



OPEN

Blockchain based medical image encryption using Arnold's cat map in a cloud environment

Saba Inam^{1✉}, Shamsa Kanwal¹, Rabia Firdous¹ & Fahima Hajjej²

Improved software for processing medical images has inspired tremendous interest in modern medicine in recent years. Modern healthcare equipment generates huge amounts of data, such as scanned medical images and computerized patient information, which must be secured for future use. Diversity in the healthcare industry, namely in the form of medical data, is one of the largest challenges for researchers. Cloud environment and the Block chain technology have both demonstrated their own use. The purpose of this study is to combine both technologies for safe and secure transaction. Storing or sending medical data through public clouds exposes information into potential eavesdropping, data breaches and unauthorized access. Encrypting data before transmission is crucial to mitigate these security risks. As a result, a Blockchain based Chaotic Arnold's cat map Encryption Scheme (BCAES) is proposed in this paper. The BCAES first encrypts the image using Arnold's cat map encryption scheme and then sends the encrypted image into Cloud Server and stores the signed document of plain image into blockchain. As blockchain is often considered more secure due to its distributed nature and consensus mechanism, data receiver will ensure data integrity and authenticity of image after decryption using signed document stored into the blockchain. Various analysis techniques have been used to examine the proposed scheme. The results of analysis like key sensitivity analysis, key space analysis, Information Entropy, histogram correlation of adjacent pixels, Number of Pixel Change Rate, Peak Signal Noise Ratio, Unified Average Changing Intensity, and similarity analysis like Mean Square Error, and Structural Similarity Index Measure illustrated that our proposed scheme is an efficient encryption scheme as compared to some recent literature. Our current achievements surpass all previous endeavors, setting a new standard of excellence.

Keywords Blockchain, Cloud computing, Arnold's cat map, Orthogonal matrix, Structural similarity index measure (SSIM)

The Internet has benefited humanity in numerous ways, the most notable of which is by providing a platform for virtual environments. Today, every industry is aggressively attempting to virtualize its operations using web applications. While the Internet and web apps have a positive reputation, they also have a negative reputation for being a growing hive for criminal activities such as online identity theft and fraudulent transactions. As a result, researchers have taken a keen interest in making the Internet and online applications more secure and trustworthy¹. For this, a new technology known as "cloud computing" has been introduced.

The concept of network-based computing dates to the early 1960s, although many believe the term "cloud computing" was first employed in its contemporary meaning on August 9, 2006, when Google CEO Eric Schmidt introduced it at an industry conference^{2,3}. Cloud computing has grown significantly in industrial technology such as Amazon, IBM, HP, Apple, and Oracle⁴⁻⁶. It is widely used in the telemedicine industry as well. Telemedicine is a fast-growing field in which medical care is provided to patients who aren't physically available at the same place as the physician⁷.

Furthermore, safe internet exchanges of patient medical information, including medical scans, are becoming more widespread. Because medicinal data is usually available in a visual manner, it must be strictly protected. Therefore, a complicated medical system requires expertise capable of accumulating medical documents in a format that allows authorized users to access them from any location^{8,9}. As we all know, medical data is growing by the day, and we need to preserve it for future use. To properly handle such a complex and vast amount of data significantly, specific technologies such as a distributed data network, scalable storage, parallel processing,

¹Department of Mathematical Sciences, Fatima Jinnah Women University, The Mall, Rawalpindi, Pakistan. ²Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, 11671 Riyadh, Saudi Arabia. ✉email: saba.inam@fjwu.edu.pk

frameworks, infrastructures, and so on are necessary. Because cloud computing is based on service-oriented architecture, it can handle these complex problems in a virtualized environment at a minimal cost^{10,11}.

Furthermore, cloud computing security issues arise because of individuality and risk management, integrity control, public services, and data access management. Individual e-mails and contact numbers can be protected from being accessed by attackers who want to get information by validating the sender's identity¹². Several solutions have been used to overcome the cloud communication problem in terms of privacy and security, but there are some restrictions. Keeping sensitive data on cloud computing is a major concern that necessitates including the defense problem that occurs on cloud computing. At this time, conventional system has been enormously enhanced to offer safety measures in the health care industry, but they include elevated prices and greater usage of computation resources in the meantime¹³.

As a result, preserving the medical images whilst retaining its reliability is critical. Data integrity refers to the assurance that the medical images doesn't change by not permitted parties. An illicit operator has the capacity to change medical images. As an outcome of the data modification or erosion in the picture, disease diagnosis will be incorrect. As a result, a strong and dependable technique for safely sending delicate health care over public channels is required¹⁴.

For this, before sending data to a cloud server, we must first encrypt it so that no one, not even the cloud server, can read it. Traditional cryptosystems, like AES¹⁵ and DES¹⁶, are unsuitable for quick image encryption because they need a large amount of computational power and a long time to complete. Many encryption algorithms have been developed to meet the criteria of security, privacy, and efficient calculation. Chaotic theory-based encryption approaches are ideal for image encryption because they provide high-level of security, greater speed, processing capacity, and process complexity. Non-periodicity, sensitivity to beginning circumstances, and unpredictability are all characteristics of chaotic maps. These are employed in picture encryption for data confusion and dispersion. The privacy and security of information are enhanced by chaotic maps. That's why we use two different chaotic maps in our proposed scheme i.e., Henon map and Arnold's cat map (ACM) for making the encryption scheme key sensitive orthogonal matrix generated from an equation of plane along with hill cipher is used.

Sending encrypted data using chaotic mappings over public channels is secure but we need more security as well as data authentication and data integrity so that the receiver at the other end will get assured that decrypted image and the original image is same. To address these concerns, the use of blockchain is proposed in this model. Blockchain technology has captured the attention of many stakeholders, including healthcare, finance, real estate, infrastructure, and governmental organizations^{17,18}.

Using blockchain to store and manage electronic health records will be efficient and safe. The combination of blockchain and cloud storage to process healthcare data will deliver high-quality services at a reasonable cost¹⁰. For its services, the blockchain network does not rely on a centralized, trustworthy third party. It is a decentralized network in which there is no single point of failure. If one or more nodes fail, there is enough redundancy to keep the rest of the network operational¹⁹.

Contribution

The previous frameworks include image encryption in cloud environment or transaction of data through blockchain. This study merges both concepts as we want a scheme where we can share sensitive data like medical images all over the world along with the confidentiality of the data. For this purpose, our proposed scheme contributes in the following ways:

- We adopt the same model as given in ref²⁰. To enhance security, this model is modified by our new proposed encryption scheme. This new proposed encryption scheme exhibits better results and performance. Different results and analysis are shown in Table 6a.
- The chaotic based Arnold's cat map with orthogonal key matrix encryption scheme uses three different keys with large key space, complexity, randomness, and high complexity. It keeps the intruders from gaining access to original medical images.
- The BCAES protects personal medical information and validates medical data using blockchain technology. As a result, privacy and data integrity have both improved.
- To check the integrity and authenticity of medical images, the concept of blockchain along with cloud server is introduced where the signed document of images is stored in blockchain, and data user can easily validate the image after verifying it through the blockchain.

The remainder of the paper is structured as follows: Section "[Related work](#)" illustrates related works of the scheme. Section "[Mathematical preliminaries](#)" is about mathematical preliminaries. Section "[Proposed blockchain based chaotic Arnold's cat map encryption scheme \(BCAES\)](#)" presents the proposed BCAES and the encryption/decryption process of the scheme. Section "[Comparative results and performance evaluation](#)" is devoted to performance evaluation. Conclusion and future work will be discussed in Section "[Conclusion](#)".

Related work

Mondal and Goswami²¹ presented an operative honeypot technique for cloud computing documents protection. Initially, a normalization procedure substitutes for and eliminates undesirable missing values from the collection. Following that, the GLCM quality selection algorithm and CNN classifier predict and categorize the assault types²². In this strategy, a cryptographic technique (honeypot) is used for encrypting the data. The CS is responsible for the key creation and key verification as well with the user for authentication. After that, the data

owner requests information from the cloud server. Honey-pot technique is used to decrypt the information after entering the key by the user. This gives valuable security, but at a great expense.

Ali et al.²³ demonstrated an encrypting technique for health care data built on a Henon chaotic map and a logistic tent map. In this encryption approach, the user produces a private encryption key by utilizing the medical center's public key. The proposed chaos-based medical image encryption method then encrypts with a private key. After that, the user digitally signs the encrypted image and sends it along with the digital signature and authentication parameters to the administrators. Finally, using a cipher image, secret key, and a digital signature, the healthcare corporation constructs the shared secret key. The authority then uses that secret key to decrypt the picture, checks it using an authenticating factor, and validates it if it is authorized.

Padhy et al.²⁴ proposes a high-level, cloud-based rural health records system that delivers low-cost services to rural residents. They have saved personal details in a cloud-based system that authorized medical researchers and doctors may use for better medical facilities and illness diagnostics in remote places. Patients have privileged access to their health information and medicines at any time for prompt treatment. This technique is less expensive than others and removes the time and other procedures required to register at a hospital.

Neela and Kavitha²⁰ proposes a Blockchain based, secured model known as BCDGE. In this model, the health care data is kept in the cloud after applying the encryption technique using Chaotic Deep GAN. It generates the private key, which is then followed by the processes of confusion and diffusion. Then the XOR approach decrypts the image by using private key that was generated. Then the sender uploads the cipher image into the cloud, makes a digital signature of it using the hash function, and stored it into blockchain. Then the digital signature may be utilized to validate the ciphertext image's validity. The suggested Chaotic Deep GAN approach features pseudo randomness, a large key space, and is particularly sensitive to alteration, according to experimental results and security studies.

For MI cloud storage, Lakshmi et al.²⁵ presented the HNN-IES (Hopfield Neural Network Images Encryption Scheme). This structure is divided into five phases. The underlying stage depicts flexible key generation using a recursive neural network. Following that, the stage shows a photograph of an explicit and unpredictable arrangement generated using HNN. The confusion and diffusion measures are therefore arranged separately in phases 3 and 4. Finally, it demonstrates the operational connection between the cloud and cryptosystem.

MeDShare²⁶ is a cloud-based healthcare data sharing platform that uses blockchain technology. The authors of this system employed smart contracts and authentication and authorization on data access via a separate platform. When transferring healthcare data between cloud structures, MeDShare can safely accomplish and maintain data authenticity and accountability. ProvChain²⁷ is a cloud-based, strong authentication system designed to improve availability and address privacy concerns. This technique is completely decentralized and relies on cloud computing for tamper-proof access through blockchain technology.

To protect medical images in the cloud, Afzal et al.²⁸ developed the biplane and Chaotic Image encryption. Initially, a biplane and chaotic encryption (BCE) used for encrypting the medical images. The chaotic key sequence key is obtained by merging the two keys obtained using the logistic map and a linear feedback shift register. Finally, after effectively retrieving the cipher image from the CS, the technique is employed to extract the plain medical image. This approach has a significant computational cost.

Mathematical preliminaries

The following mathematical ideas are used in our proposed encryption scheme: The Henon map, the orthogonal matrix, and the Arnold's cat map (ACM). Chaotic maps are the basic maps that are affected by their initial parameters. A small modification in the initial conditions can have a huge influence on the outcomes.

Henon map

Michel Henon created the Henon map in 1969. It is a discrete dynamic map with chaotic behavior due to its sensitivity to initial parameters. Mathematically, it can be expressed as follows:

$$\left. \begin{aligned} Y_{n+1} &= 1 - aY_n^2 + bZ_n \\ Z_{n+1} &= bY_n \end{aligned} \right\} \quad (1)$$

The violent behavior of chaotic system is determined by the values of the control parameters a and b . The Henon map's parameters and conditions are as follows:

1. Y_0 , where Y_0 is the initial value.
2. a is the controlled parameter, where $a \in [0, 1[$.
3. K_1 is the secret key for the permutation phase in encryption, where $K_1 = (a, Y_0)$

For $a = 1.4$, $Y_0 = 0.631$, $b = 0.3$, $Z_0 = 0.189$, this structure is chaotic. Eventually, a slight modification in parameter values might cause a system to behave differently.

It has various beneficial characteristics, including the Lyapunov exponent, unpredictability of behavior, and uniform non-variation of the intensity variable. Because of such qualities, the Henon map is highly suggested for cryptographic functions.

Orthogonal matrix

A matrix T is considered to be orthogonal if and only if it has the following properties:

$$T^t T = I \quad (2)$$

$$T^t = T^{-1} \quad (3)$$

where T^t is called the transpose of T where I is the identity matrix. During encryption this orthogonal matrix T is calculated using a plane equation $ax + by + cz = d$, where $a, b, c, d \in \mathbb{R}$.

Arnold's cat map (ACM)

ACM is a well-studied example of a discrete system with chaotic behavior²⁹. In 1960, V. Arnolds come across Arnold's cat map (ACM). He incorporated a cat picture into his work. Assuming pixel image as $P = \{(x, y) | x, y = 0, 1, 2 \dots N - 1\}$, 2-D ACM can be written as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \pmod{n} \quad (4)$$

$$A = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \pmod{n} \quad (5)$$

where p, q are positive integers, such that $|A| = 1$. It can also be written in the form of equation by taking $p = 1, q = 1$ as:

$$\left. \begin{aligned} x_{n+1} &= 2x_n + y_n \\ y_{n+1} &= x_n + y_n \end{aligned} \right\} \quad (6)$$

By using ACM, it generates an arbitrary image in the intruder's eyes by shuffling all the image's pixels. As a result of seeing the shuffled image, the attacker becomes confused and is unable to establish the accuracy of the image, which is used in the encryption process. So, the parameter R (number of iterations) in Arnold's cat map technique can be used as a secret key K_3 .

Proposed blockchain based chaotic Arnold's cat map encryption scheme (BCAES)

The five primary components of the BCAES are the data sender, CS, data user, blockchain, and encryption/decryption process. The system model of the BCAES is depicted in Fig. 1. Initially, the sender encrypts the medical images and makes a digital signature of it through the hash function SHA-256. Then the sender will encrypt the medical image using the Image encryption algorithm which is discussed in Section "Image encryption algorithm" and then encrypted image will be stored in cloud server and the signed document will be stored in blockchain. When the data user wants the medical image, he will place a request for ciphertext to cloud server. Then, the cloud server will send the relevant encrypted file to the user. After getting the cipher image, the data user will decrypt it using ACM decryption process illustrated in Algorithm 5. Now to check the integrity and authenticity of image, data user will send the decrypted file into blockchain and blockchain will validate it and sends a verification message in the form of yes or no. The primary components of our proposed model are listed below:

- *Data Sender* Data sender (who might be patients) encrypts the medical images using the ACM encryption scheme and sends the retrieved medical information to CSP. The data sender also signed the encrypted image, which is then saved into the blockchain network.
- *Cloud Server (CS)* The cloud server has two goals:
 - To store massive amounts of medical image data
 - The other is to seek for and sends the correct ciphertext in response to the data user's request.
- *Data user* To obtain the encrypted image, the data user (health professionals) requests the health care information from the CS. Furthermore, the users validate the ciphertext's validity by cross-checking the ciphertext's ID saved in the blockchain.
- *Blockchain* For creating digital signature, we used the SHA-1 algorithm to create a hash value of the image. When the data user requests a validity check, the blockchain validates the stored signature to authenticate the ciphertext's authenticity. If it is true, it returns 1; otherwise, it returns 0.
- *Encryption/Decryption* The medical image is first encrypted using Arnold's cat map (ACM) with an orthogonal key matrix and Henon map before being sent to the cloud server, whereas the inverse process will be the decryption process.

Image encryption algorithm

The image encryption algorithm is split into three phases. The first phase (confusion) uses Henon map to construct a sequence for permuting image pixels. The permuted pixels are combined with the key invertible matrix formed by a secret orthogonal matrix in the second step (permutation)³⁰. The last phase (diffusion) consists of a unique sequence created from a new Arnold's cat map that is XORed with earlier obtained outcomes. The density of the proposed scheme contributes to its resistance to attacker attempts. The process of our proposed encryption algorithm is shown in Fig. 2.

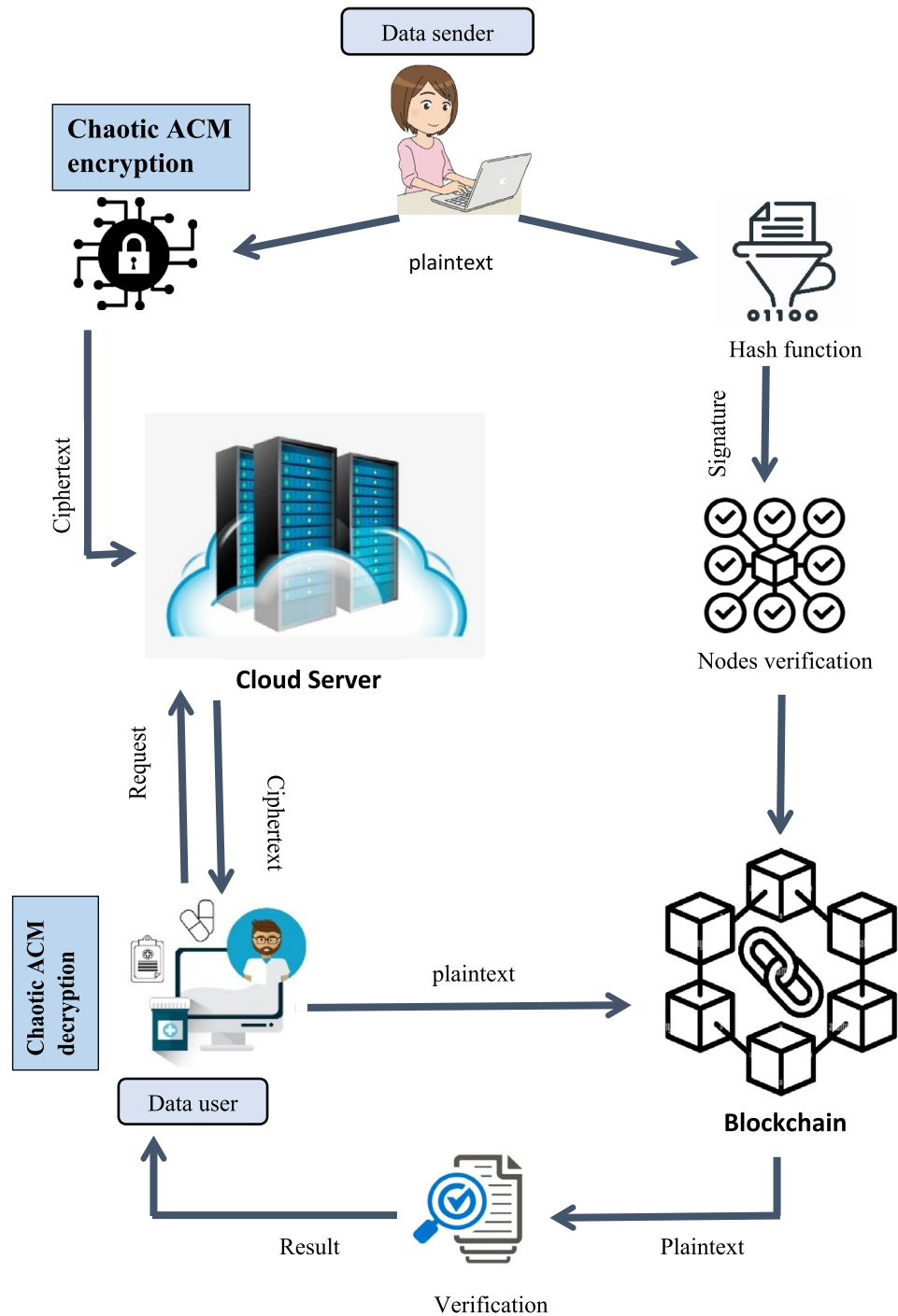


Figure 1. Model of proposed BCAES.

Permutation phase

As demonstrated in Algorithm 1, the permutation phase of our proposed encryption scheme comprises permuting the location of the pixels in an original image. In the first phase of our strategy, we use the Henon map with key K_1 to permute the pixel locations³¹. The Henon map is repeated using K_1 to generate a sequence. The chaotic sequence that is generated is sorted in ascending order. By comparing the structures of chaotic and sorted sequences, the permuted sequence is obtained. Using the permuted sequence, the original image’s one-dimensional array is recovered. The typical rule for picture variety is to choose any volume of $P \times Q \times 3$ pixels colorful picture, where Q and P are the width and height, correspondingly. The size of the original image and the encrypted image will remain unchanged.

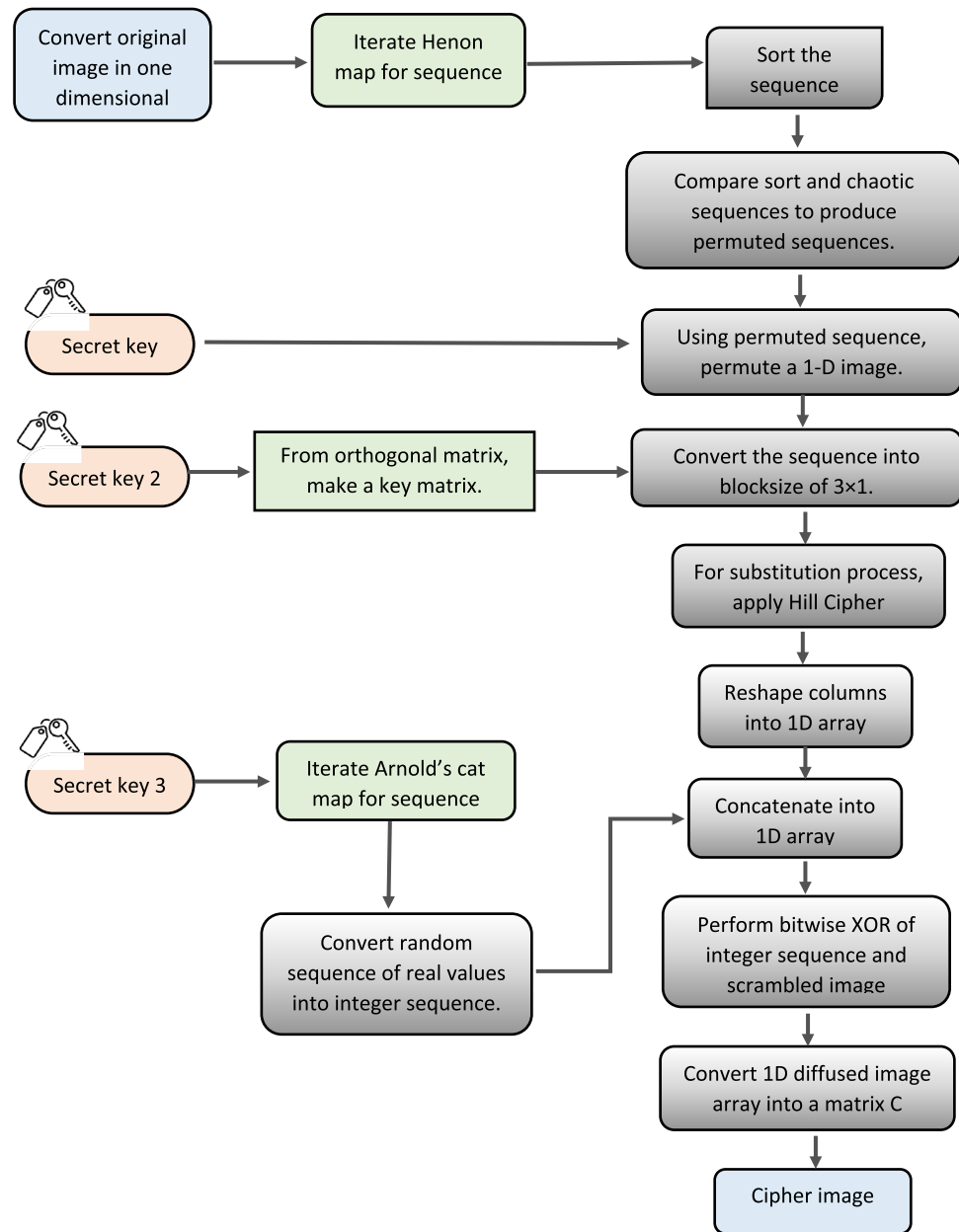


Figure 2. Workflow of encryption algorithm.

Input: Colored Medical image (I), Henon map (1), and Secret key $K_1 = (a, X_0)$.

Result: An array P of permuted pixels of medical picture (I).

1. Consider the medical image I , that is kept in an array A having dimensions $D = P \times Q \times 3$, such that P represents the quantity of rows and Q represents the quantity of columns of the image matrix I .
2. Generate a chaotic sequence $F = \{F_1, F_2, F_3, \dots, F_n\}$. using the key K_1 with Henon map. Now sort the sequence F in ascending order such as $\underline{F} = \{F_1, F_2, F_3, \dots, F_n\}$.
3. Generate the permutation vector G by observing the locations of the sequence values of F in \underline{F} and writing the altered places $G = \{G_1, G_2, G_3, \dots, G_n\}$.
4. Use G to calculate the location of an array Y to obtained P.

Algorithm 1. Pixel Permutation

Substitution phase

In this phase, the key K_2 is expressed as the orthogonal key matrix, which is created from an equation of a plane as shown in Algorithm 2. After generating key K_2 , Hill cipher will be applied to get an array E of same size as D in permutation phase. To generate an array E, firstly the permuted picture is sub-divided into $D/3$ blocks. These $D/3$ sub-sections are then multiplying with K_2 separately. After that the result will be arranged in 1-D Array E. Mathematical implementation of substitution phase is discussed in Algorithm 3.

Input: plane equation $ax + by + cz = d$, where $a, b, c, d \in \mathbb{R}$

Result: Key K_2 in the form of orthogonal matrix with dimension 3×3 .

1. Let the unit vector v span the orthogonal line O.

$$v = \frac{(a, b, c)}{\sqrt{a^2 + b^2 + c^2}}$$

From the equation $T_w = w - 2v\langle w, v \rangle$, where $\langle w, v \rangle$ is the inner multiplication of w and v .

2. For $w \in \mathbb{R}^m$, the basis vectors for $m=3$ are represented below:

$$w_1 = \{w_{11}, w_{12}, w_{13}\} = \{1, 0, 0\}, w_2 = \{w_{21}, w_{22}, w_{23}\} = \{0, 1, 0\}, \text{ and}$$

$$w_3 = \{w_{31}, w_{32}, w_{33}\} = \{0, 0, 1\}.$$

3. Resulting orthogonal key matrix will be written as follows:

$$K_2 = \begin{bmatrix} Z_{w_{11}} & Z_{w_{12}} & Z_{w_{13}} \\ Z_{w_{21}} & Z_{w_{22}} & Z_{w_{23}} \\ Z_{w_{31}} & Z_{w_{32}} & Z_{w_{33}} \end{bmatrix}$$

Algorithm 2. Key generation for substitution phase

Input: Orthogonal matrix K_2 with permuted image array P.

Result: Array E of order D.

1. Using algorithm 2, K_2 will be generated under modulus 256 of order 3×3 .
2. Generating building block H_n
 - i. Convert 1-D array E into vector blocks of size 3×3 . The nth block is represented as H_n , where.

$$n = 1, 2, 3, \dots, D/3$$

- ii. Apply the following Hill cipher formula.

$$A^n = K_2 \times H_n \pmod{256}$$

- iii. Again, arrange all A^n in a 1-D array such that.

$$E = \{A^1, A^2, A^3, A^4, \dots, A^{D/3}\}$$

Algorithm 3. Applying Hill cipher with orthogonal key matrix.

Diffusion phase

In final phase of the encryption scheme, the diffusion of pixels is illustrated in algorithm 4. In the last phase, a key K_3 is used to generate a sequence using Arnold's cat map (ACM)²⁸. Using Eq. (7), the standards of the generated sequence are modified into an integer sequence. The 1-D Array E is then bitwise XORed with the corresponding integer sequence generated by ACM. A matrix for the encoded picture has similar size as original picture is generated by rearranging the 1-D array.

Input: Array E, secret key K_3 , ACM.

Result: Cipher Image I' .

1. Produce a sequence $R = \{R_1, R_2, R_3, \dots, R_m\}$ with key K_3 and Arnold's cat map (ACM).
2. Transform W into an integer sequence using following equation.
3. To create an array, combine every single element of array E with the parallel member of P_K and execute a bitwise XOR.

$$P_K = \text{floor}(\text{mod}(R_K \times 10^{14}, 256)) \quad (7)$$

$$C_j = P_j \oplus E_j \oplus C_{j-1}, \text{ where } j = 1, 2, 3, \dots, m$$

4. Now convert the array C_j into its matrix form represented as I' , with size

$$D = P \times Q \times 3$$

Algorithm 4. Diffusion of pixels

Image decryption process

The reverse encryption method is used in the picture decryption process to get the original image. Algorithm 5 depicts three steps of the suggested decryption technique. In the first step, the Arnold's cat map (ACM) sequence is XORed with the key K_3 . K_2 is used to implement the Hill cypher using the invertible matrix. The Henon map is used to create a random sequence, and the inverse permutation is achieved by employing the key K_1 . The inverse permutation is used to reverse the permutation. To acquire the original image, the preceding array is translated into an image form³².

Input: Private keys K_1, K_2, K_3 , Cipher image I' , Henon map and ACM.

Output: Original colored medical image (I)

1. Convert the matrix form cipher image I' of order $P \times Q \times 3$ into an array.
2. By using K_3 , generate a sequence R of order $P \times Q \times 3$ and then, XOR it with the integer sequence from equation (9).
3. Every component of I' is pre-decrypted as:

$$E_j = P_j \oplus C_j \oplus E_{j-1}, \quad \text{where } j = 1, 2, 3, \dots, m$$

4. Create orthogonal matrix as K_2 as written in algorithm 2.
5. Convert the 1-D array E in vector building block H_n having dimension 3×1 .
6. Now execute the hill cipher as written in Eq. (8).

$$A^n = K_2 \times H_n \pmod{256} \quad (8)$$

7. Convert all A^n back into 1-D array P .
8. Iterate the Henon map using key K_1 to generate a sequence F . now by cataloguing H in ascending order we can obtain \underline{F} .
9. Apply inverse transformation position G^{-1} to obtain the permutation array.
10. To obtain Y , use G^{-1} on P .
11. Now convert the array in a matrix form of order $D = P \times Q \times 3$ to get original colored medical image (I).

Algorithm 5. Decryption process

Signature creation

Once the encryption procedure is complete, the sender transmits the secured health care data to the cloud server (CS) and uses a hashing algorithm to store the hash value of the medical image on the blockchain. This might be done for ciphertext integrity and authenticity. In our proposed scheme, we will apply SHA-256 to form a hash value (signature) of the encrypted image so that attackers cannot get access to the image as hash functions are one-way functions. It is impossible to decrypt the hashing value back to the original medical image³³.

Signature verification

Finally, the user verifies the signature stored into the blockchain to ensure the validity of the ciphertext. When the data user sends the decrypted image into the blockchain. The blockchain will create a hash value of it using SHA-256 and then matches the hash value of decrypted image with the hash value of original image stored into the blockchain by data sender. If it matches up, the data is authentic; otherwise, it is not. If the data is authentic or not, the blockchain will send a verification message in the form of yes or no to data user. The signature verification method is depicted in Fig. 3.

Comparative results and performance evaluation

The tests were accomplished on a UBUNTU 16.04 desktop computer equipped with an Intel(R) Core (TM) i7-6700 @ 3.40 GHz processor. The simulation is conducted using Matlab 2018a. To simulate the suggested system, we take a private blockchain using the Geth Ethereum client. Ethereum is a popular blockchain platform, and its performance has been studied by developers and researchers. Table 1 lists the software utilized for implementation.

The sample images are saved from BraTS18 dataset³⁴, the Ultrasonic Brachial Plexus dataset³⁵ and the Montgomery country chest X-rat dataset³⁶, because they represent three different anatomical regions. The sample images are colored with pixel values of length (256×256) . After encrypting the images we get the encoded image of same size i.e. (256×256) . When using a decryption technique, the encoded image and the plain image are recovered employing the methods of pixel permutation by the Henon map, pixel substitution using hill cipher with orthogonal key matrix, and pixel dispersion by Arnold's cat map. The result obtained from our

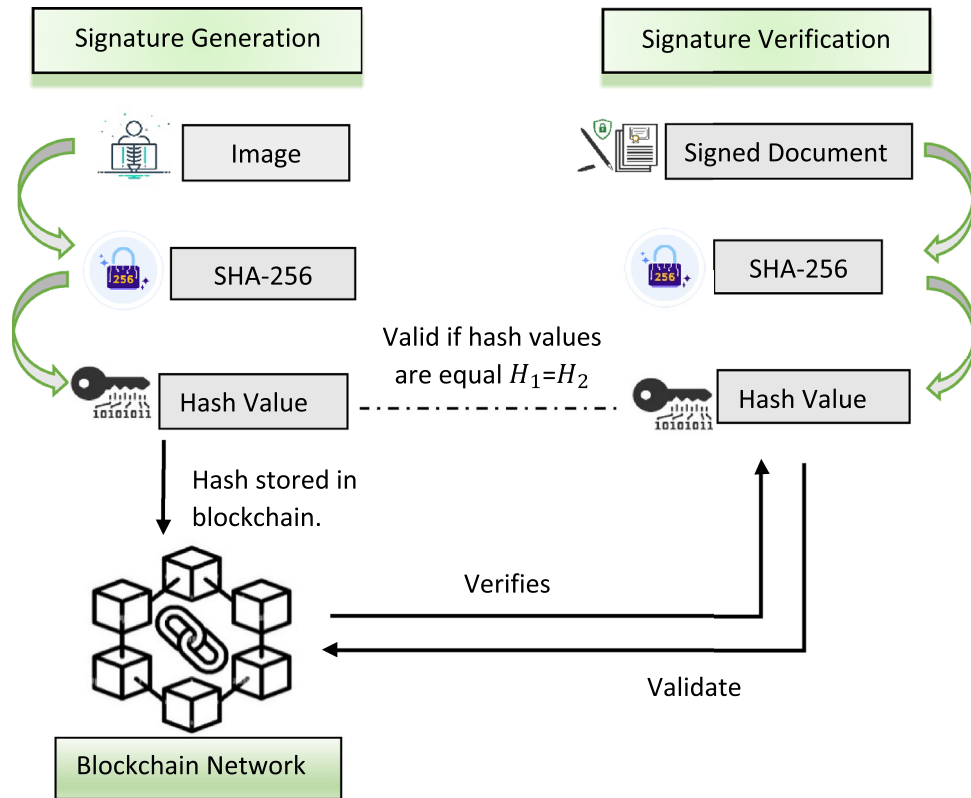


Figure 3. Model of signature generation and verification.

Software	Use	Version
Windows	Operating system	8.1
Mist	Ethereum wallet	0.9.2
Geth	Command line Ethereum client	1.7.2
Claymore pool	Claymore’s Dual Ethereum AMD GPU Miner	10
Cloud	Average RAM	512 MB
	Number of virtual machines	34
	Number of users	100
	Average bandwidth	1,000,000 MB

Table 1. Setup of parameters.

proposed encryption scheme is shown in Table 2. In our proposed encryption scheme, we use $K_1 = (0.631, 0.189)$, $K_3 = (0.015, 0.223)$, and

$$K_2 = \begin{bmatrix} 0 & 204 & 153 \\ 204 & 113 & 20 \\ 153 & 20 & 144 \end{bmatrix}$$

Security analysis

We will test our encryption scheme by some sort of security analysis mentioned below like key space analysis, key sensitivity analysis, Histogram analysis, Chi-square analysis, Information entropy etc.

Key space analysis

In essence, key space analysis examines every possible key that may be used during encryption. The key’s size must be sufficient to avoid brute force attacks. If the key space is greater than 10^{30} , an algorithm can avoid exhaustive attacks using existing statistical methods³⁷. Our proposed encryption scheme depends upon three different keys. Henon and Arnold’s cat map’s control parameters make up the keys K_1 and K_3 , respectively. The overall number of chances to select the keys might be $(10^{15})^2 \times (10^{15})^2 = (10)^{60} \approx (2)^{240}$. In our suggested encryption

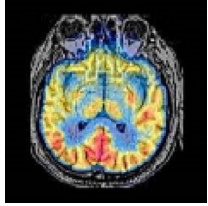
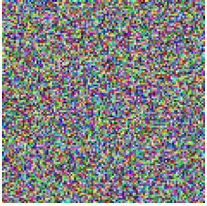
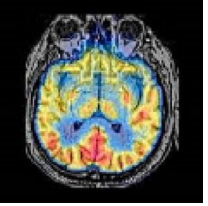
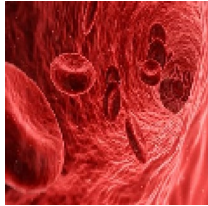

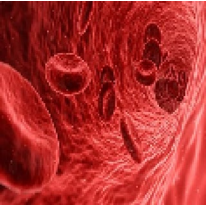
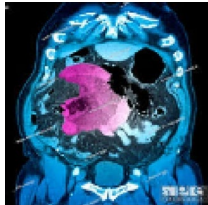
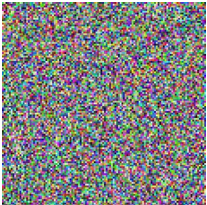
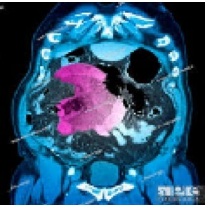

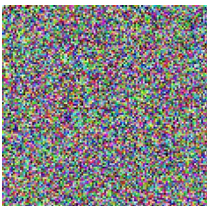

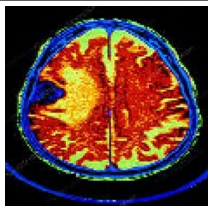

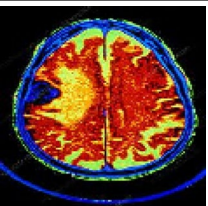
Sr. No.	Original	Encrypted	Decrypted
1			
2			
3			
4			
5			

Table 2. Encryption and decryption result of our proposed scheme.

scheme, first and last phase is secure enough to be protected against a brute force attack, even if the size of the keys for two algorithms can be up to 60. Consequently, K_2 's key space is infinite in size, as there are unlimited alternatives for selecting the four coefficients a , b , c , and d since the second key K_2 for the substitution phase is produced using an equation of the plane $ax + by + cz = d$, where $a, b, c, d \in \mathbb{R}$.

Key sensitivity analysis

The scheme's secret keys are fundamental to its encryption scheme. Three keys make up the encryption method we suggest. With the current approach, even a very slight modification to any portion of the secret key causes a complete change in the decryption algorithm's result. This indicates that if we modify the first key $K_1 = (a, X_0)$ by adding 0.0000000000000001, we will not be able to retrieve the original medical image using that key. It's obvious that the encrypted image lacks any hints or gestures from the original image. Our suggested cryptosystem's algorithms are extremely vulnerable to secret keys.

Information entropy

This measurement has been used to assess the degree of uncertainty and quantify the randomness or instability of a private key. Equation (9) is used to determine the information entropy of images.

$$\sum_{i=0}^{m-1} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (9)$$

where m is the quantity of pixels, as well as $P(m_i)$ stands for the chance that pixel (m_i) will appear³⁸. The maximum entropy for images is 8. The acquired private key has a fair amount of unpredictability, as demonstrated by its entropy, which is around 7.9992. Comparing different encryption techniques with our proposed scheme, Fig. 4 shows the entropy result for the images shown in Table 2.

Chi-square test analysis

It can support the regularity in the histograms of the encrypted images. The excellent consistency in encoded image histograms is demonstrated by the low chi-square value. It can be evaluated using Eq. (10).

$$Y_r^2 = \sum_{i=0}^{255} \frac{(O_i - E_i)^2}{E_i} \tag{10}$$

where E_i is the expected frequency and o_i is the observed frequency of i . Using Eq. (11), E_i (expected frequency) can be determined.

$$E_i = \frac{\text{sizeofanimage}}{26} \tag{11}$$

Figure 5 compares the Chi-Square value of our proposed chaotic ACM with existing techniques. It is clearly demonstrated from the figure that our proposed encryption scheme has high level of consistency as compared to other existing techniques.

Histogram analysis

Histogram analysis is a revolutionary method of evaluating image pixels. It must be distinguishable from the encrypted and original image. The simple image's pixels are constantly different and non-uniform. It is evident that the cypher image's histogram is largely uniform. It is clear, that the dispersion of pixels in the original image's cypher image does not provide any information³⁰. The three parts of the histogram for the original and cypher images—red, green, and blue—are displayed in Table 3. By Table 3, the histogram of cipher images is reasonably uniform. Regarding the dissemination of pixels in the original medical image, there is no proof. Thus, it becomes very challenging for hackers to retrieve useful information from the encrypted images.

Sensitivity analysis

The one-pixel value of the original picture is changed at random during the study. The suggested encryption method is then applied to the two images to generate two sets of private keys—one before and one after changing a pixel value. The variations between two private keys are now estimated using two methods to measure their sensitivity. Two metrics—the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity

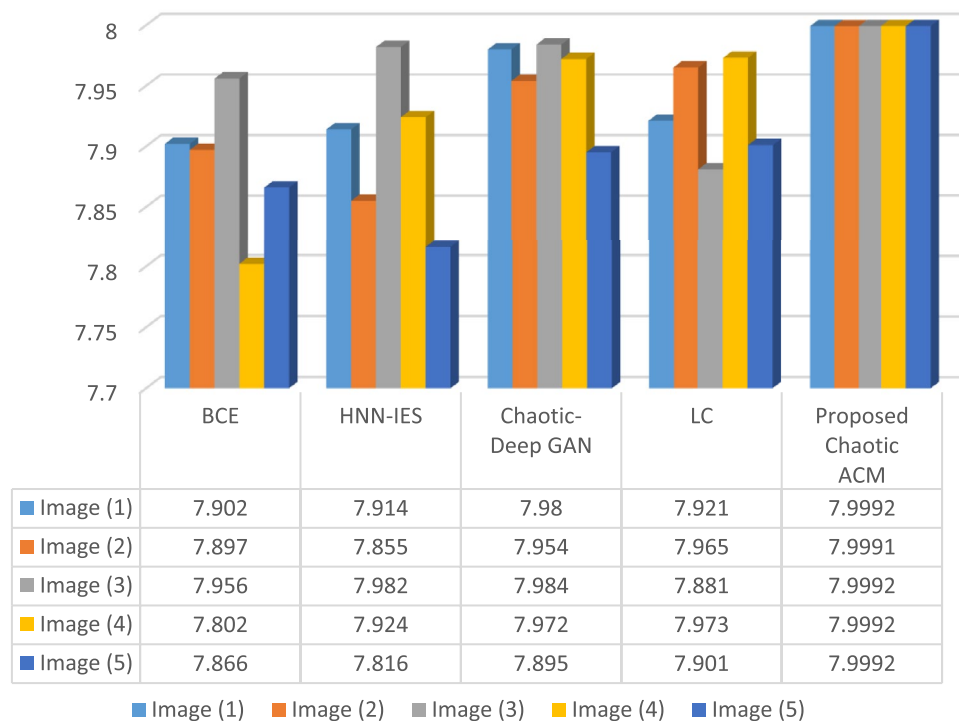


Figure 4. Comparison of entropy result for various methods.

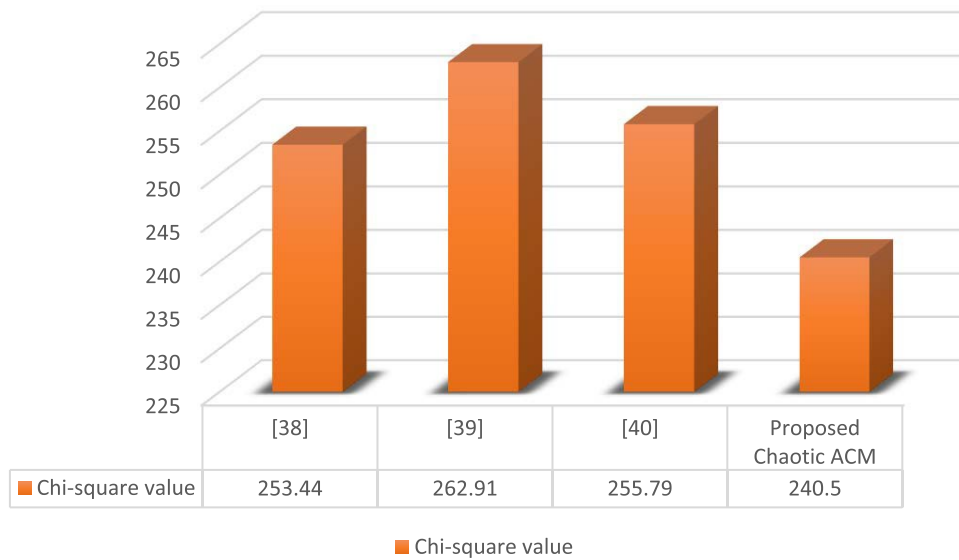


Figure 5. Chi-square test analysis.

(UACI)—are used to assess the deviation between the secret keys. The experiment demonstrates how even minor changes to the plain image may have a major influence on the encrypted images. When a greater value of NPCR is attained, a more secure cryptosystem is built that will protect against a variety of attacks. Equations (12) and (13) shows the formulas to calculate the NPCR and UACI respectively.

$$NPCR = \frac{\sum_{i=0}^m \sum_{j=0}^n R(i,j)}{I_s} \times 100 \tag{12}$$

$$UACI = \frac{1}{I_s} \left[\sum_{i=0}^m \sum_{j=0}^n \frac{|X(i,j) - X'(i,j)|}{256} \right] \times 100 \tag{13}$$

And,

$$R(i,j) = \begin{cases} 1, R_1(i,j) \neq R_2(i,j) \\ 0, R_1(i,j) = R_2(i,j) \end{cases} \tag{14}$$

where R_1 and R_2 represent the pixel values at location (i,j) , and I_s represents the size of the image.

According to Fig. 6, a little change in the actual image’s pixel value resulted in changes between generated private keys of over 99.63%, by average intensity changes exceeding 33%. It indicates that the generated secret key is sensitive to the original image and thus fulfills both randomness and uncertainty.

Correlation analysis of nearby pixels

The correlation coefficient demonstrates similarities between contiguous pixels in the diagonal, horizontal and vertical ways. The confusion and diffusion processes between the original and encrypted image are tested using correlation Cr . It may be computed using Eq. (15).

$$Cr = \frac{m(\sum_{i=1}^n p_i q_i - \sum_{i=1}^n p_i \sum_{i=1}^n q_i)}{(m \sum_{i=1}^n (p_i)^2 - (\sum_{i=1}^n p_i)^2)(m \sum_{i=1}^n (q_i)^2 - (\sum_{i=1}^n q_i)^2)} \tag{15}$$

wherever, p_i and q_i are the values of two nearby pixels, and m is the total pixel value used to calculate the coefficient. The maximum correlation factor value of 1 indicates that there is a strong association between neighboring pixels³⁹. In order, to prevent an attacker from obtaining the necessary data, the proposed cryptosystem must employ low correlation coefficients that are close to zero. Table 4 displays the correlation distribution values for the original and cypher images in three different orientations. The pixels RGB component distribution of the encrypted medical images is shown in Table 5 vertically, horizontally, and diagonally. The data demonstrate that neighboring pixels in the encrypted image are not correlated since they are nearer to 0. In comparison, 16,430 pairs of random pixels are used, along with 4500 pairs of randomly selected surrounding pixels.

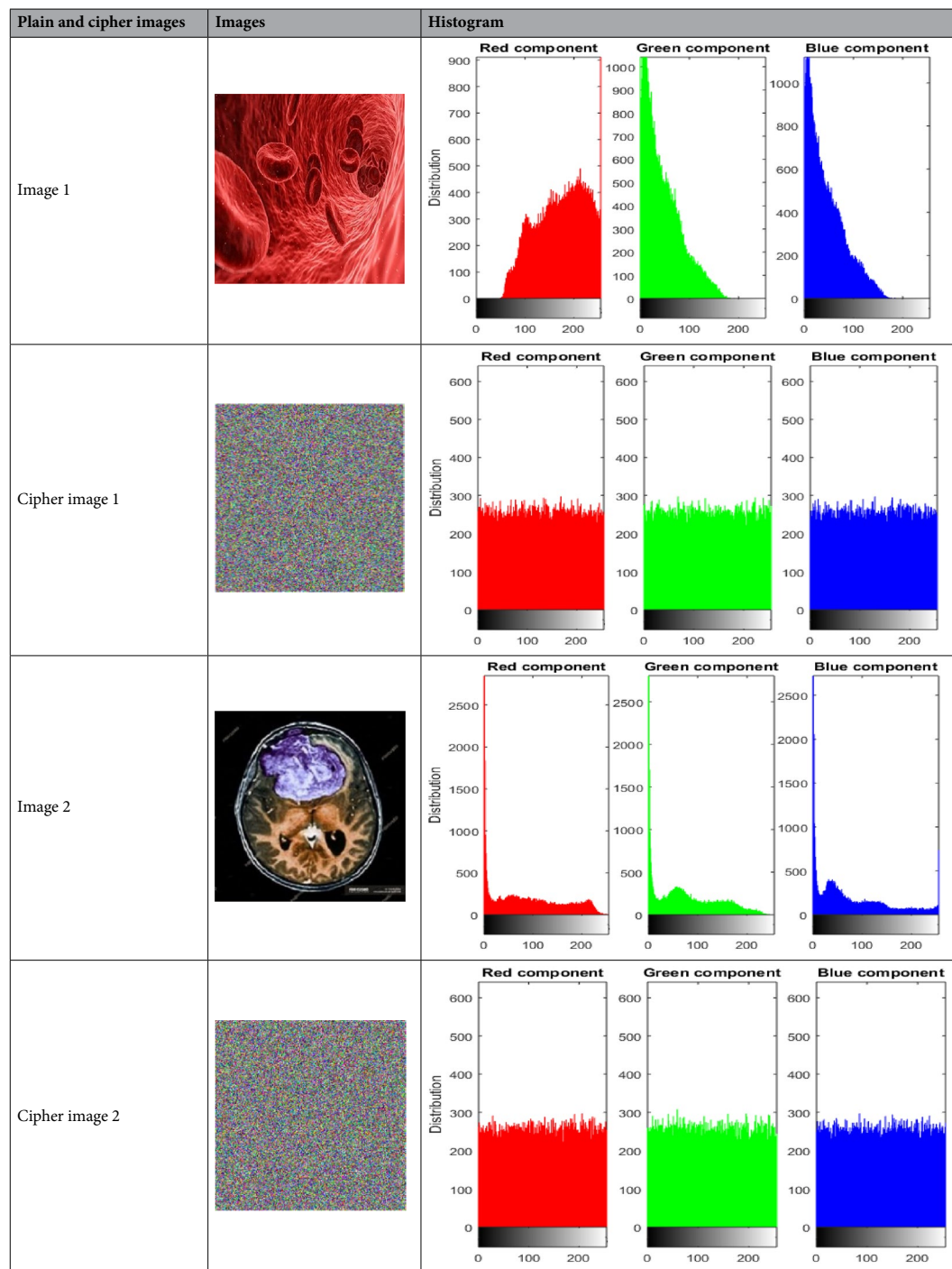


Table 3. Histogram analysis.

Similarity analysis

To preserve the standard of medical image in our proposed cryptosystem, we will apply some similarity analysis like Mean Square Analysis (MSE), Structural similarity Index Measure (SSIM), Peak Signal Noise Ratio (PSNR) etc. And then compare our proposed schemes with already existing techniques like BCDGE, HNN-IES and BCE.

Mean square analysis

The accuracy and variance between two images are assessed using the mean square error (MSE). A high MSE score indicates significant variation between the original and encrypted images^{31,40,41}. The MSE values are calculated using Eq. (16).

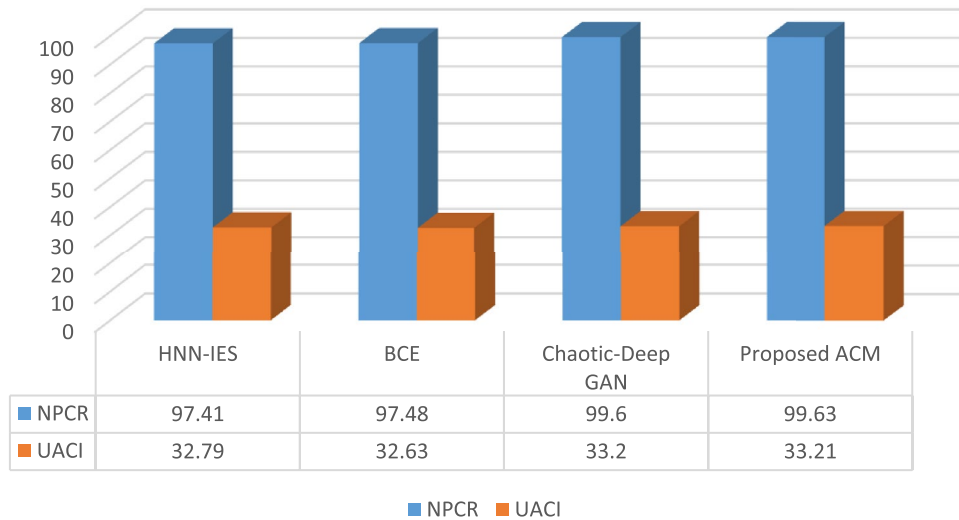


Figure 6. Comparison of NPCR and UACI valued for different methods.

Direction/color		Horizontal	Vertical	Diagonal
Blue	Original	0.9776	0.9759	0.9568
	Encrypted	0.00007	0.0044	-0.0019
Green	Original	0.9668	0.9688	0.9402
	Encrypted	0.0036	-0.0006	-0.0030
Red	Original	0.9597	0.9711	0.9365
	Encrypted	0.0009	0.0064	-0.0027

Table 4. Correlation coefficient values.

$$MSE = \frac{1}{I_d} \sum_{k=1}^P \sum_{l=1}^Q (M(i,j) - N(i,j))^2 \tag{16}$$

where I_d represents the dimension of the image, $M(i,j)$ represents the ($M(i,j)$) denotes the original medical image, and ($N(i,j)$) denotes the encoded image. Figure 7 shows the relationship among the MSE values of our proposed cryptosystem with some existing techniques like HNN-IES, BCE, Chaotic-Deep GAN.

Peak signal noise ratio (PSNR)

To compare the ciphered picture’s quality to the plain image, PSNR analysis is performed. A low PSNR value parallels to a significant change between the encrypted and the original image. PSNR can be investigated using Eq. (17).

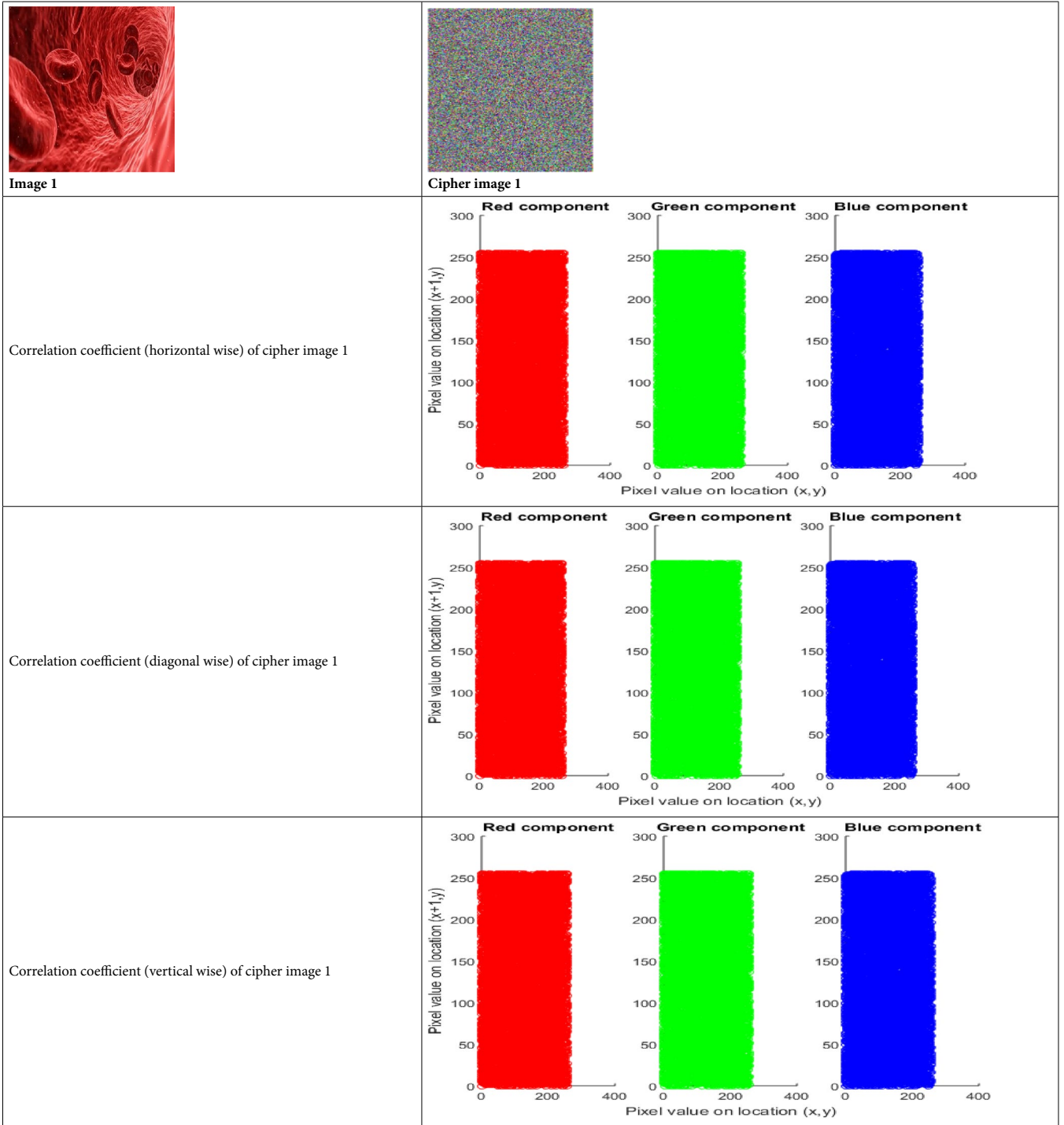
$$PSNR = 10 \cdot \log \frac{255^2}{MSE} \tag{17}$$

Structural similarity index measure (SSIM)

It is used to determine the resemblance among colored plain image and cipher image. Equation (18) is used to calculate the SSIM value for images.

$$SSIM = \frac{(2\mu_{p_1}\mu_{p_2} + s_1)(2\delta_{p_1}p_2 + s_2)}{(\mu_{p_1}^2\mu_{p_2}^2 + s_1)(\delta_{p_1}^2\delta_{p_2}^2 + s_2)} \tag{18}$$

where p_1 and p_2 indicates two images, $2\delta_{p_1}p_2$ denotes the covariance of p_1 and p_2 , $\delta_{p_1}^2$ denoted the variance of p_1 , $\delta_{p_2}^2$ denotes the variance of p_2 , μ_{p_1} denotes the mean value of p_1 , μ_{p_2} denotes the mean value of p_2 , and s_1 and s_2 are constants to ensure stability of images. A greater SSIM score, which ranges from 0 to 1, denotes a high degree of similarity between two images. Our proposed BCAES is evaluated using 5 different medical images and comparison between values of Average PSNR and SSIM with some other schemes are represented in Fig. 8.



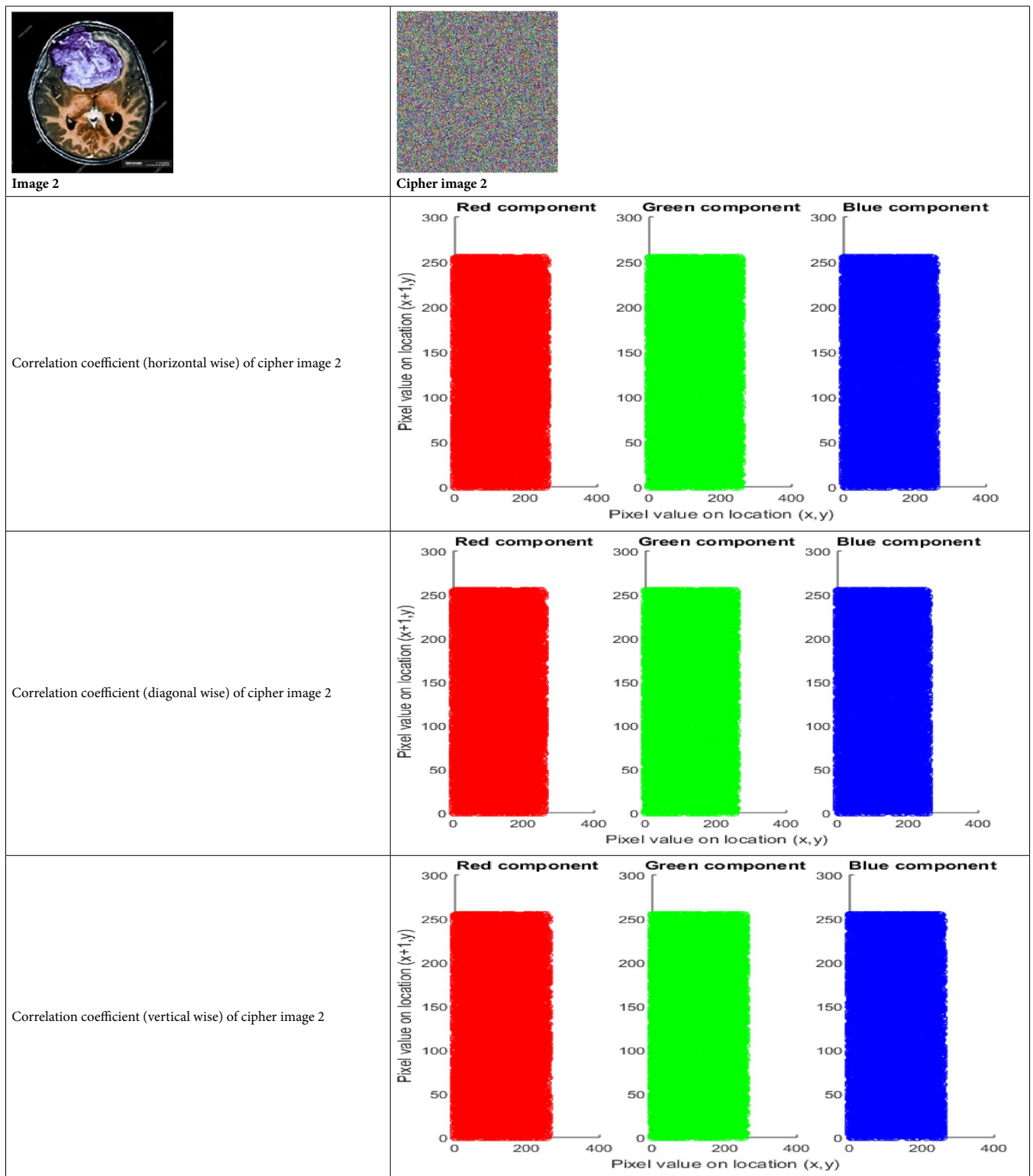


Table 5. Correlation analysis of adjacent pixels for proposed cryptosystem.

Time complexity

The runtime of chaotic ACM encryption on medical photos of various resolutions is evaluated in Fig. 9 to evaluate the performance of the proposed network. At 256×256 resolution, our proposed encryption scheme can encrypt and decrypt 32 medical images per second, but 28 at 512×512 resolution. On pictures of 512×512 and 256×256 resolution, our method has been demonstrated to give the shortest encryption times when compared to competing approaches like HNN-IES, BCE and BCDGE.

Differential attack analysis

Differential attacks are a kind of attacks where a criminal makes an effort to decrypt a picture without using private keys. For this, the intruder/attacker arbitrarily chooses a set of ordinary images, gain access to the encryption device to produce the corresponding encrypted images and then relates the cipher images to extract the mysterious data⁴². To ascertain the impact of one pixel value change in original image on the cipher image, a differential attack is employed. Therefore, the harder it is for attackers to figure out how to connect an encrypted image to a plain image, the greater the NPCR number. According to Fig. 6's findings, the suggested encryption strategy has a greater NPCR value than the approaches currently in use, demonstrating its effectiveness in combating differential attacks.

Integrity and confidentiality analysis

A significant security problem is the privacy of healthcare information stored in the cloud. Cloud companies have taken measures to protect the secrecy of their data due to the high costs of reputation damage. Due to the availability of attackers, data secrecy in the cloud can't be readily preserved and safeguarded. Analysis of the proposed system's data integrity and confidentiality is therefore crucial. The suggested BCAES encrypts the medical images using three different private keys before sending them to the cloud server. Without these three different private keys, it is impossible to decrypt the encrypted image.

Moreover, the data saved on the cloud server can only be accessed by the organization or individual that has the data owner's permission. As a result, only authorized individuals can decipher the ciphertext, protecting the privacy of the data^{43,44}. Additionally, the signatures of each block guarantee data integrity. The blockchain network makes distinctions among different nodes and users based on their authenticity. The blockchain system ensures that only the authenticated user can decrypt the encrypted message using the secret keys by determining if the user has the right to do so.

Conclusion

Cloud storage solutions are vulnerable to several security issues due to their openness. Careful analysis of the security measures is necessary when creating a cloud-based database for medical images. As a result, this study recommends BCAES, a secure architecture based on blockchain. Here, we suggested a revolutionary chaotic map-based image encryption method that will be saved in the cloud. The suggested method first generates a permutation phase using a Henon chaotic map. A Hill cypher with a key derived from an orthogonal matrix by considering a plane's equation is employed for substitution. And then diffusion step uses an Arnold's cat map (ACM) to create a sequence, which is bitwise XORed with each pixel's value. The Henon map handles the confusion phase of the proposed algorithm's operation, while the ACM handles the diffusion phase. The sender than signs the ciphertext's ID puts it into the blockchain and uploads the encrypted image to the cloud. Later, the ciphertext image's integrity may be confirmed using the signature. The suggested Chaotic ACM approach features three different keys, a large key space, and is particularly sensitive to alteration, according to experimental results and security studies. Comparing the BCAES architecture to other current methods, a high level of protection/security is thereby offered. Not only confidentiality but also authentication and integration of data. Table 6 shows different analysis results of our proposed scheme.

Though, use of classical chaotic systems have some inherent limitations, such as periodicity, easy destruction of phase space, and low lyapunov exponent. To handle these issues, many researchers have focused on improving classical chaotic systems to enhance their chaotic dynamic characteristics through a process called chaotification. The goal of chaotification is to make up for these limitations and improve the performance of chaotic encryption algorithms. As a future goal, this work may be modified or extended by replacing the classical chaotic maps with the maps obtained after the chaotification process.

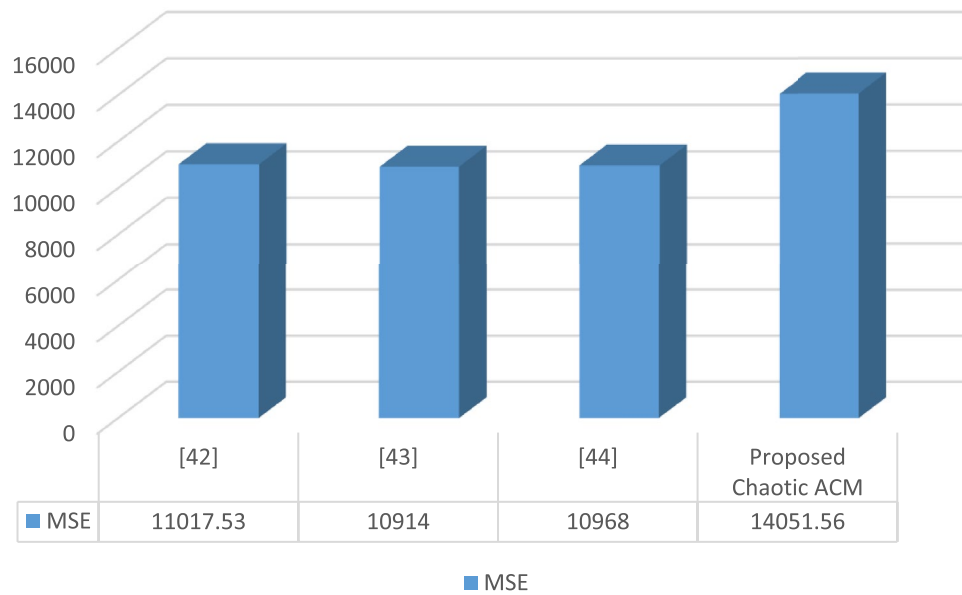


Figure 7. MSE analysis.

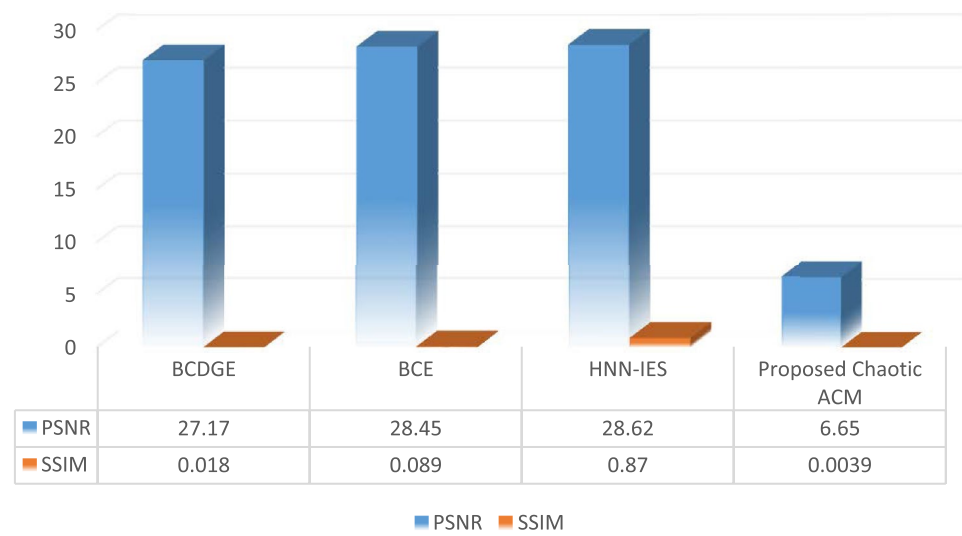


Figure 8. PSNR and SSIM analysis.

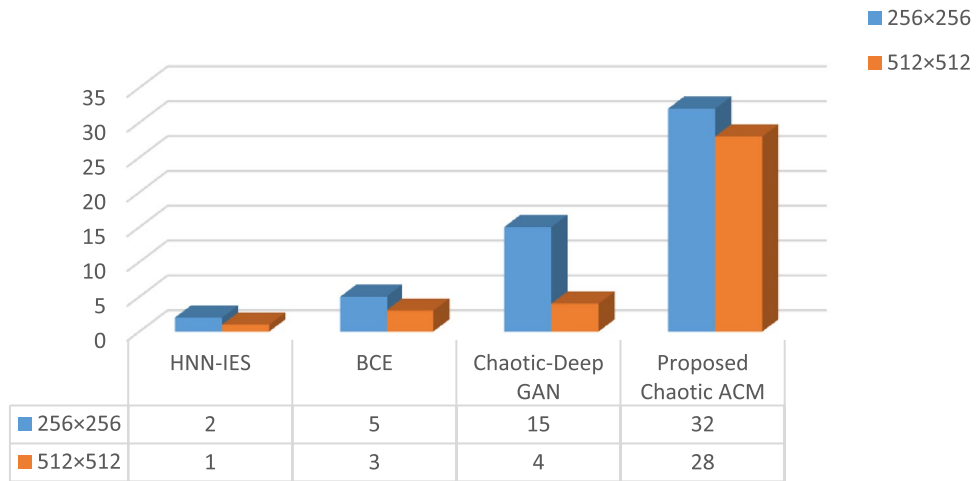


Figure 9. Analysis of time complexity.

Analysis of image encryption scheme	BCE ²⁸	HNN-IES ²⁵	Chaotic deep GAN ²⁰	Proposed model
(a)				
Information Entropy	7.902	7.914	7.980	7.9992
NPCR	97.48	97.41	99.60	99.63
UACI	32.63	32.79	33.20	33.21
PSNR	28.45	28.62	27.117	6.65
SSIM	0.089	0.87	0.018	0.0039
Time complexity	5 images per second	2 images per second	15 images per second	32 images per second
Analysis of image encryption scheme	³⁰	³⁹	⁴²	Proposed model
(b)				
Chi-square test	253.44	262.91	255.79	240.5
Analysis of image encryption scheme	³¹	⁴⁰	⁴¹	Proposed model
(c)				
MSE	11,017.53	10,914	10,968	14,051.56

Table 6. Analysis results.

Data availability

The data used to support the findings of this study are included within the article.

Received: 25 October 2023; Accepted: 5 March 2024

Published online: 07 March 2024

References

- Ravi, D., Ramachandran, S., Vignesh, R., Falmari, V. R. & Brindha, M. Privacy preserving transparent supply chain management through hyperledger fabric. *Blockchain Res. Appl.* **3**(2), 100072 (2022).
- Bokhari, M. U., Makki, Q. & Tamandani, Y. K. A survey on cloud computing. In *Big Data Analytics* 149–164 (2018).
- Mishra, S., Sharma, S. K. & Alowaidi, M. A. Analysis of security issues of cloud-based web applications. *J. Ambient Intell. Humaniz. Comput.* **12**(7), 7051–7062 (2020).
- Altowajiri, S. M. An architecture to improve the security of cloud computing in the healthcare sector. In *Smart Infrastructure and Applications* 249–266 (2020).
- Dutta, A., Misra, C., Barik, R. K. & Mishra, S. Enhancing mist assisted cloud computing toward secure and scalable architecture for smart healthcare. In *Advances in Communication and Computational Technology* 1515–1526 (Springer, Singapore, 2021).
- Sri Vigna Hema, V. & Kesavan, R. ECC based secure sharing of healthcare data in the health cloud environment. *Wirel. Pers. Commun.* **108**(2), 1021–1035 (2019).
- Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M. & Fouda, M. M. A new image encryption algorithm for grey and color medical images. *IEEE Access* **9**, 37855–37865 (2021).
- Pourjabbar Kari, A., Habibizad Navin, A., Bidgoli, A. M. & Mirnia, M. A new image encryption scheme based on hybrid chaotic maps. *Multimed. Tools Appl.* **80**(2), 2753–2772 (2021).
- Vaseghi, B., Mobayen, S., Hashemi, S. S. & Fekih, A. Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption. *IEEE Access* **9**, 25911–25925 (2021).
- Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K. & Chang, V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *J. Med. Syst.* **42**(8), 1–11 (2018).

11. Devi, K. R., Suganyadevi, S., Karthik, S. & Ilayaraja, N. Securing medical big data through blockchain technology. In *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)* Vol. 1 1602–1607 (IEEE, 2022).
12. Zhang, Q., Yang, L. T., Castiglione, A., Chen, Z. & Li, P. Secure weighted possibilistic c-means algorithm on cloud for clustering big data. *Inf. Sci.* **479**, 515–525 (2019).
13. Sivaram, M. *et al.* Secure storage allocation scheme using fuzzy based heuristic algorithm for cloud. *J. Ambient Intell. Humaniz. Comput.* **12**, 5609–5617 (2020).
14. Haber, S. & Stornetta, W. S. How to time-stamp a digital document. *J. Cryptol.* **3**, 99–111 (1990).
15. Mahajan, P. & Sachdeva, A. A study of encryption algorithms AES, DES and RSA for security. *Glob. J. Comput. Sci. Technol.* **13**, 15–22 (2013).
16. Mandal, A. K., Parakash, C. & Tiwari, A. Performance evaluation of cryptographic algorithms: DES and AES. In *Proceedings of the IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India* 1–5 (2012).
17. Balasamy, K., Krishnaraj, N. & Vijayalakshmi, K. Improving the security of medical image through neuro-fuzzy based ROI selection for reliable transmission. *Multimed. Tools Appl.* **81**(10), 14321–14337 (2022).
18. Kanwal, S., Inam, S., Ali, R. & Cheikhrouhou, O. Lightweight noncommutative key exchange protocol for IoT environments. *Front. Environ. Sci.* **10**, 996296 (2022).
19. Hasan, M. R. *et al.* The applicability of blockchain technology in healthcare contexts to contain COVID-19 challenges. *Libr. Hi Tech* **39**(3), 814–833 (2021).
20. Neela, K. L. & Kavitha, V. Blockchain based chaotic deep GAN encryption scheme for securing medical images in a cloud environment. *Appl. Intell.* **53**(4), 4733–4747 (2022).
21. Mondal, A. & Goswami, R. T. Enhanced honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security. *Microprocess. Microsyst.* **81**, 103719 (2020).
22. Pradeep, G., Bala, S., Satheesh, N. P., Mahalakshmi, M., Balasamy, K. & Suganyadevi, S. An effective framework for detecting epileptic seizures using CNN and encrypted EEG signals. In *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)* 611–617 (IEEE, 2023).
23. Ali, T. S. & Ali, R. A novel medical image signcryption scheme using TLTS and Henon chaotic map. *IEEE Access* **8**, 71974–71992 (2020).
24. Padhy, R. P., Patra, M. R. & Satapathy, S. C. Design and implementation of a cloud based rural healthcare information system model. *Univ. J. Appl. Comput. Sci. Technol.* **2**(1), 149–157 (2012).
25. Lakshmi, C. *et al.* Neural-assisted imagedependent encryption scheme for medical image cloud storage. *Neural Comput. Appl.* **33**, 6671–6684 (2020).
26. Sharma, P. K., Moon, S. Y. & Park, J. H. Block-VN: A distributed blockchain based vehicular network architecture in smart city. *J. Inf. Process. Syst.* **13**(1), 84 (2017).
27. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K. & Njilla, L. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing* 468–477 (IEEE Press, 2017).
28. Afzal, I., Parah, S. A., Hurrah, N. N. & Song, O. Y. Secure patient data transmission on resource constrained platform. *Multimed. Tools Appl.* **83**, 15001–15026 (2020).
29. Jolfaei, A. & Mirghadri, A. A novel image encryption scheme using pixel shuffler and A5/1. In *Proceedings of the 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI10)*, Sanya, China (2010).
30. Hosny, K. M., Kamal, S. T. & Darwish, M. M. A color image encryption technique using block scrambling and chaos. *Multimed. Tools Appl.* **81**, 505–525 (2022).
31. Kanwal, S. *et al.* An effective color image encryption based on Henon map, tent chaotic map, and orthogonal matrices. *Sensors* **22**(12), 4359 (2022).
32. Kanwal, S. *et al.* A new image encryption technique based on sine map, chaotic tent map, and circulant matrices. *Secur. Commun. Netw.* <https://doi.org/10.1155/2022/4152683> (2022).
33. Inam, S., Kanwal, S., Zahid, A. & Abid, M. A novel public key cryptosystem and digital signatures. *Eur. J. Eng. Sci. Technol.* **3**(1), 22–30 (2020).
34. Menze, B. H. *et al.* The multimodal brain tumor image segmentation benchmark (BRATS). *IEEE Trans. Med. Imaging* **34**(10), 1993–2024 (2014).
35. www.kaggle.com/c/ultrasound-nerve-segmentation/data/?select=sample submission.csv
36. Jaeger, S. *et al.* Two public chest X-ray datasets for computer-aided screening of pulmonary diseases. *Quant. Imaging Med. Surg.* **4**(6), 475–477 (2014).
37. Chidambaram, N., Raj, P., Thenmozhi, K. & Amirtharajan, R. Advanced framework for highly secure and cloud-based storage of colour images. *IET Image Process.* **14**, 3143–3153 (2020).
38. Kanwal, S. *et al.* Analytic study of a novel color image encryption method based on the chaos system and color codes. *Complexity* **2021**, 1–19 (2021).
39. Hosny, K. M., Kamal, S. T. & Darwish, M. M. Novel encryption for color images using fractional-order hyperchaotic system. *J. Ambient Intell. Humaniz. Comput.* **13**(2), 973–988 (2022).
40. Masood, F. *et al.* A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. *Wirel. Pers. Commun.* **127**(2), 1405–1432 (2021).
41. Shen, M., Deng, Y., Zhu, L., Du, X. & Guizani, N. Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach. *IEEE Network* **33**(5), 27–33 (2019).
42. Banu, S. A. & Amirtharajan, R. A robust medical image encryption in dual domain: Chaos-DNA-IWT combined approach. *Med. Biol. Eng. Comput.* **58**(7), 1445–1458 (2020).
43. Enab, M. *Image Encryption of Internet of Medical Things Privacy using AES* (2022).
44. Sowmiya, L., Rajasekaran, A. S., Suganyadevi, S., Sureshkumar, S., Subramaniam, G. & Jaazieliah, R. A secure authenticated message transfer in healthcare application. In *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)* 1–6 (IEEE, 2023).

Author contributions

1. Conceptualization, Methodology & Formal analysis: S.I. & S.K. 2. Supervision: S.I. 3. Writing original draft: R.F. 4. Review & editing: F.H.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to S.I.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2024