Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2024.00057

Research Article

A secure framework for multimedia transmission in medical images using DNA cryptography

Malathy N[1,*], Navin G[1], Sriram S[1], Bala Subramaniyan S[1]

[1]*Department of Information Technology, Mepco Schlenk Engineering College, Sivkasi, 626005, India*

ARTICLE INFO

Article history
Received: 05 July 2023
Revised: 23 September 2023
Accepted: 05 March 2024

Keywords:
DNA Cryptography; Elephant Heard Optimization; Encryption; Lorentz Map; Multimedia Transmission; Medical Images; Steganography

ABSTRACT

Images created by smart cameras and sensors are greatly at risk when transmitted over a public network because of the dynamic and open nature of the medical imaging ecosystem. Encryption is an effective method for safeguarding medical digital images. This article discusses a framework for image security that employs DNA cryptography and DNA steganography. The key is Generated using logistics and Lorentz map and uses the Elephant Heard Optimization Algorithm for optimization for the generated key. This key is utilized to do Row and Column rotation using the Rubik's cube algorithm. We next select the DNA encoding-decoding rule and carry out the DNA XOR operation. Finally, we carry out DNA Steganography using the four-phase method. The proposed scheme's average NPCR (99.6566%), UACI (33.4588%), Entropy (7.98), and long key value of 10135are superior to those of the existing schemes and more resistant to various attacks, according to the result analysis.

Cite this article as: Malathy N, Navin G, Sriram S, Bala Subramaniyan S. A secure framework for multimedia transmission in medical images using DNA cryptography. Sigma J Eng Nat Sci 2025;43(1):222–233.

INTRODUCTION

A multimedia security framework is a crucial tool for preventing unauthorized access to and exploitation of digital media. This framework combines DNA cryptography, steganography, and chaotic maps to offer a stable environment for multimedia data. A safe platform for multimedia data is provided by chaotic maps, which convert a picture into a chaotic map that is challenging to decipher. The use of steganography, on the other hand, makes it challenging for an intrusive party to ascertain whether a hidden message is present within a multimedia file. Data is encrypted and decrypted using DNA strands utilizing DNA cryptography, guaranteeing that the information is secure and private. The framework is made to give multimedia data a secure and dependable environment while ensuring that unauthorized access is avoided. The framework also offers a secure environment for data transfer and storage because data is encrypted and kept securely.

DNA steganography is a type of steganography that conceals information in the coding of DNA strands. This method involves encoding and embedding messages in strands of DNA that are difficult to detect. DNA steganography is used to hide data, images, audio, and other types of information in the DNA code of a living organism or a

***Corresponding author.**
*E-mail address: malathy@mepcoeng.ac.in

This paper was recommended for publication in revised form by Editor-in-Chief Ahmet Selim Dalkilic

DNA sample extracted from a living organism. The data is encrypted and then embedded in the sequence of the four nucleotides of the DNA. Mathematical operations called chaotic maps are used to encrypt digital data. These operations generate unpredictable, chaotic outputs, which make them a good option for secure data storage. Chaotic maps and encryption techniques are employed to safeguard multimedia data against unauthorized access. Steganography is the art of concealing confidential information or messages within other digital media, such as photos, audio files, and movies. Sensitive information is concealed using this method so that it is difficult for an unauthorized user to find it.

Using DNA cryptography, it is possible to store digital information inside DNA strands. This method is based on the fact that DNA molecules can fit a lot of information into a tiny amount of space. Since the information is encoded into DNA molecules, unauthorized access to it is essentially impossible. This multimedia security framework is made to give digital multimedia material secure storage. It consists of several security measures used in tandem to guard against the unauthorizedness and manipulation of data. The framework combines DNA cryptography, steganography, and chaotic maps to produce an impenetrable barrier for safeguarding digital multimedia data.

The framework also offers sophisticated capabilities that can be used to spot any unauthorized data modification, like data authentication and verification. An innovative security system called the Multimedia Security Framework was created to safeguard digital multimedia assets against unauthorized access and manipulation. It builds an impenetrable wall for safeguarding digital data by fusing chaotic maps, steganography, and DNA cryptography. The framework offers a safe and dependable environment for storing digital content and is simple to deploy.

The medical imaging ecosystem is dynamic and open, images produced by smart cameras and sensors are highly vulnerable when shared over a public network. Encryption is a reliable technique to protect digital medical images. However, encryption alone is not sufficient to transfer the data in a secured manner.DNA Cryptography and steganography is a recent trend used for secure data transmission. Together with that logistic and chaotic key generation along with Elephant Heard optimization techniques to generate a secured key made the Medical image transmission very safe and secure

Related Works

The model combines two potent encryption methods, chaos, and DNA cryptography, to offer a high level of security for medical images. As a result, it is challenging for hackers to access the photographs and defeat the encryption. The model is quite adaptable and may be used with many medical photos [1]. Because of this, it can be used in industrial applications where a lot of images are produced and saved [2]. The encryption process must be quick and effective. Without affecting the security of the photos, the model can quickly encrypt and decode photographs. As the system generates encryption keys using chaotic maps, it offers a high level of protection for medical images [3]. Chaotic maps make it harder for attackers to compromise the encryption since they are highly unpredictable and sensitive to starting conditions.

The encrypted and decrypted times of the methods are quick, making them appropriate for real-time applications [4]. This is crucial for time-sensitive medical imaging applications, such as emergency medical services. The approach has a low computational overhead, therefore encrypting and decrypting images only need a small amount of CPU power [5]. This qualifies it for deployment on devices with constrained resources, like smartphones or tablets. The system is robust to various attacks including statistical, differential, and brute-force attacks. This makes sure that even in the face of sophisticated attackers, the encrypted medical photos are secure. HIPAA and GDPR are only two examples of the several data protection laws that the plan complies with. This qualifies it for usage in settings like hospitals where following rules is crucial [6]. The device is simple to integrate into current medical imaging systems, making it an affordable option for medical image protection. The method provides a high level of security for medical photos, ensuring that they cannot be accessed or interfered with by unauthorized. Since the scheme's encryption keys are generated using a safe process, it is challenging for attackers to circumvent the encryption. The approach has a low computational overhead, therefore encrypting and decrypting images only need a small amount of CPU power [5].

DNA strands are employed in DNA cryptography to provide a special key that can be used to encrypt and decrypt multimedia data. Specifically, the binary bits created from the DNA strands are employed as a key for encryption and decryption. Furthermore, the key is challenging to guess because it is created using DNA strands, making it a safe method of data transmission.DNA steganography, on the other hand, is a method that uses DNA strands to conceal data within multimedia information. The audiovisual content is subsequently encoded with the binary bits created from the DNA strands. Using this method, sensitive information can be masked in multimedia data that is sent through the Internet of Things. Furthermore, because it is included within the multimedia material, it is challenging to spot the embedded data. As embedded data may be used to detect any unauthorized access or data tampering, this technology is also utilized to detect any harmful behavior in the medical image.

Additionally, the employment of logistics and Lorentz maps in DNA steganography adds another level of security to the transmission of multimedia in the medical image. Mathematical operations like the Lorentz map and logistics are employed to produce random numbers. The embedded data is then encrypted and decrypted using the key provided by this random collection of integers. The random

sequence can be used to identify any malicious medical actions, adding an extra degree of security to the data. In conclusion, a safe framework for multimedia transmission in the Internet of Things is provided by the employment of DNA cryptography and steganography along with logistic and Lorentz maps. With the help of this framework, the data is protected against unauthorized access and manipulation. Additionally, this framework adds an extra layer of security by encrypting and decrypting data using random integers. As a result, this framework offers a solid answer to the medical's need for secure multimedia data transmission. It has been investigated in the past how to employ DNA cryptography and steganography for safe data storage and communication. The authors in [7] discusses the various encryption technique adopted for medical image encryption. In [8] the authors proposed five-dimensional multi-band multi-wing chaotic system for medical image encryption.

As embedded data may be used to detect any unauthorized access or data tampering, this technology is also utilized to detect any harmful behavior in the Untraditionally, the employment of logistic and Lorentz maps in DNA steganography adds another level of security to the transmission of multimedia in the Internet of Things. The random sequence can be used to identify any malicious IoT actions, adding an extra degree of security to the data. In conclusion, a safe framework for multimedia transmission in the Internet of Things is provided by the employment of DNA cryptography and steganography along with logistic and Lorentz maps. With the help of this framework, the data is protected against unauthorized access and manipulation. Additionally, this framework adds an extra layer of security by encrypting and decrypting data using random integers. As a result, this framework offers a solid answer to the IoT's need for secure multimedia data transmission. The major contribution of this article is

1. Secured and optimized key generation by combining Lorentz, logistics map, and Elephant Heard optimization algorithm.
2. Encrypt and Decrypt the medical images using a Rubik's cube and DNA steganography mechanism.
3. The proposed system is evaluated with various attacks and measured with various parameters like NPCR, UACI, MSE, PSNR, and MAE.

MATERIALS AND METHODS

Materials

A. Chaotic maps

A chaotic map is a type of mathematical function that uses chaotic behavior, meaning that it is highly sensitive to initial conditions and can produce unpredictable and seemingly random outputs over time. Chaotic maps have found applications in various fields, including cryptography, data encryption, and image processing, because of their inherent unpredictability and complexity.

1) Logistic map: It is a non-linear discrete-time dynamical system that displays complicated behavior as the value of r changes, and is frequently used in the natural and social sciences to simulate population dynamics, ecology, and phenomena [2]. It is denoted as a mathematical expression in equations 1 to 6.

$$a_{x-1} = \alpha a_x(1 - a_x) + \beta b_x^2 a_x + \gamma c_x^3 \quad (1)$$

$$b_{x-1} = \alpha b_x(1 - b_x) + \beta c_x^2 a_x + \gamma a_x^3 \quad (2)$$

$$c_{x-1} = \alpha c_x(1 - c_x) + \beta a_x^2 a_x + \gamma b_x^3 \quad (3)$$

$$a_{x+1} = f_y = \begin{cases} \lambda a_x, & \text{if} a_p < \frac{1}{2} \\ \lambda(1 - a_x), & \text{if} a_p > \frac{1}{2} \end{cases} \quad (4)$$

$$\emptyset_{x+1} = \emptyset_x + \delta - \frac{k}{2\pi}\sin(2\pi\emptyset_x) \quad (5)$$

$$a_{x+1} = \cos(y * \arccos(a_x)) \quad (6)$$

2) **Lorentz maps**: A two-dimensional dynamical system called the Lorenz map is used to simulate the behavior of chaotic systems. It is a discrete-time map that iterates through one location in the plane to a new point set of parameters. A variety of chaotic behaviors are shown on the map, which can be utilized to comprehend intricate dynamical systems [4]. It is mathematically represented using the equation 7 – 9.

$$a = \propto (b - a) \quad (7)$$

$$b = ta - b - ac \quad (8)$$

$$c = ab - xc \quad (9)$$

The parameters are x, t, and. When selecting $\propto = 10$, t = 28, and x = 8/3, the system enters a chaotic scope. Therefore, given beginning values for x0, y0, and z0, the system will spread quickly and produce values that are significantly different from those produced by a system given only slightly different values for x0, y0, or z0.

B. Rubik's cube

The Fredrich Method, which has numerous phases, is the most widely used algorithm.

1. Cross: In this step, you must arrange the cube's top side so that each of its edge pieces lines up with the centerpiece of the opposing face.

2. F2L (First Two Layers): In this stage, each of the last few edge pieces must be paired with the appropriate corner piece from the bottom layer.
3. OLL (Orient Last Layer): In this stage, the last layer is oriented to ensure that every piece is facing the right way.
4. PLL (Permute Last Layer): In this phase, the edge and corner pieces of the last layer are switched around to make sure they are all in the right places.

C. DNA encoding and decoding rule

All living things are built and function according to genetic instructions found in DNA, a lengthy, double-stranded molecule. The nucleotide sequence, which makes up DNA's building blocks, contains these instructions. The four nucleotides that make up DNA are adenine (A), thymine (T), guanine (G), and cytosine (C) [2]. The genetic information that is passed down from one generation to the next is determined by the arrangement of these nucleotides in a DNA strand [9]. The complementary pairing of nucleotides serves as the foundation for the DNA encoding rule. A and C are always paired with T and G, respectively. As each nucleotide is paired with a complementary partner, the sequence of nucleotides on one strand of DNA determines the sequence of nucleotides on the other strand.

D. DNA XOR operation

A logical operation called the XOR operation accepts two inputs and produces a single output. The XOR technique can be used to compare the sequences of two distinct DNA strands in the context of DNA and is given in Table 1. Comparing the equivalent nucleotides in each DNA strand is the XOR process. The XOR output is 0 when the nucleotides match [10]. The XOR output is 1 when the nucleotides are not identical. For instance, the XOR operation would result in the output 1101 if the first strand had the sequence AGCT and the second strand had the sequence TCAG.

E. Elephant heard optimization for key generation phase

Elephant Herding Optimization (EHO) is a metaheuristic optimization algorithm, drawing inspiration from the herding behavior of elephants in nature [11]. Within EHO, a clan operator is employed to adjust the spacing between elephants within each clan relative to a lead matriarch elephant. Extensive comparisons have showcased EHO's outperformance against numerous state-of-the-art metaheuristic algorithms across a wide array of benchmark problems and application domains. The following assumptions are taken into account in EHO.

1. The elephant population consists of certain clans, each with a set number of elephants.
2. In every generation, a predetermined number of male elephants will depart from their family unit to live independently, distant from the primary elephant group.
3. Each clan of elephants is led by a matriarch.

Clan operator updation:

In the EHO algorithm, the positioning of each elephant in a clan is influenced by its matriarch. The formula for determining the new position of elephant p in clan cli is given by Equation (10) as follows,

$$y_{n,cli,p} = y_{cl,p} + al \times (y_{b,cli} - y_{cli,p}) \times ra \quad (10)$$

where xnew,ci,j and xci,j denote the new and old positions of the elephant, respectively. The parameter al has values in the range of [0,1] representing a scaling factor, while ra in the range of [0,1] is a randomization factor. The best elephant in the clan, denoted as xbest,ci, influences this calculation and is determined by Equation (11).

$$y_{n,cli,p} = Be \times y_{cent,cl} \quad (11)$$

The parameter Be values in the range of [0,1] in Equation (11) determines the degree of influence of the center individual xcenter,ci on the new position The center individual ycenter,cli of clan ci is calculated using Equation (12) for each dimension, where nocli is the number of elephants in clan ci. The variable d ranges from 1 to D, representing the dimensions of the problem space.

$$y_{cent,cl} = \frac{1}{no_{cli}} \times \sum_{p=1}^{n_{cli}} ycli \quad (12)$$

Separation operator:

It deals with the leaving of male elephants from the family and it is updated using equation (13)

$$y_{wor,cli,p} = y_{min} + (y_{max} - y_{min}) + 1 \times ran \quad (13)$$

F. DNA steganography

A data security technique called DNA steganography involves encoding digital information into DNA strands. As the data can only be decoded using a particular set of enzymes or methods, this technology is utilized to conceal information from prospective adversaries [12-16]. A developing technology called DNA steganography provides a safe way to transmit and store data.DNA molecules are used to store digital data during the process of DNA steganography. The four nucleotides that make up DNA serve as the genetic code's building blocks.

Table 1. DNA XOR operation rules

XOR	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	G
T	T	G	C	A

A DNA strand can be made to carry information by changing the order of these nucleotides. Then, without being seen by customary security measures, this encoded data can be kept and transmitted. When employing DNA steganography, the information is encrypted and then coded into DNA strands. The encrypted data can then be transferred to someone else or saved for later use. The recipient must possess the same set of enzymes or encoding methods as those used to encode the data to decode it. In comparison to more conventional data security measures, DNA steganography has several benefits. The data is kept in a manner that is hard to find, making it considerably more secure. The data is also a lot less than it would be using conventional data security techniques, which makes it simpler to store and send. Finally, DNA steganography is far more secure than other data security techniques since it is harder to reverse engineer.

Security Framework for Medical Images

Figure 1 shows the overall proposed system. A set of rules, regulations, and procedures called a suggested security framework for medical images are intended to guarantee the secure and reliable transmission, storage, and processing of digital photographs in industrial settings. To defend against a variety of threats and attacks, such as data breaches, unauthorized access, and cyber-attacks, the framework typically includes a set of security controls and measures, such as access controls, authentication mechanisms, encryption protocols, and network security mechanisms. Access restrictions limit authorized people and devices' access to medical photos. confirming users' identities and making sure they have the right permissions to access and modify photos.utilizing powerful encryption methods to secure medical photos during transport and storage.

Phase 1: Key Generation Phase

The process known as Lorentz Map Key Generation, which is based on the Lorentz Attractor, is used to produce random numbers. In its iterations, this algorithm uses chaotic behavior to produce unpredictable and robust cryptographic keys. Three nonlinear differential equations make up the Lorentz Attractor, which results in complicated and chaotic behavior and is given in Equations 14-16.

$$a_0 = \mathrm{mod}(a, 1) \tag{14}$$

$$b_0 = \mathrm{mod}(b, 1) \tag{15}$$

$$c_0 = \mathrm{mod}(c, 1) \tag{16}$$

The seed, the initial value generated by this process, is used to loop over the system of equations until a stable value is attained. The cryptographic key is then created using this steady value. Logistic Map Key Generation is an algorithm that creates random numbers using the Logistic Map as a basis and it is mathematically represented in equations 17-19. The generated Key is then optimized using Elephant Heard Optimization.

$$a_x = \mathrm{mod}\big((a_x * T), 8\big) \tag{17}$$

$$b_x = \mathrm{mod}\big((b_x * T), 8\big) \tag{18}$$

$$c_x = \mathrm{mod}((c_x * T), \mathrm{ImageHeight}) \tag{19}$$

Phase 2: Encryption Phase

Chaotic behavior to produce unpredictable and robust cryptographic keys. A single nonlinear differential equation system called the logistic map generates complicated and unpredictable behavior. The seed, the initial value generated by this process, is used to loop over the system of equations until a stable value is attained. The cryptographic key is then created using this steady value. The Lorentz Map is a condensed variant that results in chaotic behavior with fewer iterations than the Logistic Map. A combination of symmetric and asymmetric cryptography is used in the encryption phase of a multimedia security framework for the Lorentz map, Logistic map, Steganography, DNA Cryptography, and Rubik's Cube algorithm. First, the message is broken up into smaller data blocks and encrypted using an AES-compatible symmetric encryption technique. This is accomplished by creating a random key for every block and using the created keys to encrypt the blocks and it is given in equation 20.

$$\mathrm{Bimage}(x,(16y)) = \mathrm{dec2bin}(\mathrm{Image}(x,y)) \tag{20}$$

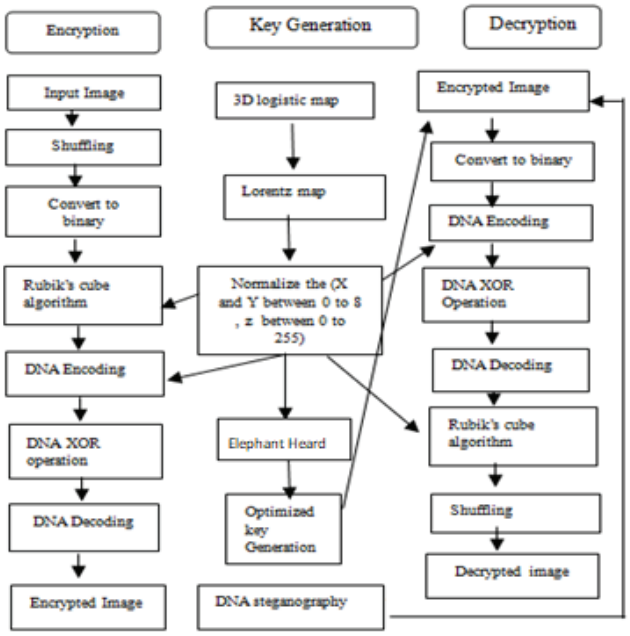


Figure. 1. Block diagram.

1	2	3	4
5	6	6	7
9	10	11	12
13	14	15	16

⇨

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Figure 2. Shuffling of pixels

The key is then encrypted using an asymmetric encryption technique, like RSA, as the following step. This is accomplished by encrypting the key with a public key and decrypting it with a private key. After that, a digital signature is added to the encrypted blocks and encrypted keys before they are merged and delivered over the network. Finally, a mixture of the Lorentz map, Logistic map, Steganography, DNA Cryptography, and Rubik's Cube method is used to encrypt the multimedia file.

Figure 2 shows the shuffling of pixels. The multimedia file is encrypted using a random number sequence produced by the Lorentz map. The file is further encrypted using a chaotic string of numbers that are produced by the logistic map. The encrypted data is. then inserted into the multimedia file using steganography, and a unique DNA sequence is created using DNA cryptography. Finally, the data is scrambled and rendered illegible using the Rubik's Cube algorithm. This multimedia security framework's encryption phase makes sure that all data is securely encrypted, making it challenging for an adversary to decode. They would still require the keys and the digital signature to unlock the encrypted data, even if they were to get their hands on it and it is denoted in equation 21.

$$\text{Image}(x,y)=\text{bin2dec}(\text{Bimage}(x,(16ay))) \quad (21)$$

Phase 3. Decryption Phase

The unencrypt ion of the encrypted multimedia data can start the decryption phase for a multimedia security framework based on the Lorentz map, Logistic map, steganography, DNA cryptography, and Rubik's cube algorithms. To do this, the data must first be decrypted using the Lorentz map and Logistic map algorithms, which restore the data's original form from the encrypted state. Then, any concealed data that is included in the multimedia data can be extracted using the steganography algorithm. After that, the data can be decrypted using the encrypted key and the DNA cryptography algorithm.

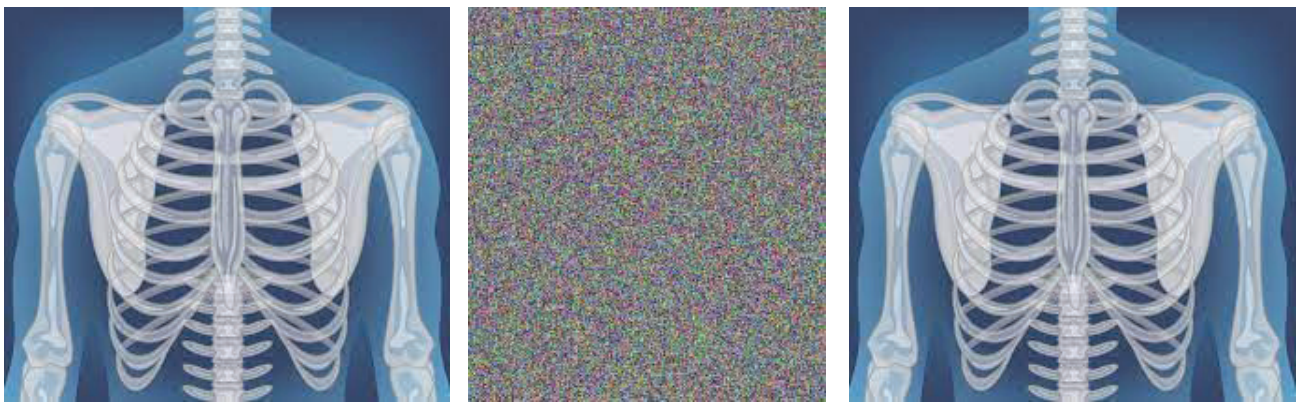
The DNA sequence of the encrypted data is used by this approach to generate a special key that may be used to decrypt the data. Finally, the encrypted data can be decrypted using the Rubik's cube algorithm. To decrypt the data, this technique alters the state of a Rubik's cube. The integrity and validity of the multimedia data can be checked once all the methods have been applied to decode it. This can be achieved by verifying that the decrypted data matches the original by comparing it to the original unencrypted data. Finally, users can use the decrypted data it is given in Figures 3 and 4.

1	3	2	4
9	11	10	12
5	7	6	8
13	15	14	16

⇨

1	3	2	4
9	11	10	12
5	7	6	8
13	15	14	16

Figure 3. Shuffling back of pixels.



(a) (b) (c)

Figure 4. Original image (a), encrypted Image (b), decrypted Image (c).

RESULTS AND DISCUSSION

This section looks at how the experiment's findings and conclusions were interpreted. The proposed model is subjected to numerous analyses to determine how resistant and covert it is to various attacks. Correlation coefficient (CC), information entropy, and histogram analysis are performed to assess the proposed model's resistance against statistical attacks. The number of pixels change rate (NPCR) and unified average changed intensity (UACI) tests are carried out to assess resistance to differential attacks. Keyspace analysis is used to evaluate stability against brute-force attacks. The experiment was carried out using an Intel Core i3 computer with 8 GB of RAM and a 2.10 GHz processor. The MATLAB (R2018a) program is used to analyze 100 256x256 pixel images.

A. Statistical Attack Analysis

In a statistical attack, an attacker analyses a set of data or cryptographic material using statistical methods to find flaws or concealed information [17,18]. This can entail looking for statistical abnormalities that can point to a flaw in the encryption system, analyzing patterns in the data, or examining relationships between various variables. A known plaintext attack is an illustration of a statistical assault; in this scenario, the attacker has access to both the plaintext and the ciphertext of a communication and utilizes statistical analysis to determine the encryption key or algorithm.

1) Correlation coefficient analysis: A statistical method for determining the degree and direction of the linear link between two variables is correlation links in huge datasets is a typical task in data analysis and research. If two variables have a perfect positive correlation they move at the same rate and in the same direction. They move at the same speed in opposite directions when the correlation coefficient is exactly negative one, There is no association between the two variables, as indicated by a correlation coefficient of 0. It is given in Figure 5 by applying the equation 22 - 24.

$$\Omega_{xy} = \frac{con(x,y)}{\sqrt{T(x)T(y)}} \tag{22}$$

$$\mathrm{Cov(x,y)} = \frac{1}{I}\sum_{k=1}^{I}(x_j - \mathrm{Z(x)})(y_j - \mathrm{Z(y)}) \tag{23}$$

$$\mathrm{T(x)} = \frac{1}{I}\sum_{j=1}^{I} x_j - \mathrm{Z}(x))^2 \tag{24}$$

Where x and y stand for the pixel's intensity levels. I is a representation of all available pixels. Expectation, variance, and covariance are each represented by Z(x), T(x), and cov(x,y), respectively. The correlation plots for the original, cipher, and decrypted images are displayed in the horizontal, vertical, and diagonal directions, respectively. Table 3 also displays the correlation coefficients (CC) for all three directions. Table 3 and Figures 7-9 map makes clear that the CC for cipher pictures is close to zero, making the proposed technique resistant to statistical attacks.

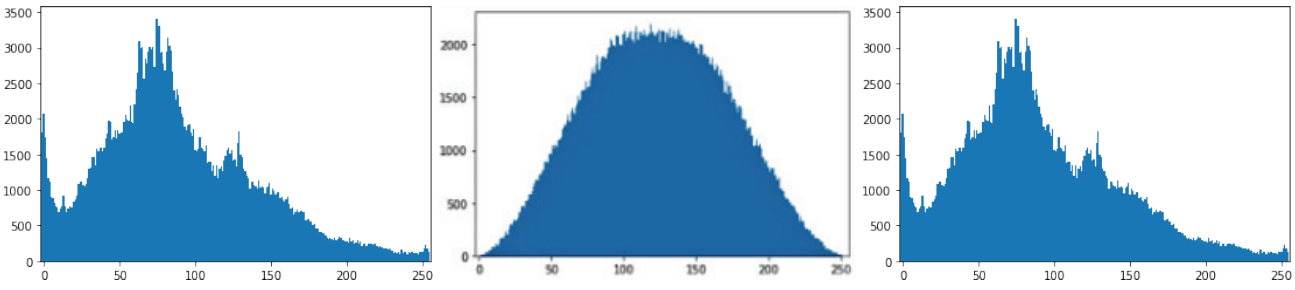
2) Information entropy: The level of uncertainty or randomness in a set of data or information is measured by information entropy [19]. Quantifying the amount of information in a message or signal is a widespread practice in information theory, computer science, and other disciplines. Entropy is frequently used to calculate the bare minimum of bits needed to represent a set of symbols or messages in the context of information theory. A message's entropy, for instance, would be 1 bit if it had two symbols, each of which had a probability of 0.5. This is because only one bit is needed to encode the message and it is given in equation 25.

$$\mathrm{IE} = \sum_{j=1}^{I} F(x_i)\log_2 \frac{1}{F(x_i)} \tag{25}$$

Where F (x_i) is the probability of the xi data and L is the total number of distinct data points. Table 2 lists the IE of

Table 2. Information entropy of image

Sample Image	Entropy value	
	Original Image	Encrypted image
Sample Image 1	5.4431	7.4678
Sample Image 2	5.2342	7.3526
Sample Image 3	5.0785	7.9994
Sample Image 4	4.9999	7.6573
Sample Image 5	5.8657	7.1427
Average	5.3242	7.5239



(a) (b) (c)

Figure 5. Original image (a), ciphered image (b), deciphered image (c).

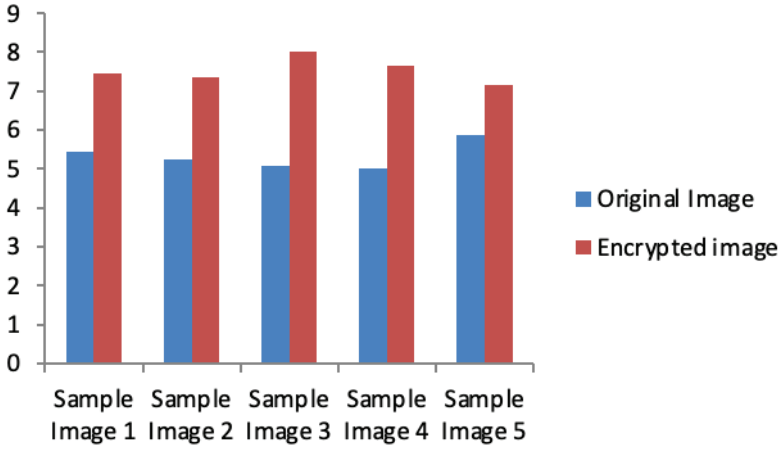


Figure 6. Information entropy of image.

cipher images using the suggested technique and is represented in Figure 6. Table 4 shows that the IE value for the cipher image is close to eight, making the proposed technique resistant to statistical attacks.

B. Histogram Analysis

The intensity of pixels in the cipher image must be distributed uniformly for the cryptosystem to function properly [20]. In this investigation, a histogram graph is used to plot the pixel intensity. It is evident from the original image's pixel intensity is dispersed unevenly. It can be seen from the pixel arrangement is equally dispersed and completely different from the original configuration. Additionally, it can be shown that the intensity of the pixel distribution is the same as it was in the original image. It follows that the proposed approach can fend off statistical attacks.

a) Differential attack analysis

To learn more about the encryption technique or the plaintext, a sort of cryptanalysis called differential attack analysis compares differences between pairs of related ciphertexts. Block ciphers and other symmetric encryption techniques are frequently put to the test using differential attacks [21-24].

2) NPCR and UACI analysis

NPCR calculates the proportion of pixels in the ciphertext picture that are altered when a single pixel in the plaintext image is altered. The average variation between corresponding pixels in the plaintext and ciphertext pictures is measured by UACI using equations 26- 27.

$$\text{NPCR}=\frac{\sum_{x,y} S(x,y)}{MXN} \text{ X } 100\% \tag{26}$$

$$\text{UACI}=\frac{\sum_{x,y} |C1(x,y)-C2(x,y)|}{MXNXMx} \text{X}100\% \tag{27}$$

Where M, N, and Mx stand for the industrial image's pixel's length, breadth, and maximum intensity, respectively. The encrypted image $A_1(x,y)$ is the original, and $A_2(x,y)$ is the encrypted image created by changing the intensity value in the original image. Additionally, the following is how L(x,y)is defined using equation 28.

$$L(x,y) = \begin{cases} 0, if\ A_1(x,y) = A_2(x,y) \\ 1, if A_1(x,y) \neq A_2(x,y) \end{cases} \tag{28}$$

It is clear from Table 3's NPCR and UACI results for the six test images that the anticipated algorithm can fend off differential attacks as given in Figure 7.

c) Exhaustive attack analysis

In exhaustive attack analysis, commonly called brute force, all potential keys or passwords are tested until the right one is discovered [25,26]. It is a basic and direct technique for attacking cryptographic systems and is frequently used when there are no known flaws or when other approaches have failed.

1) Key space analysis

By counting the number of potential keys that the encryption algorithm can generate, key space analysis is a technique for assessing the strength of a cryptographic key. The encryption algorithm is thought to be more secure the

Table 3. NPCR and UACI values

Sample image	NPCR value (%)	UACI value (%)
Sample image 1	42.4287	37.5432
Sample image 2	42.8793	37.5672
Sample image 3	42.9876	37.9877
Sample image 4	42.1344	37.1253
Sample image 5	42.9021	37.0983
Average	42.6664	37.4643

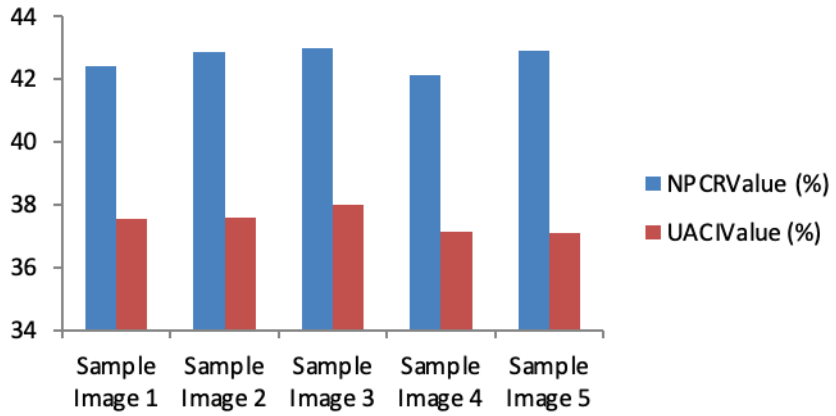


Figure 7. NPCR and UACI values.

larger the key space. The collection of all potential keys that can be used with a specific encryption algorithm is known as the key space in symmetric key cryptography. The key's size and the technique employed determine the key space. A 128-bit AES key, for instance, has a key space of 2128 potential keys.

2) Key sensitivity analysis (KSE)

A method for assessing how sensitive a cryptographic algorithm is to changes in the encryption key is called key sensitivity analysis. It is a method for figuring out how much a modest modification to the key will impact the ciphertext generated by the encryption algorithm. When evaluating the security of a cryptographic algorithm, the algorithm's sensitivity to key changes is a crucial consideration. A highly sensitive algorithm makes it more challenging for an attacker to guess the key and decrypt the ciphertext since even a tiny change in the input key will have a significant impact on the final ciphertext.

Key sensitivity study normally entails using a given key to encrypt a plaintext message, then changing that key slightly and encrypting the same plaintext message once more. To calculate their differences, the generated ciphertexts are compared. The algorithm is thought to be particularly sensitive to key changes if the difference is substantial. If there is little change, the algorithm

C. Whale-phishing attacks

Whale phishing is a specific kind of targeted phishing assault that targets senior executives and other significant individuals within a company or organization. The majority of the time, these attacks involve a highly customized email or another form of communication that is intended to look trustworthy and persuade the victim to click on a harmful link or download a corrupt attachment. These assaults are intended to steal private data or obtain access to delicate systems. If successful, whale phishing attempts can cause serious financial and reputational harm, so it's critical to be aware of them and take precautions to protect yourself.

D. Visual quality analysis

A technique for evaluating the visual quality of digital photos or videos is visual quality analysis. It entails assessing the aesthetic appeal of an image or video using a variety of approaches and metrics and contrasting it with a reference image or video to assess the degree of distortion or degradation.

1) MSE, PSNR, and MAE analysis: Three metrics that are frequently used in visual quality analysis to assess how well image or video processing algorithms perform are MSE, PSNR, and MAE.MSE calculates the average squared difference between the original and processed images' pixel values. The processed image is more comparable to the original image the lower the MSE value. The PSNR metric evaluates the relationship between the highest pixel value and the root mean squared error (RMSE) between the raw and processed images. The processed image's visual quality has improved. The MAE calculates the average absolute difference between the original and processed images' pixel values. The processed image is more comparable to the original image with the lower MAE value. Table 4 and Figure 8 show the MSE, PSNR, and MAE analysis using equation 29-31.

$$\text{MAE} = \frac{\sum M \sum N[P(i,j)-C(i,j)].}{MXN} \tag{29}$$

$$\text{MSE} = \frac{\sum M \sum N[P(i,j)-C(i,j)]^2}{MXN} \tag{30}$$

$$\text{PSNR} = 20\log_{10}\frac{(Max)}{\sqrt{MSE}} \tag{31}$$

Table 4. MSE, PSNR, and MAE of images

Sample image	MSE	PSNR	MAE
Sample image 1	1.0647	43.8782	90.7632
Sample image 2	1.0453	43.8792	90.5123
Sample image 3	1.1562	43.4231	89.9873
Sample image 4	1.5247	43.9872	90.6832
Sample image 5	1.0887	43.5461	89.6771

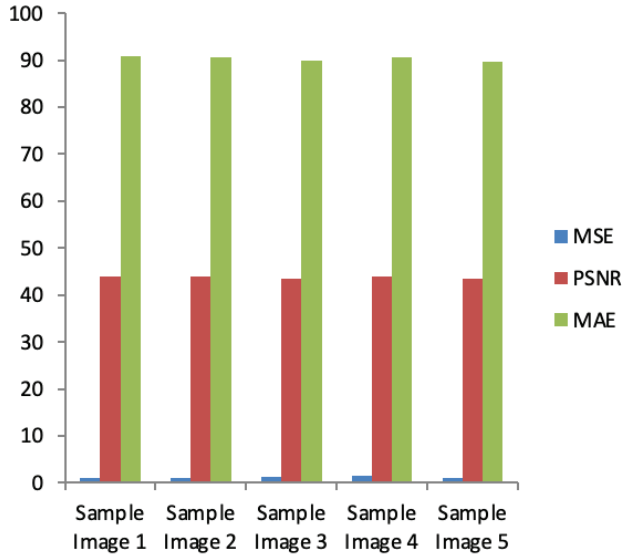


Figure 8. MSE, PSNR, and MAE of images.

E. Malware attacks

Images can be the target of a variety of malware assaults. Attacks most frequently take the form of malicious code being inserted into an image file. This code may be intended to reroute users to harmful websites or to install malicious software on a machine. Attackers can also add malicious content to already-existing photos or even build brand-new images containing dangerous content. Additionally, hackers can conceal dangerous code in image files. A malicious program, for instance, might be concealed within an image file, and the picture file itself might be used as a cover to evade detection. Steganography is another tool that attackers might employ to cloak harmful code in an image

F. MIM attack

An example of a cyberattack is a man-in-the-middle (MITM) attack, in which the attacker intercepts and modifies communication between two parties. An attacker can take, change, and manipulate images before they are conveyed to the intended recipient in the case of photographs. The attacker has further control over the images the recipient sees, allowing them to monitor the user's actions and steal information. Images can be attacked using several different methods, including data packet manipulation, website takeover, and the introduction of malicious software. To access the user's system and maybe steal data, the attacker can also insert harmful code within the image.

G. Result comparison

It is possible to compare the outcomes of the idiot pictures based on DNA cryptography in detail using chaotic maps. The outcomes of the encryption and decryption processes, the security levels, the processing time, and the accuracy of the findings may all be compared.DNA cryptography employing chaotic maps offers a high level of security for the encryption and decryption operations since it combines chaos theory DNA sequence encoding and encryption techniques. Table 5 and Figure 9 shows the result analysis.

Table 5. Result in comparison analysis

Metrics	Iqbal et al.	Lone et al.	Chai et al.	Our Work
Key Space	10^{135}	2^{306}	10^{53}	10^{135}
NPCR	42.768	42.987	42.879	42.4252
UACI	37.872	37.356	37.127	37.761
Entropy	7.0819	7.7628	7.2362	7.6521

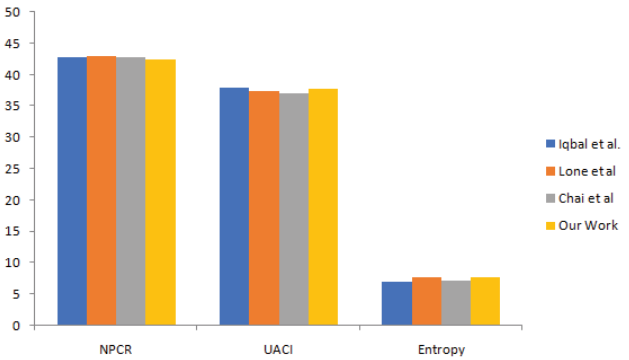


Figure 9. Result in comparison analysis.

This guarantees secure encryption and decryption of the data. Because the encryption techniques used by chaotic map cryptography are intricate and challenging to break, they offer a high level of protection.DNA cryptography utilizing a chaotic map is more efficient than other encryption techniques in terms of processing speed. It is extremely efficient because both the encryption and decryption procedures can be completed in a few seconds. Finally, when utilizing DNA cryptography with a chaotic map, the findings are similarly extremely accurate. Data is effectively safeguarded from intruders thanks to accurate and secure encryption and decryption procedures.

CONCLUSION

An efficient method of preventing unauthorized access to medical photos is provided by the proposed secure framework for multimedia transmission in medical images utilizing DNA cryptography. The solution that is being presented is based on the idea of DNA cryptography, which uses the DNA sequences of medical photos for encryption and decryption. This framework employs a modified version of the Hill Cipher algorithm for encryption and decryption. The suggested technique offers a quick and secure method of sending multimedia in medical photos. Overall, the suggested approach is an effective way to prevent unwanted access to medical photos. A DNA

cryptography model based on images has the potential to be a strong tool for safely storing and sharing data. A secure and trustworthy data storage, transport, and authentication method could all be made possible by using DNA in cryptography. Moreover, it might make data encryption and decryption less computationally intensive, opening up access to a larger range of users. Also, this technology may help to improve data privacy and security while defending data against hostile attacks. In the future, the security can be further improved with two-layer steganography mechanisms and secured and optimized key generation using hybridization of maps and other optimization algorithms. It is widely used in the medical field and uses cutting-edge methods like telemedicine, smart health, and e-health applications. This has brought attention to the problem that medical images are frequently created and distributed online, requiring security against unauthorized use.

ACKNOWLEDGEMENTS

The authors would like to thank Mepco schlenk engineering college for this support.

AUTHORSHIP CONTRIBUTIONS

Authors equally contributed to this work.

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

REFERENCES

[1] Kumar S, Sharma A, Sharma V. An Image Security Model Based on Chaos andDNA Cryptography for medical Images.IEEE2020;8:172694–172705.

[2] Ravichandran P, Praveenkumar, J, Rayappan BB, Amirtharajan R. Chaos-based crossover and mutation for securing dicom image. Comput Biol Med 2016;72:170–184. [CrossRef]

[3] Tian Y, Lu Z. Novel permutation-diffusion image encryption algorithm with chaotic dynamic s-box and DNA sequence operation. AIP Adv 2017;7:085008. [CrossRef]

[4] Ahmad MA, Bhutto MA. An Image Security Model Based on Chaos and DNA Cryptography for medical Images.IEEE2020;8:131918–131930.

[5] Huo D, Zhou DF, Yuan S, Yi S, Zhang L, Zhou X. Image encryption using exclusive-or with DNA complementary rules and double random phase encoding. Phys Lett A2019;383:915–922. [CrossRef]

[6] Khade PN, Narnaware M. 3D chaotic functions for image encryption. Int J Comput Sci2012;9:323–328.

[7] Pankaj S, Dua M. Chaos based medical ımage encryption techniques: A comprehensive review and analysis. Inform Secur J 2024;33:332–358. [CrossRef]

[8] Zhuang Z, Zhuang Z, Wang T.Medical image encryption algorithm based on a new five-dimensional multi-band multi-wing chaotic system and QR decomposition. Sci Rep 2024;14:402. [CrossRef]

[9] Zhang LB, Zhu ZL, Yang BQ, Liu WY, Zhu HF, Zou MY. Cryptanalysis and improvement of an efficient and secure medical image protection scheme. Math Problems Eng 2015;2015:1–11. [CrossRef]

[10] Ravichandran D, Praveenkumar PJ, Rayappan BB, Amirtharajan R. DNA chaos blend to secure medical privacy. IEEE Trans. Nanobiosci 2017;16:850–858. [CrossRef]

[11] Wu TY, Fan X, Wang K-H, Lai C-F, Xiong N, Wu JM. DNA computation-based image encryption scheme for cloud CCTV systems. IEEE 2023;7:181434–181443. [CrossRef]

[12] Mohammed A, Hussein M, Ali M. An image security model based on chaos and DNA cryptography for medical images.Sensors2021;21:461.

[13] Ozturk A, Aydin A, Cetin O. An image security model based on chaos and DNA cryptography for medical images.Int J Electric Comput Eng 2020;10:1025–1033.

[14] Fu C, Meng W, Zhan Y, Zhu Z, Lau FCM, Tse CK, et al. An efficient and secure medical image protection scheme based on chaotic maps. Comput Biol Med 2013;43:1000–1010. [CrossRef]

[15] Liu J, Ma Y, Li S, Lian J, Zhang X. A new simple chaotic system and its application in medical image encryption. Multimedia Tools Appl 2022;77:22787–22808. [CrossRef]

[16] Wang X, Shi Q. New type crisis: Hysteresis and fractal in the coupled logistic map. Chin J Appl Mech 2005;4:501–506.

[17] Dagadu JC, Li JP, Aboagye EO. Medical image encryption based on hybrid chaotic dna diffusion. Wireless Pers Commun 2019;108:591–612. [CrossRef]

[18] Iqbal N, Hanif M, Ul Rehman Z, Zohaib M. On the novel image encryption based on chaotic system and DNA computing. Multimedia Tools Appl 2022;81:8107–8137. [CrossRef]

[19] Lone PN, Singh D, Mir UH. "Image encryption using DNA coding and three-dimensional chaotic systems," Multimedia Tools Appl 2022;81:5669–5693. [CrossRef]

[20] Sheela SJ, Suresh KV, Tandur D. Secured transmission of clinical signals using hyperchaotic DNA confusion and diffusion transform. Int J Digit Crime Forensics 2019;11:43–64. [CrossRef]

[21] Chai X, Gan Z, Lu Y, Chen Y, Han D. A novel image encryption algorithm based on the chaotic system and DNA computing. Int J Modern Phys C 2017;28:1750069. [CrossRef]

[22] Zhang Q, Liu L, Wei X. Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. AEU- Int J Electron Commun 2020;68:186–192. [CrossRef]

[23] Chai X, Gan Z, Yuan K, Chen Y, Liu X. A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Comput Appl 2019;31:219–237. [CrossRef]

[24] Zhang M, Peng B, Chen Y. An efficient image encryption scheme for industrial internet-of-things devices," in Proceeding 2nd International ACM Workshop SecurityPrivacy Internet-of-Things. 2019. p. 38–43. [CrossRef]

[25] Khan PW, Byun Y. A blockchain-based secure image encryption scheme for the industrial Internet of Things. Entropy 2023;22:175–200. [CrossRef]

[26] Wang GG, Deb S, Coelho LS. Elephant herding optimization. 3rd International Symposium on Computational and Business Intelligence, 2015. [CrossRef]