 bits. If the image data does not evenly divide into 512-bit blocks, the final block is zero-padded to meet the required length. Fig. 10 presents an overview of the general architecture of the proposed encryption process.

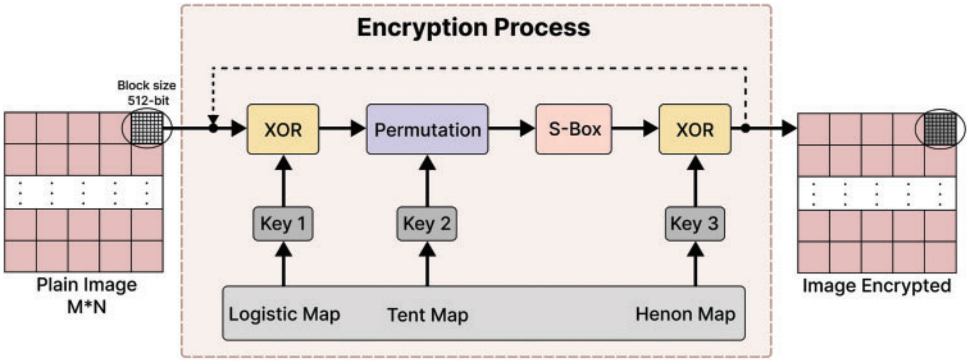


Figure 10: General architecture of our image encryption process

As shown in Fig. 10, the encryption process is split into four operations.

- **Operation 1 (Diffusion):** The first operation is an XOR operation in which we applied an XOR between a block of plaintext image and a block of the key 'key1' generated by the logistic map. This operation is important for our work because it masks the original pixel values, eliminates the redundant pixels, and equalizes grey levels throughout the image.
- **Operation 2 (Confusion):** The next operation is a level-pixel permutation. Permutation is an efficient technique for shuffling the pixel positions, effectively reducing the correlation between adjacent pixels in the original image. That operation utilized the Hilbert curve of order 3 and the 'key2' generated by the tent map. Based on the key block's parity, the medical image's pixels undergo scrambling by starting the Hilbert curve from the top-left (TL) or the bottom-right (BR).
  The process is illustrated in Fig. 11a,b. The Hilbert curve starts from the top-left if the key value is even. Conversely, if the key value is odd, it starts from the top-right:
- **Operation 3 (Diffusion):** This operation involves substituting all the permuted pixels from the previous stage using an S-Box. We utilized a dynamic S-box generated via the logistic map. This dynamic S-box serves to enhance the security of the proposed system. Therefore, the logistic map is applied iteratively to produce a random vector of size 256. This vector is then arranged in a matrix of size 16 × 16 to create the S-box. Consequently, to enhance the randomness and complexities of the proposed scheme, this S-box is applied to the diffused layer to produce a highly secure cipher image.
  Each pixel of the block is replaced by a specific value from the S-Box as mentioned in Eq. (10):

$$S_p = SBox\left(P_{ij}\right) \tag{10}$$

where S_p represents the substituted pixel, P denotes the pixel obtained from the previous step, and i and j represent the index position. Table 1 illustrates the S-Box generated in the standard 16 × 16 format.

- **Operation 4 (Diffusion):** This operation is another XOR operation that is performed among the block obtained in the previous step and the key block 'key3' generated by the Henon map. This step conceals all the encryption operations carried out on the image.

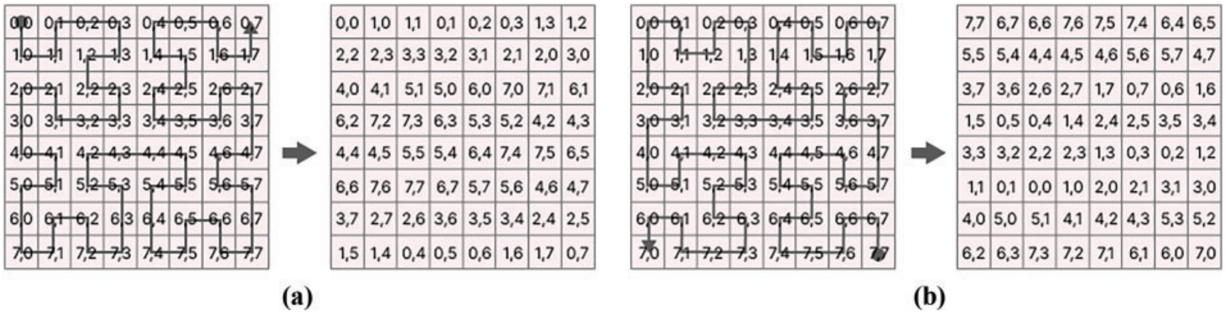


Figure 11: (a) Top-left Hilbert curve process. (b) Bottom-right Hilbert curve process

Table 1: Substitution box

S-Box	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	72	13	148	182	62	64	200	192	241	95	134	26	144	183	70	111
1	117	28	101	42	255	85	212	248	206	130	140	41	6	199	162	171
2	84	90	163	57	204	190	210	165	184	3	82	105	176	33	7	239
3	44	88	164	218	45	102	197	81	225	22	80	153	118	136	170	195
4	29	89	237	65	114	207	228	36	150	121	46	155	17	69	104	172
5	161	138	214	19	198	139	196	14	177	48	97	243	52	94	253	32
6	191	168	25	145	158	233	96	174	152	229	54	221	4	249	201	135
7	151	223	58	116	194	49	7	181	213	224	40	173	20	63	216	217
8	132	71	77	133	131	115	179	193	11	79	235	156	78	93	98	34
9	230	251	76	112	39	27	203	107	236	74	247	127	143	157	47	113
A	83	124	122	129	24	73	38	60	51	23	67	128	61	252	238	187
B	56	137	245	211	125	147	53	175	8	92	0	208	254	242	31	100
C	103	189	5	87	166	149	12	18	106	188	205	154	159	232	99	160
D	202	123	227	86	110	126	108	109	37	180	220	222	215	35	141	1
E	219	240	246	250	119	169	234	226	10	146	178	185	30	43	75	186
F	209	59	55	91	244	167	66	50	21	120	68	231	15	16	142	2

All these operations are applied until passing by all blocks of the plaintext image. Finally, the last step in this encryption phase involves combining all the ciphered blocks to maintain the final cipher image.

4.3 Decryption Process

To decrypt the encrypted image and recover the corresponding plain image, the reverse of the encryption process is followed. Starting from operation 4 and moving backward to operation 1, the steps are reversed using the correct initial conditions. The detailed decryption process is represented in Fig. 12.

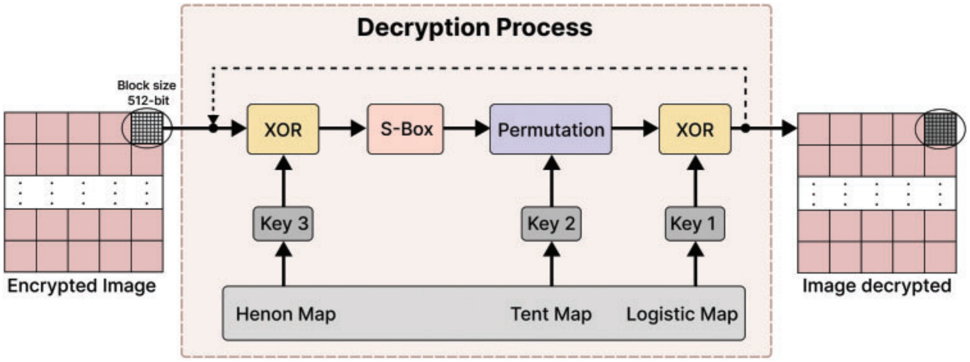


Figure 12: Decryption process

Operation 1 performs a bitwise XOR between the cipher image block and the key block Key3. Operation 2 applies an inverse S-Box substitution to each element of the resulting block from the previous step, enhancing non-linearity. The specific inverse S-Box used is provided in Table 2.

Table 2: Inverse substitution box

S-Box	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	186	223	255	41	108	194	28	46	184	118	232	136	198	1	87	252
1	253	76	199	83	124	248	57	169	164	98	11	149	17	64	236	190
2	95	45	143	221	71	216	166	146	122	27	19	237	48	52	74	158
3	89	117	247	168	92	182	106	242	176	35	114	241	167	172	4	125
4	5	67	246	170	250	77	14	129	0	165	153	238	146	130	140	137
5	58	55	42	160	32	21	211	195	49	65	33	243	185	141	93	9
6	102	90	142	206	191	18	53	192	78	43	200	151	214	215	212	15
7	147	159	68	133	115	16	60	228	249	73	162	209	161	180	213	155
8	171	163	25	132	128	131	10	111	61	177	81	85	26	222	254	156
9	12	99	233	181	2	197	72	112	104	59	203	75	139	157	100	204
A	207	80	30	34	50	39	196	245	97	229	62	31	79	123	103	183
B	44	88	234	134	217	119	3	13	40	235	239	175	201	193	37	96
C	7	135	116	63	86	54	84	29	6	110	208	150	36	202	24	69
D	187	240	38	179	22	120	82	220	126	127	51	224	218	107	219	113
E	121	56	231	210	70	105	144	251	205	101	230	138	152	66	174	47
F	225	8	189	91	244	178	226	154	23	109	227	145	173	94	188	20

Operation 3 reverses the permutation using a Hilbert curve of order 3, and finally, Operation 4 applies another XOR operation with the key block Key 1.

5 Signature Generation

- **The creation of signature:** Once the encryption process is complete, the sender uploads the resulting encrypted data to the cloud and utilizes a hash function to record the hashed value of the image onto the blockchain. That step is essential for ensuring the integrity and authenticity of the cipher image. In the proposed system, we used SHA-256 to produce a hash value, which serves as a signature for the encrypted image. This ensures that attackers can't access the original image because hashing functions are unidirectional. This makes it impossible to reverse back the hashed value to the original image.

- **The verification of signature:** To verify the authenticity of the ciphered image, the data user initiates a signature verification process based on the information stored on the blockchain. This process involves computing the hash value of the received image and comparing it with the original hash value previously recorded on the blockchain by the sender. A successful match confirms the integrity and authenticity of the image, while any discrepancy indicates potential tampering or data corruption. Fig. 13 illustrates the complete signature verification process.

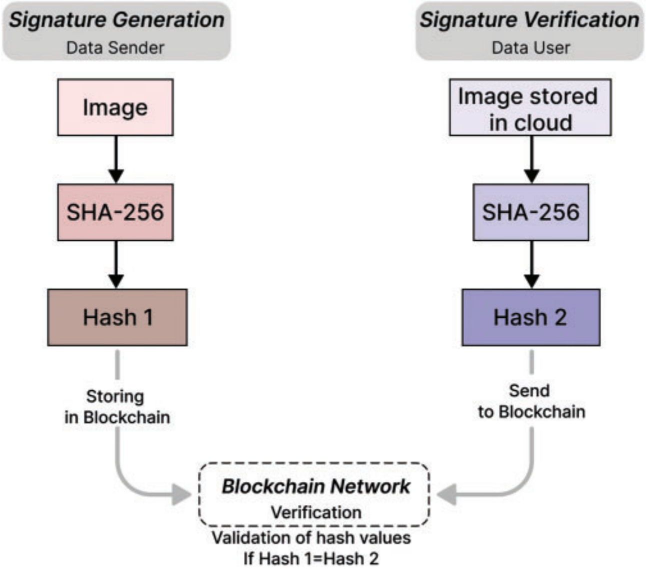


Figure 13: The process of generating and verifying digital signatures

6 Performance and Security Analysis

This section outlines a series of tests suggested to evaluate the security performance of the proposed algorithm. By comparing the encryption results with those of several other researchers using experimental images, which consist of medical images with the same sizes 512 × 512. These images fall into two categories: normal medical images and images depicting diseases. While both types represent the same medical issue, there are slight differences that can only be diagnosed by a specialist (doctor). Despite their close similarity, the encryption results for these images are entirely distinct. The encryption and decryption protocols were tested using multiple gray-scale medical images.

We initialize the parameters as follows: $\mu_l = 4.0$ for the logistic chaotic sequence, $\mu_t = 2.0$ for the tent sequence, and $a = 1.4$ and $b = 0.3$ for the Henon sequences.

6.1 Experimental Evaluation of the Blockchain Environment

To assess the efficiency and responsiveness of the blockchain component within the proposed framework, a series of tests were conducted on a private Ethereum blockchain environment configured using the Geth client and simulated locally via Ganache, details are shown in Table 3.

Table 3: Performance metrics

Metric	Value
Average block time	6.2 s
Transaction throughput	~22 transactions/second
Transaction latency	~6.1 s (end-to-end)
Gas used per hash storage	~22,000 gas
Smart contract cost	<0.001 ETH per transaction (testnet)

The blockchain was tested with the following setup:

- Environment: Ganache CLI (v7.7.5)
- Consensus Mechanism: Proof of Authority (PoA)
- Client: Geth (Go Ethereum)
- Interaction: Python Web3.py library
- System: Intel® Core™i5-1035G1 CPU @ 1.19 GHz, 20 GB memory, and 64-bit Windows 10

The blockchain operated smoothly under private conditions, with reliable performance and low latency. Since PoA does not require extensive mining or complex consensus calculations, the network showed predictable and consistent timing, making it suitable for medical applications where integrity is critical and timeliness is essential.

6.2 Execution Time Analysis

We evaluated the encryption and decryption algorithm's performance on 8 grayscale images, all sized 512 × 512 pixels. Table 4 details these execution times in seconds, showing an average encryption time of 0.70932525 s.

Table 4: Execution time measurements for the encryption and decryption processes

Image	Brain_ normal	Brain_ tumor	Chest_ normal	Chest_ pneumonia	Kidney_ normal	Kidney_ stone	Lung_ normal	Lung_ cancer
Encryption time (s)	0.629918	0.772861	0.707593	0.708836	0.601376	0.844424	0.725164	0.684430
Decryption time (s)	0.687428	0.809152	0.897831	0.980619	0.560338	0.721823	0.651668	0.624451

6.3 Analysis of Key Space

An ideal image encryption scheme should possess a sufficiently large key space and exhibit high sensitivity to its key. The key space size represents the number of possible keys in the cryptographic system. Consequently, the key space must exceed 2^{100} to ensure that the algorithm is capable of resisting brute force attacks [41]. In the proposed cryptosystem, initial conditions are: $x_{0\log istic}$, x_{0tent}, x_{0henon}, and y_{0henon} and the parameters are: r, μ, a, and b. The $x_{\log istic}$, x_{tent}, x_{henon} and y_{henon} are the key parameters with 10^{-10} of precision. Thus, the total key space for our proposed algorithm is as follows: $10^{8\times 10} = 10^{80} \simeq 2^{266} > 2^{100}$. That equation meets the security requirements outlined in the standard. Consequently, the encryption algorithm possesses a sufficiently large key space to withstand various brute-force attacks.

6.4 National Institute of Standards and Technology (NIST) Analysis

The NIST test, developed as an effective estimation measure for randomness in encrypted images. It is referred to as the NIST SP 800 analysis.

The NIST test has been utilized for the assessment of the overall quality of the dynamic offset. The random behavior of selected chaotic maps utilized in the suggested system has been confirmed through the National Institute of Standards and Technology. The test comprises 15 statistical tests, each of which yields a p-value (randomness probability). Accordingly, it has been employed to assess the randomness of the chaotic sequences generated by the three utilized maps, as illustrated in Fig. 14. All fifteen tests were successfully completed, as evidenced by the figure. Consequently, it has been demonstrated that the generated sequences by the Logistic map, Tent map, and Henon map achieve a great level of randomness.

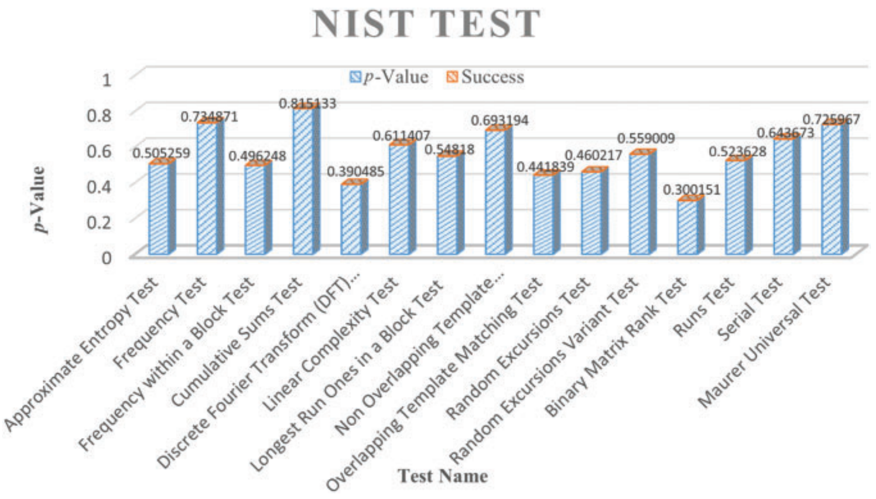


Figure 14: Nist test analysis

6.5 Differential Attack Analysis

The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are essential metrics for assessing an encryption algorithm's resistance to differential attacks. NPCR reflects the percentage of changed pixels in the cipher image when a single pixel in the plaintext is modified, while UACI measures the average intensity difference. High NPCR and UACI values indicate strong sensitivity to input changes, demonstrating robust security. These metrics are computed using the following equations:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100\%,\ UACI = \frac{1}{m \times n} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \tag{11}$$

$$D(i,j) = \begin{cases} 1, C_1(i,j) \neq C_2(i,j) \\ 0, C_1(i,j) = C_2(i,j) \end{cases} \tag{12}$$

where m and n represent the dimensions of the image while C_1 and C_2 are two encrypted images generated from original images that differ by only one pixel in gray value.

In this paper, an experiment was executed for each test image. To calculate those values, we randomly selected from the original image a pixel value and changed it. The results illustrated in Table 5 indicate that most NPCR values are greater than 99%, and the UACI values are above 33%. This outcome indicates that the algorithm possesses high sensitivity to plaintext variations and demonstrates strong resilience against differential attacks.

Table 5: NPCR and UACI analysis

Image	Brain_ normal	Brain_ tumor	Chest_ normal	Chest_ pneumonia	Kidney_ normal	Kidney_ stone	Lung_ normal	Lung_ cancer
NPCR (%)	99.6105	99.6295	99.6128	99.5967	99.6204	99.6192	99.6177	99.6204
UACI (%)	33.4444	33.4277	33.4818	33.4455	33.5286	33.4814	33.5081	33.4254

6.6 Structural Similarity Index Measure (SSIM)

SSIM Index is a test utilized to measure the degree of resemblance between two images. It is based on the fact that pixels have strong interdependencies, specifically when they are located close together. These dependencies convey vital information about how the visual scene gets structured. The resulting SSIM index ranges from −1 to 1, where 1 is achievable only if the two sets of data are identical. Eq. (13) is utilized to determine the SSIM value for images.

$$SSIM\left(x,y\right)=\left[l\left(x,y\right)^{a}\times c\left(x,y\right)^{b}\times s\left(x,y\right)^{c}\right] \tag{13}$$

This formula is based on three measurements of comparison between samples of x and y: (l) is the luminance (l), (c) is the contrast, and (s) is the structure as shown in Eqs. (14)–(16):

$$l\left(x,y\right)=\frac{2\mu_x\mu_y+c_1}{\mu_x^2\mu_y^2+c_1} \tag{14}$$

$$c\left(x,y\right)=\frac{2\sigma_x\sigma_y+c_2}{\sigma_x^2\sigma_y^2+c_2} \tag{15}$$

$$s\left(x,y\right)=\frac{\sigma_{xy}+c_3}{\sigma_x\sigma_y+c_3} \tag{16}$$

Table 6 shows that the results obtained from the SSIM analysis are very close to zero. These results demonstrate that the original and cipher images are not similar. Consequently, no pertinent data can be extracted from the encrypted image to reconstruct the original image.

Table 6: SSIM analysis

Image	Brain_ normal	Brain_ tumor	Chest_ normal	Chest_ pneumonia	Kidney_ normal	Kidney_ stone	Lung_ normal	Lung_ cancer
SSIM	0.0049	0.0055	0.0097	0.0072	0.0036	0.0020	0.0078	0.0069

6.7 Mean Squared Error (MSE) & Peak Signal to Noise Ratio (PSNR)

The quality of the proposed encryption system can be quantitatively evaluated by comparing the original and encrypted images. The Peak Signal-to-Noise Ratio (PSNR) is employed to measure the perceptual difference in quality between the plain and encrypted images, whereas the Mean Squared Error (MSE) quantifies the pixel-level variance between them. Table 7 presents the computed PSNR and MSE values. The formulas for calculating PSNR and MSE are defined as follows:

$$PSNR = 20\log\left(\frac{255}{\sqrt{MSE}}\right)(dB) \tag{17}$$

$$MSE = \frac{1}{M \times N}\sum_{y=1}^{M}\sum_{x=1}^{N}\left[P(x,y) - C(x,y)\right]^2 \tag{18}$$

where *P(x, y)* is the plain image, *C(x, y)* is the cipher image and (*M*, *N*) are the dimensions of the images. A lower MSE indicates less error, and due to the inverse relationship between MSE and PSNR, this results in a higher PSNR value. A higher value of PSNR indicates a better quality of the signal relative to the noise.

Table 7: PSNR and MSE results

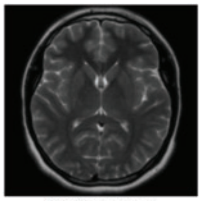
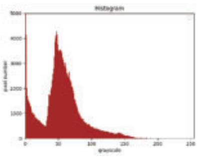
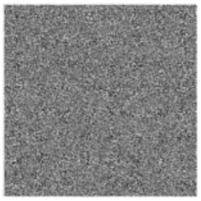
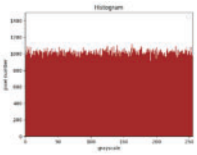
Image	Brain_ normal	Brain_ tumor	Chest_ normal	Chest_ pneumonia	Kidney_ normal	Kidney_ stone	Lung_ normal	Lung_ cancer
PSNR	36.0982	36.0693	36.0798	36.1351	36.0276	36.1050	36.0851	36.1244
MSE	15.9680	16.0747	16.0359	15.8331	16.2299	15.9432	16.0163	15.8721

The greater the PSNR value is, the better the image separation result. In this context, the signal refers to the plain image, while the noise represents the error in reconstruction.

6.8 Histogram Analysis

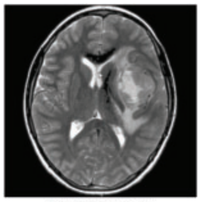
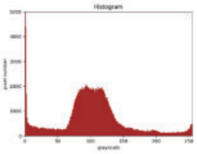
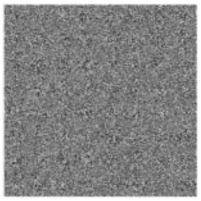
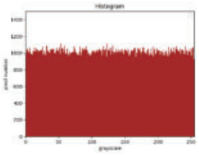
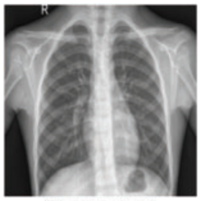
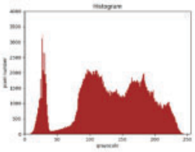
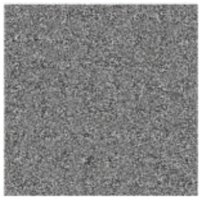
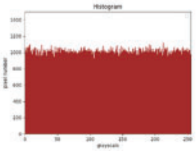
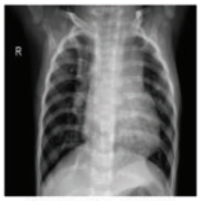
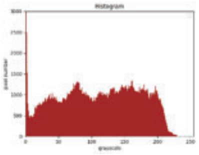
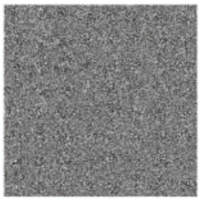
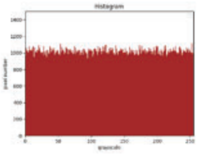
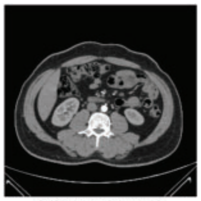
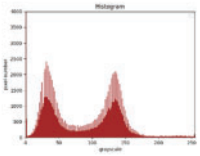
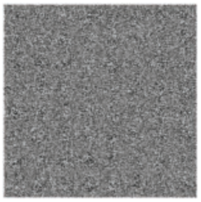
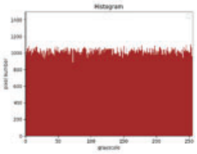
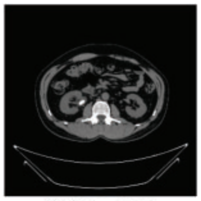
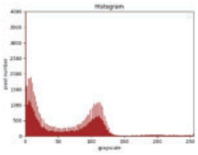
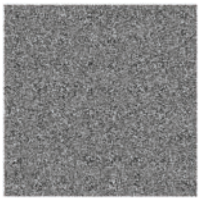
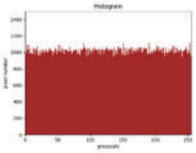
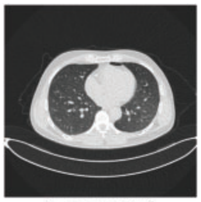
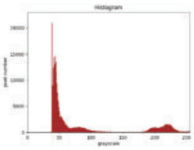
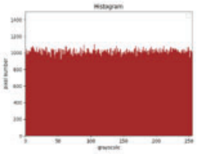
An image histogram represents the distribution of pixel intensities across gray levels and provides valuable statistical insight. For encrypted images, a uniform histogram is essential as it obscures patterns and prevents information leakage. In this study, eight images of identical dimensions were used. As shown in Table 8, plaintext image histograms exhibit distinct peaks and valleys, whereas the histograms of the corresponding ciphered images are uniformly distributed. This uniformity confirms the absence of statistical correlation between plaintext and ciphered images, highlighting the algorithm's effectiveness in resisting statistical attacks.

Table 8: Histogram results of grayscale medical images; plain images; and encrypted images

Original image	Histogram	Encrypted image	Histogram
 Brain-normal			

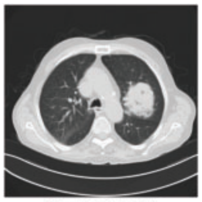
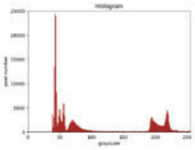
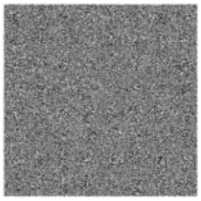
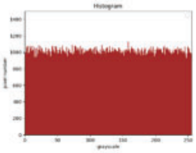
(Continued)

Table 8 (continued)

Original image	Histogram	Encrypted image	Histogram
 Brain-tumor			
 Chest-normal			
 Chest-pneumonia			
 Kidney-normal			
 Kidney-stone			
 Lung-normal			

(Continued)

Table 8 (continued)

Original image	Histogram	Encrypted image	Histogram
 Lung-cancer			

For quantitative analysis of the performance of pixel value distribution, we present histogram variances as a measure to assess the uniformity of encrypted images. The histogram variance is calculated in the Eq. (19):

$$\operatorname{var}(Z) = \frac{1}{p^2} \sum_{i=1}^{p} \sum_{j=1}^{p} \frac{1}{2} \left(z_i - z_j\right)^2 \tag{19}$$

The greater the uniformity of encrypted images, the lower the variance values. Here, Z represents the vector of histogram values $Z = \{z_1, z_2, \ldots, z_{256}\}$, while $z_i$and z_j denote the counts of pixels with gray values equal to i and j, respectively.

Table 9 presents the histogram variance values for both the original images and their corresponding encrypted images, generated using the proposed algorithm.

Table 9: Variance of the histogram of different images

Image	Variance							
	Brain_ normal	Brain_ tumor	Chest_ normal	Chest_ pneumonia	Kidney_ normal	Kidney_ stone	Lung_ normal	Lung_ cancer
Plain-image	24,457,920.0	33,646,376.0	530,110.25	9,754,035.0	75,128,270.0	140,831,650.0	6,588,584.0	6,287,471.0
Encrypted image	921.8672	960.6875	970.41406	1027.7734	855.64844	1072.7344	1038.5156	1158.6172

6.9 *Information Entropy*

Entropy is a thermodynamic physical quantity that describes the degree of disorder in a physical system. In the context of digital images, information entropy represents the distribution of each grey level. The Eq. (20) is used to calculate information entropy:

$$E(m) = -\sum_{i=1}^{M} p(m_i) \,.\, \log_2 p(m_i) \tag{20}$$

With m is the information entropy of the gray image, M is the total number of symbols and $p(m_i)$ is the probability that the image pixel value appears. For an ideal algorithm, the ciphertext image should appear completely random, with an information entropy value approaching the theoretical maximum of 8. Table 10 presents the entropy values computed for the cipher-images corresponding to the test plaintext images. As shown, the entropy results are consistently close to 8, indicating a high level of randomness in the encrypted images. This suggests that the proposed algorithm effectively minimizes the risk of information leakage through statistical analysis.

Table 10: Information entropy of original and encrypted images

	Entropy							
Image	**Brain_ normal**	**Brain_ tumor**	**Chest_ normal**	**Chest_ pneumonia**	**Kidney_ normal**	**Kidney_ stone**	**Lung_ normal**	**Lung_ cancer**
Plain-image	5.5958	5.6891	7.5463	6.9477	4.3543	2.7459	6.1358	6.3323
Cipher-image	7.9993	7.9993	7.9993	7.9993	7.9994	7.9992	7.9993	7.9992

6.10 Correlation Analysis

The pixel correlation test is a widely used technique for evaluating the effectiveness of image encryption algorithms. It assesses the degree of correlation between adjacent pixels in an image, where an ideal encryption scheme should significantly reduce this correlation. To perform this analysis, 2000 pairs of adjacent pixels are randomly selected from the horizontal, vertical, and diagonal directions of both the original and encrypted images. The correlation coefficients are then computed to quantify the decorrelation achieved by the encryption process. This test is performed as follows:

$$C_{x,y} = \frac{Cov\left(x,y\right)}{\sqrt{D\left(x\right)}.\sqrt{D\left(y\right)}} \tag{21}$$

With:

$$Cov\left(x,y\right) = \frac{1}{K}\sum_{i=1}^{K}\left(x_i - E\left(x\right)\right)\left(y_i - E\left(y\right)\right) \tag{22}$$

$$E\left(x\right) = \frac{1}{K}\sum_{i=1}^{K}x_i \tag{23}$$

$$D\left(x\right) = \frac{1}{K}\sum_{i=1}^{K}\left(x_i - E\left(x\right)\right)^2 \tag{24}$$

Here, x and y are presented as two adjacent pixels, and N as the sample counts. $E(x)$ donates the mathematical expectation of x, and $D(x)$ denotes the standard deviation.

Fig. 15 represents the distribution of 2000 pixel pairs in different directions for original and encrypted images of the two Brain example. In the original images and in vertical direction, the majority of points cluster near the diagonal line, indicating that vertically adjacent pixels have similar values. Similar distributions are observed for horizontal and diagonal directions. In every direction in the encrypted images, the dots are randomly dispersed throughout the space. This indicates that no relationship exists among the adjacent pixels of the cipher image.

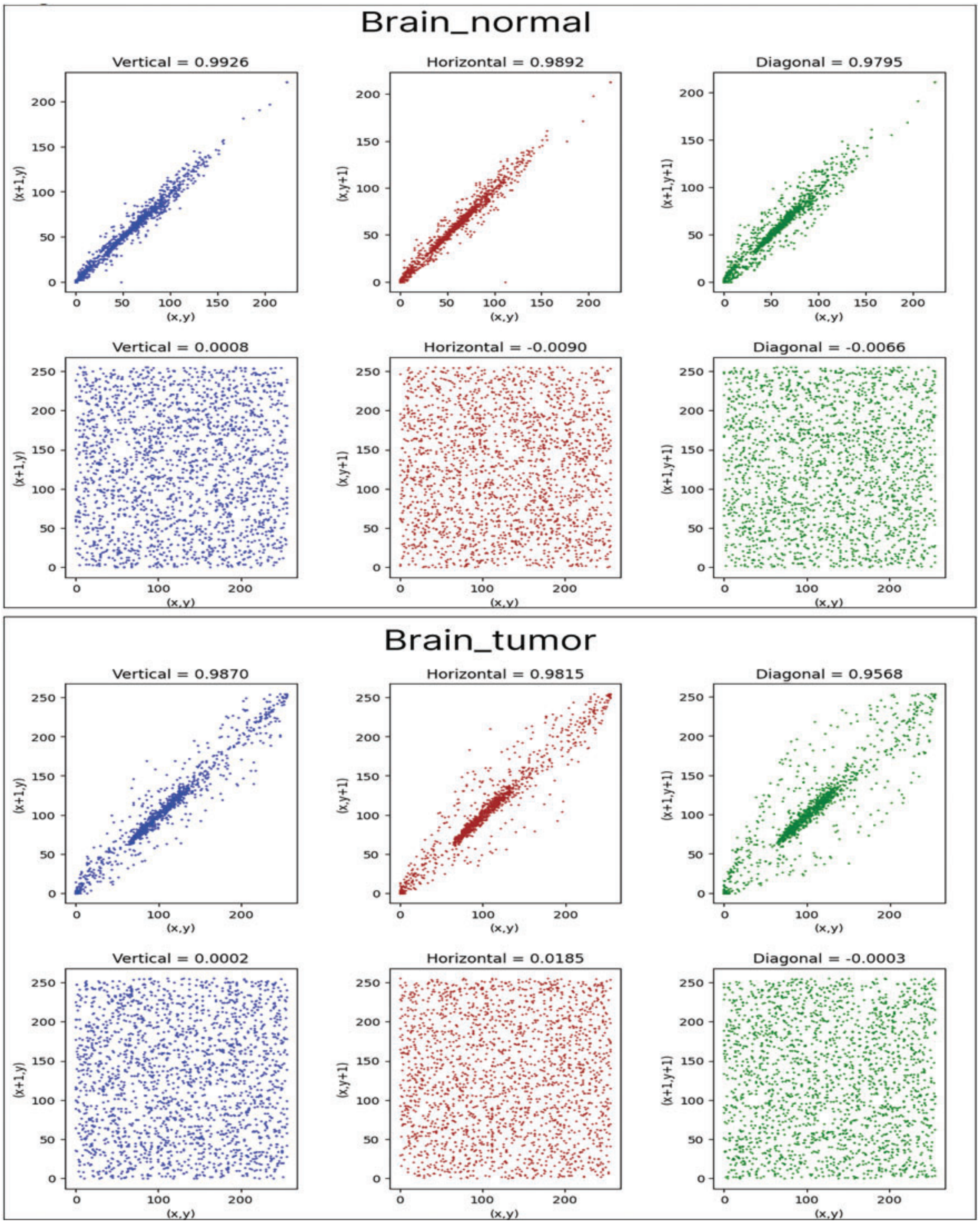


Figure 15: Distribution of 2000 pairs of adjacent pixels randomly selected from the original images in the vertical, horizontal, and diagonal directions

It is shown in Fig. 15 that the correlation coefficients of the plain images are all above 0.5, with the pixel distribution concentrated near the diagonal. This indicates a strong correlation between adjacent pixels in the original image.

However, this strong correlation is disrupted after encryption, and the correlation coefficient approaches 0, indicating that the encrypted image pixels are uncorrelated. Table 11 illustrates the correlation values between neighboring pixels in the horizontal, vertical, and diagonal directions for both the original and encrypted images.

Table 11: Correlation coefficient of the plaintext image and the corresponding ciphered image in the horizontal (H), vertical (V) and diagonal (D) directions

Image		**Original image**	**Encrypted image**
Brain_normal	**V**	0.9926	0.0008
	H	0.9892	−0.0090
	D	0.9795	−0.0066
Brain_tumor	**V**	0.9870	0.0002
	H	0.9815	0.0185
	D	0.9568	−0.0003
Chest_normal	**V**	0.9972	−0.0114
	H	0.9931	−0.0600
	D	0.9906	0.0030
Chest_pneumonia	**V**	0.9966	0.0066
	H	0.9965	−0.0289
	D	0.9935	0.0069
Kidney_normal	**V**	0.9772	0.0444
	H	0.9789	0.0045
	D	0.9514	0.0049
Kidney_stone	**V**	0.9595	0.0043
	H	0.9624	0.0027
	D	0.9219	0.0179
Lung_normal	**V**	0.9884	0.0014
	H	0.9908	0.0139
	D	0.9765	0.0061
Lung_cancer	**V**	0.9956	0.0190
	H	0.9964	0.0007
	D	0.9905	−0.0092

7 Comparative Study

Numerous image encryption techniques have been developed and are used as benchmarks for evaluating the performance of the proposed method. Table 12 presents a comparative analysis of existing encryption schemes. Based on this comparison, a blockchain-based image encryption method tailored for medical images is suggested. The proposed algorithm is evaluated using a dataset of eight medical images, and its average performance is assessed through key metrics including key space, MSE, PSNR, NPCR, UACI, SSIM, and global entropy. The results are summarized in Tables 13 and 14.

Table 12: Comparison of current encryption solutions

Paper	Year	Encryption quality	Technique	Decentralized
El-Shafai et al. [21]	2021	Normal	DNA rules and chaotic maps	No
El-Shafai et al. [22]	2022	Normal	Neural Stacked Auto-Encoder (SAE) framework	No
Neela et al. [29]	2023	Normal	Chaotic Deep GAN Encryption and Blockchain	Yes
Inam et al. [30]	2024	Good	Arnold's cat map encryption and Blockcain	Yes
Kumari T et al. [31]	2024	Good	Multi-chaotic maps and Blockchain	Yes
Proposed	2025	Good	Block-cipher based chaotic maps and Blockchain	Yes

Table 13: Comparison of average entropy and key space with other schemes

Scheme	El-Shafai et al. [21]	El-Shafai et al. [22]	Neela et al. [29]	Inam et al. [30]	Kumari T et al. [31]	Proposed
Global Entropy	7.9974	7.92	7.98	7.9992	7.9995	**7.9993**
Key Space	2^{263}	10^{21}	–	2^{240}	2^{469}	2^{266}

Table 14: The comparison of average MSE, PSNR, NPCR, UACI and SSIM with other schemes

Scheme	MSE	PSNR(dB)	NPCR (%)	UACI (%)	SSIM
El-Shafai et al. [21]	–	52.73	99.69	32.24	0.0039
El-Shafai et al. [22]	–	7.98	99.62	33.31	0.0046
Neela et al. [29]	124.60	–	99.60	33.86	0.018
Inam et al. [30]	14,051.56	6.65	99.63	33.21	0.0039
Kumari T et al. [31]	–	7.3682	99.60	33.48	0.0064
Proposed	15.9966	36.0905	99.6159	33.4678	0.0059

As shown in Table 13, the information entropy values of the encrypted images generated by the proposed cryptosystem are consistently close to 8, indicating a high level of randomness. These values surpass those reported in Refs. [21,22,29,30] and are comparable to those in Ref. [31], suggesting strong resistance to entropy-based attacks. Furthermore, the proposed method demonstrates a larger key space than those in Refs. [21,22,30], though slightly smaller than Ref. [31]; nonetheless, it remains sufficiently large to resist brute-force attacks.

Table 14 highlights the proposed scheme's efficiency, showing superior PSNR values compared to most existing methods, indicating better image quality retention. Moreover, the NPCR and UACI values confirm the robustness of the proposed algorithm against differential attacks, outperforming several compared schemes, though not all.

The results above demonstrate that the proposed encryption scheme performs as well as or better than other standard schemes. Additionally, it meets the current demands, establishing its high acceptability.

8 Conclusion

This paper presents a Blockchain-based image encryption algorithm utilizing chaos theory to enhance data security, privacy, and authenticity. The sender encrypts the medical image, generates a SHA-256 digital signature, stores the ciphered image in the cloud, and records the signature on the blockchain. Upon request, the user retrieves the encrypted image from the cloud and verifies its authenticity via the blockchain before decryption. Comprehensive security evaluations; including histogram analysis, key space testing, correlation coefficient analysis, entropy measurement, and differential attack resistance demonstrate that the proposed scheme offers robust protection against various cryptographic threats.

Future work will focus on extending this encryption framework to real-time telemedicine applications, enabling secure and efficient transmission of medical images in dynamic healthcare environments.

Acknowledgement: The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Group Project under grant number (RGP2/473/46).

Funding Statement: This work was supported by the Large Group Project under grant number (RGP2/473/46).

Author Contributions: Rim Amdouni designed the algorithm and software implementation. Mahdi Madani analyzed and validated the algorithm. Mohamed Ali Hajjaji and El Bay Bourennane analyzed and validated the results. Mohamed Atri read and evaluated the final manuscript. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Material: This study does not include any datasets. No new data were generated or analyzed during this study.

Ethics Approval: This study does not involve human participants or animals; therefore, ethical approval is not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Manju Bala P, Rajmohan R, Ananth Kumar T, Ajagbe SA, Adigun MO. Quantum blockchain-oriented data integrity scheme for validating clinical datasets. In: Exploring intelligent healthcare with quantum computing. Stevenage, UK: IET; 2024. p. 259–78 doi:10.1049/pbhe060e_ch13.
2. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling blockchain: a data processing view of blockchain systems. IEEE Trans Knowl Data Eng. 2018;30(7):1366–85. doi:10.1109/tkde.2017.2781227.
3. Khan PW, Byun Y. A blockchain-based secure image encryption scheme for the industrial Internet of Things. Entropy. 2020;22(2):175. doi:10.3390/e22020175.
4. Chen M, Malook T, Rehman AU, Muhammad Y, Alshehri MD, Akbar A, et al. Blockchain-Enabled healthcare system for detection of diabetes. J Inf Secur Appl. 2021;58:102771. doi:10.1016/j.jisa.2021.102771.
5. Ajagbe SA, Florez H, Awotunde JB. AESRSA: a new cryptography key for electronic health record security. In: Applied informatics. Cham, Switzerland: Springer International Publishing; 2022. p. 237–51. doi:10.1007/978-3-031-19647-8_17.
6. Aggarwal S, Chaudhary R, Aujla GS, Kumar N, Choo KR, Zomaya AY. Blockchain for smart communities: applications, challenges and opportunities. J Netw Comput Appl. 2019;144:13–48. doi:10.1016/j.jnca.2019.06.018.

7. Bhardwaj A, Chaudhary R, Aslam AM, Budhiraja I. Blockchain-based robust SDN framework for digital twin-enabled IoT networks. In: IEEE 98th Vehicular Technology Conference (VTC2023-Fall); 2023 Oct 10–13; Hong Kong, China. p. 1–6. doi:10.1109/VTC2023-Fall60731.2023.10333591.
8. Rai HM, Shukla KK, Tightiz L, Padmanaban S. Enhancing data security and privacy in energy applications: integrating IoT and blockchain technologies. Heliyon. 2024;10(19):e38917. doi:10.1016/j.heliyon.2024.e38917.
9. Hosseinzadeh M, Malik MH, Safkhani M, Bagheri N, Le QH, Tightiz L, et al. Toward designing a secure authentication protocol for IoT environments. Sustainability. 2023;15(7):5934. doi:10.3390/su15075934.
10. Liu J, Yang D, Zhou H, Chen S. A digital image encryption algorithm based on bit-planes and an improved logistic map. Multimed Tools Appl. 2018;77(8):10217–33. doi:10.1007/s11042-017-5406-2.
11. Sneha PS, Sankar S, Kumar AS. A chaotic colour image encryption scheme combining Walsh-Hadamard transform and Arnold-Tent maps. J Ambient Intell Humaniz Comput. 2020;11(3):1289–308. doi:10.1007/s12652-019-01385-0.
12. Rathee G, Sharma A, Saini H, Kumar R, Iqbal R. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimed Tools Appl. 2020;79(15–16):9711–33. doi:10.1007/s11042-019-07835-3.
13. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Pers Ubiquitous Comput. 2024;28(1):59–72. doi:10.1007/s00779-021-01583-8.
14. Azbeg K, Ouchetto O, Jai Andaloussi S. BlockMedCare: a healthcare system based on IoT, Blockchain and IPFS for data management security. Egypt Inform J. 2022;23(2):329–43. doi:10.1016/j.eij.2022.02.004.
15. Naskar PK, Bhattacharyya S, Nandy D, Chaudhuri A. A robust image encryption scheme using chaotic tent map and cellular automata. Nonlinear Dyn. 2020;100(3):2877–98. doi:10.1007/s11071-020-05625-3.
16. Masood F, Boulila W, Alsaeedi A, Khan JS, Ahmad J, Khan MA, et al. A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and Logistic Gaussian map. Multimed Tools Appl. 2022;81(21):30931–59. doi:10.1007/s11042-022-12844-w.
17. Ibrahim S, Alharbi A. Efficient image encryption scheme using henon map, dynamic S-boxes and elliptic curve cryptography. IEEE Access. 2020;8:194289–302. doi:10.1109/access.2020.3032403.
18. Alexan W, Elkandoz M, Mashaly M, Azab E, Aboshousha A. Color image encryption through chaos and KAA map. IEEE Access. 2023;11:11541–54. doi:10.1109/access.2023.3242311.
19. Singh KN, Singh OP, Singh AK, Agrawal AK. EiMOL: a secure medical image encryption algorithm based on optimization and the Lorenz system. ACM Trans Multimed Comput Commun Appl. 2023;19(2s):1–19. doi:10.1145/3561513.
20. Anand A, Singh AK. An improved DWT-SVD domain watermarking for medical information security. Comput Commun. 2020;152(3):72–80. doi:10.1016/j.comcom.2020.01.038.
21. El-Shafai W, Khallaf F, El-Rabaie EM, El-Samie FEA. Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. J Ambient Intell Humaniz Comput. 2021;12(10):9007–35. doi:10.1007/s12652-020-02597-5.
22. El-Shafai W, Khallaf F, El-Rabaie EM, Abd El-Samie FE. Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. Neural Comput Appl. 2022;34(13):10629–53. doi:10.1007/s00521-022-06994-z.
23. Yepdia LMH, Tiedeu A. Secure transmission of medical image for telemedicine. Sens Imag. 2021;22(1):17. doi:10.1007/s11220-021-00340-8.
24. Malika A, Sharma RS. A novel image encryption based on feedback carry shift register and blockchain for secure communication. Int J Appl Eng Res. 2021;16(6):466–77.
25. Brabin D, Ananth C, Bojjagani S. Blockchain based security framework for sharing digital images using reversible data hiding and encryption. Multimed Tools Appl. 2022;81(17):24721–38. doi:10.1007/s11042-022-12617-5.
26. Ravi RV, Goyal SB, Verma C, Raboaca MS, Enescu FM, Mihaltan TC. Image encryption using block chain and chaos for secure communication. In: 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI); 2022 Jun 30–July 1; Ploiesti, Romania. p. 1–6. doi:10.1109/ECAI54874.2022.9847446.

27. Abrar A, Abdul W, Ghouzali S. Secure image authentication using watermarking and blockchain. Intell Autom Soft Comput. 2021;28(2):577–91. doi:10.32604/iasc.2021.016382.
28. Doreen Hephzibah Miriam D, Dahiya D, Nitin, Rene Robin CR. Secured cyber security algorithm for healthcare system using blockchain technology. Intell Autom Soft Comput. 2023;35(2):1889–906. doi:10.32604/iasc.2023.028850.
29. Neela KL, Kavitha V. Blockchain based Chaotic Deep GAN Encryption scheme for securing medical images in a cloud environment. Appl Intell. 2023;53(4):4733–47. doi:10.1007/s10489-022-03730-x.
30. Inam S, Kanwal S, Firdous R, Hajjej F. Blockchain based medical image encryption using Arnold's cat map in a cloud environment. Sci Rep. 2024;14(1):5678. doi:10.1038/s41598-024-56364-z.
31. Kumari T, Singh D, Singh B. Multi-chaotic maps and blockchain based image encryption. Concurr Comput. 2024;36(14):e8092. doi:10.1002/cpe.8092.
32. Arif J, Khan MA, Ghaleb B, Ahmad J, Munir A, Rashid U, et al. A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution. IEEE Access. 2022;10(2):12966–82. doi:10.1109/access.2022.3146792.
33. Phatak SC, Rao SS. Logistic map: a possible random-number generator. Phys Rev E. 1995;51(4):3670–8. doi:10.1103/physreve.51.3670.
34. Kiran Parameshachari BD, Panduranga HT. Medical image encryption using SCAN technique and chaotic tent map system. In: Recent advances in artificial intelligence and data engineering. Singapore: Springer; 2021. p. 181–93. doi:10.1007/978-981-16-3342-3_15.
35. Hénon M. A two-dimensional mapping with a strange attractor. In: The theory of chaotic attractors. New York, NY, USA: Springer New York; 1976. p. 94–102. doi:10.1007/978-0-387-21830-4_8.
36. Jawad LM. A new scan pattern method for color image encryption based on 3D-Lorenzo chaotic map method. Multimed Tools Appl. 2021;80(24):33297–312. doi:10.1007/s11042-021-11295-z.
37. Shahna KU, Mohamed A. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. Appl Soft Comput. 2020;90(4):106162. doi:10.1016/j.asoc.2020.106162.
38. Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. J Inf Secur Appl. 2020;50(10):102407. doi:10.1016/j.jisa.2019.102407.
39. Tariq N, Qamar A, Asim M, Khan FA. Blockchain and smart healthcare security: a survey. Procedia Comput Sci. 2020;175(9):615–20. doi:10.1016/j.procs.2020.07.089.
40. Zhai S, Yang Y, Li J, Qiu C, Zhao J. Research on the application of cryptography on the blockchain. J Phys Conf Ser. 2019;1168:032077. doi:10.1088/1742-6596/1168/3/032077.
41. Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcation Chaos. 2006;16(8):2129–51. doi:10.1142/s0218127406015970.