International Journal of Reliable and Quality E-Healthcare
Volume 11 • Issue 4

A DNA Sequencing Medical Image Encryption System (DMIES) Using Chaos Map and Knight's Travel Map

Adithya B., Puducherry Technological University, India
Santhi G., Puducherry Technological University, India

ABSTRACT

This research aims to devise a method of encrypting medical images based on chaos map, Knight's travel map, affine transformation, and DNA cryptography to prevent attackers from accessing the data. The proposed DMIES cryptographic system performs the chaos intertwining logistic map diffusion and confusion process on chosen pixels of medical images. The DNA structure of the medical image has generated using all eight DNA encoding rules that are dependent on the pixel positions in the medical image. Knight's travel map is decomposed, which helps to prevent tampering and certification after the diffusion process. Finally, to avoid the deformity of medical data, a shear-based affine transformation is used. Compared to existing standard image encryption systems, the extensive and complete security assessment highlights the relevance and benefits of the proposed DMIES cryptosystem. The proposed DMIES can also withstand various attacks like statistical, differential, exhaustive, cropping, and noise attack.

KEYWORDS

Affine Transformation, Chaos Map, DNA Cryptography, Image Encryption, Intertwining, Knight Map, Knight Tour, Logistic Map, Medical Image Encryption

INTRODUCTION

Advanced technologies such as smart health, electronic health, and telemedicine are applied in medicine. In addition, physicians and medical consultants use open-source networks, such as cloud computing platforms to store and update personal patient information. Modern technologies like telesurgery, teleradiology, and medical data (including medical images) are vulnerable to security breaches due to the rise of telemedicine services. Public digital communication networks distribute these images (Priyanka & Maheshkar, 2017) for interpretation and diagnosis through network storage facilities. Hence, medical image security solutions must resist security attacks while preserving the diagnostic quality of encrypted images. In this case, processing medical images could result in irreparable diagnostic errors. Therefore, the images will be encrypted using the cryptographic

DOI: 10.4018/IJRQEH.308803

techniques like Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Adleman (RSA) (Lokeshwari et al., 2015). However, these approaches have not been proved to be effective due to the intrinsic features of enormous data capacity, a strong correlation between neighboring pixels, and increased redundancy (Al-Husainy, 2012; Ravichandran et al., 2015). Therefore, chaos-based methods have received much attention in recent research (Enayatifar et al., 2015; Li et al., 2015; Belazi et al., 2016; Jin & Liu, 2017).

Chaotic systems have intrinsic features like sensitivity, ergodicity, and unpredictability. In the initial environment, they exhibit unpredictable behaviour. The chaotic dynamics system is unreliable and has the appearance of noise (Sankpal & Vijaya, 2014). Therefore, the chaotic dynamics system and the cryptographic system have a close interaction. The property of topological transitivity assures the chaotic map's ergodicity and is related to the diffusion characteristics of the chaotic cryptosystem (Mao & Chen, 2005). In a cryptographic system, the sensitivity of chaos to the aspects of the beginning circumstances is employed for keys. Hence, chaotic maps are currently engaged in various image encryption methods (Askar et al., 2015; Belazi et al., 2016). However, these results are due to the poor diffusion function, vulnerability to selected attack strategies, and lack of statistical features of specific chaotic maps (Chen et al., 2004; Gao et al., 2006; Parvin et al., 2016). The use of chaos for encryption is not always reliable (Yap et al., 2015; Bechikh et al., 2015; Norouzi et al., 2017). Therefore, the primary challenge for researchers is to maintain the security and secrecy of medical images while reducing the processing time of encryption technologies.

Cryptography, steganography, and watermarking are some of the accessible image encryption techniques. These traditional approaches are insufficient to ensure a high degree of medical imaging security. For image encryption schemes, chaotic maps are combined with other algorithms such as Deoxyribonucleic Acid (DNA) coding (Wang et al., 2015; Hu et al., 2017; Li et al., 2018), cellular automata (Souyah & Faraoun, 2016; Srichavengsup & San-Um, 2016), and other forms of combination (Enayatifar et al., 2015; Tang et al, 2015; Jin & Liu, 2017) to get the use of chaotic maps.

PRELIMINARY WORKS

The chaos map, DNA sequence operations, knight's travel map, affine transform of medical image encryption methods have been discussed.

Chaos Intertwining Logistic Map

Chaos maps have developed as dynamical systems where initial conditions and control parameters were susceptible to each other. A substantial divergence will arise from minor changes in the initial conditions. Our capacity to forecast the behaviour of chaotic systems over extended periods has been severely limited due to this sensitivity. Cryptographic keys are calculated from the initial state in chaos-based encryption systems. Chaos maps can be classified as either high-dimensional maps or one-dimensional maps. One-dimensional maps frequently have only one variable and a small number of parameters. More than one variable and few parameters are referred to as high-dimensional mapping. This section examines the following definition of a complex chaotic map of intertwined logistic relationships (Sam et al., 2012). A high-dimensional map of chaos is calculated by Equation (1-3):

$$x_{n+1} = \left[\mu \times k_1 \times \left(1 - x_n\right) \times y_n + z_n\right] \bmod 1 \tag{1}$$

$$y_{n+1} = \left[\frac{\mu \times k_2 \times y_n + z_n \times 1}{\left(\left(x_{n+1}\right)^2 + 1\right)}\right] \bmod 1 \tag{2}$$

$$z_{n+1} = \left[\mu \times \left(k_3 + x_{n+1} + y_{n+1}\right) \times \sin\left(z_n\right)\right] \bmod 1 \tag{3}$$

Among them $\left|k_1\right| > 33.5, \left|k_2\right| > 37.9, \left|k_3\right| > 35.7$ are system parameters, the range of $0 < \mu < 3.999$ control parameter. The sequence distribution becomes more uniform in the intertwining logistic chaos map, and, more crucially, blank windows have been removed. In contrast, an intertwining logistic chaos map's sequence distribution is more uniform, but its action is more complicated than a standard logistic map. The pixels of the medical image have shuffled using intertwining chaotic sequence. The degree of chaos has a complicated confusion feature that is strongly dependent on the initial state. As a result, it is appropriate for providing security for medical images. With the help of DNA cryptography, the chaos map enhances the security of medical images.

Operations of DNA Sequence

The field of DNA cryptography is a relatively new form of encryption that has served to transmit, store, and compute data in a network. Using various DNA sequences, a unique DNA structure has constructed for each medical image in DNA cryptography. The four nucleotide principles that regulate the fundamental DNA structure are Thymine (T), Cytosine (C), Guanine (G), and Adenine (A) (Wang et al., 2009). The molecule consists of two chains joined by a hydrogen atom. These chains are combined to form a double helix structure.

A primary sequence consists of complementary chains, such that C is complementary to G, and T is complementary to A. Similarly, 0 and 1 are contrary in a binary form; hence, 01 and 10 are contrary, while 00 and 11 have contrasted. As a result, the nucleotide bases G, C, A, and T are represented by the numbers 10, 01, 00, and 11, respectively. This technique will generate 4! = 24 distinct encoding patterns. However, there are only eight DNA decoding and encoding rules that satisfy the contrary pair base defined in Table 1. The DNA structure of medical images has generated using these coding principles. Each medical image will obtain a unique DNA structure. In this way, the proposed DMIES guarantees high levels of security for medical images using medical image encryption.

Knight's Travel Map

The knight's travel map (Bai et al., 2013; Ghosh & Badhuri, 2017; Younus & Younus, 2019) represents a knight's movements on a chessboard. This game involves the knight visiting only one court or square per turn. If the knight returns to the same court where they started, the journey is neither closed nor open. The problem of the knight's tour has turned into a mathematical challenge, prompting new image processing and pattern-based study. In a chess game, the knight's actions are crucial for winning the

Table 1. Eight coding and decoding principles of DNA

Rule	00	01	11	10
1	A	G	T	C
2	A	C	T	G
3	G	A	C	T
4	C	A	G	T
5	G	T	C	A
6	C	T	G	A
7	T	G	A	C
8	T	C	A	G

game. The knight journey is not limited to an 8 x 8 board; it can expand to any M x N size. The size of the chessboard must be at least 5 x 5 to get the solution for knight travel. Therefore, the proposed DMIES provides permutation over the DNA-coded image to protect the logs or records of the medical images. It also raises the level of protection for medical images.

Affine Transformation

Affine transformation (Liang et al., 2016) is a sort of linear mapping that preserves the integrity of points, planes, and straight lines. A set of parallel lines remains parallel after an affine translation. It is often necessary to perform affine transformations to detect geometric distortions or deviations produced by non-ideal camera angles. In satellite imaging, for example, affine transformations vary for panoramic stitching, wide-angle lens distortion, and visual registration. The images should be converted and fused to a flat, broad coordinate system to minimize distortion. As a result, the proposed DMIES allows interactions and calculations without considering image distortion, thus minimizing security breaches.

RELATED WORKS

In the existing literature, DNA (Deoxyribonucleic acid) cryptography and chaotic systems are complex methods. These strategies are still in their early stage, so a thorough review of the literature is as follows.

Kanso & Ghebleh (2015) proposed a 2D chaotic cat map for selectively encrypting medical images. The composite image in the medical image only hides sensitive information. The 2D chaotic cat map is vulnerable to brute force attempts because of its limited key space. Anusudha et al. (2017) created a DNA masking utilizing a simple logistic map based on DNA sequence principles. A genetic algorithm is used to achieve the optimum DNA masking. Electronic patient data is contained in a DNA coding to create a digital watermark image. This technique has an extremely high computational cost. Hence, a reliable and simple calculating process is required.

Lin & Wang (2010) proposed encryption is performed using a piecewise linear memristor and a chaotic map. Wang et al. (2009) proposed multilayer encryption using DNA sequences, a pseudo-random generator, and a hyperchaotic map. However, due to multiple layers of encryption, computation requires more time. Fu et al. (2013) and Krishnamoorthi & Murali (2014) proposed cryptosystem encrypt images by using the tent map, baker map, and Lorenz system. The initial state of the chaotic map is essential because security depends on it. The system is subject to exhaustive search attacks due to a lack of key space.

According to the literature review, encryption approaches cannot resist all potential attacks and cannot guarantee high-level security with minimal processing effort. Due to DNA cryptography's unique nature and the high level of confusion property that governs a chaos map, it is essential to ensure a high standard of security. However, they take longer to compute. Therefore, lowering the processing time of medical image encryption is a significant research problem. The proposed DMIES primary goal is to minimize computing time while maintaining high security. Medical image cryptosystem employs intertwining chaos map, DNA sequence, knight's map, and affine transformation is proposed to save computing time and provide high-degree protection for medical images.

The following are the goals of the proposed DMIES: 1) The chaotic system's confusion and diffusion procedure are bid to the medical image's chosen pixels. 2) To ensure a high degree of protection, the intertwining chaotic system is randomly generated. 3) Instead of using a single DNA encoding and decoding rule, every rule is combined to create a single DNA structure. Because the pixels in each medical image determine the coding and decoding techniques, each medical image has its distinctive DNA structure. 4) Knight's map scrambling process dislocates the pixels very far from their initial positions to protect the logs of medical images. 5) The pixel location is displaced from one index to another using the affine transform to remove the artifacts of encrypted medical images.

As stated in the article, section 1 discusses the encryption techniques used for medical images. The proposed DMIES cryptosystem for medical imaging has described in Section 2. Then, section 3 contains security analyses and experimental results. Finally, the conclusion has derived in section 4.

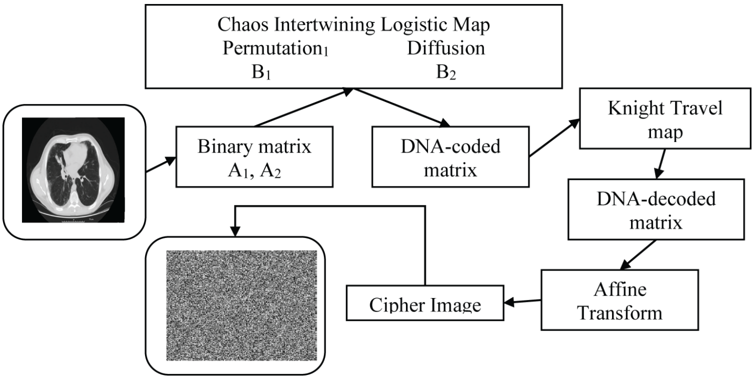
MATERIALS AND METHODS

In the proposed DMIES, figure 1 shows how the chaos map, knight's travel map, DNA operations, and affine transform provide security for medical images. First, pixels are chosen from the original medical image in the proposed DMIES using the Pixel Chosen Technique (PCT), depicted in Algorithm 1. Matrix A_1 contains the selected pixels, whereas matrix A_2 contains the remaining pixels. Both matrices are transformed to a binary image of 8 bits. Using the eight DNA base patterns, 8-bit binary images have converted to 4-bit DNA-coded matrices of B_1 and B_2. The binary image's pixel index determines which DNA encoding rules are used.

Chosen of DNA Principles

The DNA-coded matrix employs various DNA coding principles based on pixel indexes rather than using particular coding rules. The choosing of the DNA rule is calculated by Equation (4):

Figure 1. Block diagram of proposed DMIES to encrypt medical images



Algorithm 1. PCT

```
Input: Original medical image $m_i(a, b)$, where a and b denotes row and column size
Output: Matrixes $A_1$ and $A_2$ are used to store selected pixels.
        for ii = 0 to a
        do
                for jj = 0 to b
                do
                        c = $m_i$(ii, jj);
                        d = c % 3;
                        e = floor(d);
                        f = e - d;
                if (f < 0)
                then
                        $A_1$(ii,jj) = $m_i$(ii,jj);
                else
                        $A_2$(ii,jj) = $m_i$(ii,jj);
                end
        end
end
```

$$rule_n = \left(Index\left(m_i\left(ii,jj\right)\right) \bmod 8\right) + 1 \tag{4}$$

where $Index\left(m_i\left(i,j\right)\right)$ is the medical image's pixel index. If the pixel index is 151, then 151 mod 8 is 7 + 1 = 8. To convert 8-bit: 00011110 to 4-bit: TCAG, use Rule 8: 00 = T, 01 = C, 11 = A, and 10 = G. In this technique, distinct DNA rules are applied for each pixel to build a distinct DNA-coded matrix.

Permutation$_1$ Process

Pixel randomization is a chaotic system's confusion or permutation process. By disrupting the B_1 pixel of the DNA-coding matrix, the intertwining chaos map is utilized to produce a chaotic sequence. In the permutation process, the chaotic arrangements are structured to rearrange the pixels. For example, if the chaotic sequence has the indexes P_i [0 1 2 3] and P: (1.5, 0.97, 0.6, 1.3), then an ordered sequence has the indexes P_i [1 0 2 3] and P: (0.97, 1.5, 0.6, 1.3). The pixels of B_1 are shuffled using this index. The pixels of the DNA-coded matrices are scrambled in this form.

Diffusion Process

A chaotic system diffuses its values by changing its values at specific points. For example, modifying the pixel values of a DNA-coded matrix is achieved by using the DNA-XOR operation. Such as DNA-coded matrix B_1 contains the DNA sequence: T C A G, while the DNA-coded matrix B_2 has the DNA sequence: A T G C. These two sequences are merged using XOR, and the result: T C C A, which is a whole distinct sequence B_d in Equation 5:

$$B_d = bitxor\left(B_1, B_2\right) \tag{5}$$

Permutation$_2$ Process

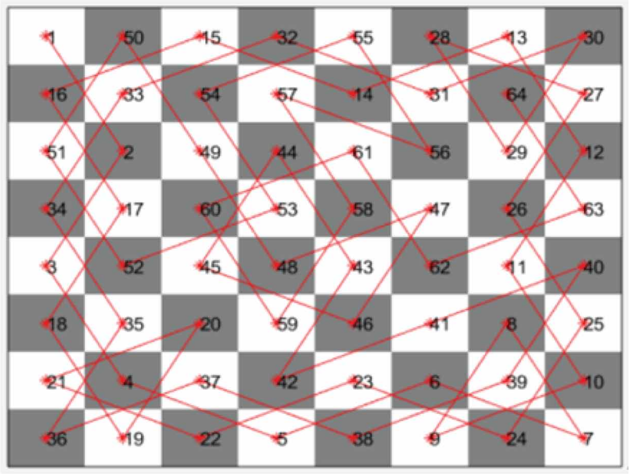
DNA-coded matrix values are dislocated from the original index using the knight's travel map or permutation$_2$ process. The only way for a knight to traverse around the board is in an L form. Because the pixels can't return to a spot, they've already visited. As a result, that pixel is displaced a long way from its original place. There are a plethora of options for the knight's sequence. There are roughly 78 different sequences for a 4 x 4 block. Similarly, there are over 1000 different scrambling sequences for 8 x 8 blocks. On an 8×8 chessboard, Figure 2 shows a pattern formed by the knight's journey. The 8 x 8 image blocks can compute Knight's sequence as *C8* is represented in Equation 6, where C is denoted as the block size:

$$C8 = \left\{ \begin{array}{cc} 0 & for\, n \le 7 \\ 6\left(7n^2 - 98n + 342\right) & otherwise \end{array} \right\} \tag{6}$$

Decoding Rules of DNA

In computing, DNA decoding converts a matrix of DNA codes into a binary image. The DNA decoding rules turn the DNA-coded matrix into a binary image after being subjected to permutation$_1$, diffusion, and permutation$_2$ processes. DNA-coded matrix pixels have decoded with the last two bits. These bits determine which decoding rules should be used (see Table 2). For instance, creating a binary medical image from a DNA-coded matrix, the two last bits extract CC from rule 7 of the matrix value ATGC.

Figure 2. 8 x 8 Knight's travelling in L form



1	50	15	32	55	28	13	30
16	33	54	57	14	31	64	27
51	2	49	44	61	56	29	12
34	17	60	53	58	47	26	63
3	52	45	48	43	62	11	40
18	35	20	59	46	41	8	25
21	4	37	42	23	6	39	10
36	19	22	5	38	9	24	7

Table 2. Decoding rules of DNA

Rule	00	01	11	10	Decoding	
1	A	G	T	C	AA	TA
2	A	C	T	G	AG	TG
3	G	A	C	T	AT	TT
4	C	A	G	T	AC	TC
5	G	T	C	A	GA	CA
6	C	T	G	A	GT	CT
7	T	G	A	C	GC	CC
8	T	C	A	G	GG	CG

Transformation Process

The proposed DMIES employs a shear-based affine transformation. From (r, s), the image is sheared to (r', s'). Geometric, scaling, reflection, and rotation are all examples of affine transformations. The pixel location is relocated from one index to another using the affine transform. DNA-decoded matrixes are sheared using the transformation process. Affinity transform can compute as A_T and *h* specify the shear factor along with the *r,s,* and *t*-axis is represented in Equation 7. Finally, a cipher image is generated by changing the binary image to a grayscale image. Algorithm 2 shows the detailed stages of the DMIES encryption for better comprehension:

$$A_T = \begin{bmatrix} 1 & h_{rs} & h_{rt} & 0 \\ h_{sr} & 1 & h_{st} & 0 \\ h_{tr} & h_{ts} & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{7}$$

Algorithm 2. Proposed DMIES

```
Input: $m_i(a, b)$ is original medical image
Output: $m_{ie}(a, b)$ is cipher image
Step 1: Start
Step 2: Divided matrices
            $A_1(a,b)$ = Selected pixels of $m_i(a, b)$ using PCT Algorithm 1;
            $A_2(a,b)$ = Remaining pixels of $m_i(a, b)$;
Step 3: Follow section 3.1 to convert the original image to binary images.
            $D_{i1}(a \times 8,b \times 8)$ = dec2bin($A_1(a,b)$);
            $D_{i2}(a \times 8,b \times 8)$ = dec2bin($A_2(a,b)$);
Step 4: Using the DNA base encoding principles given in Section 2.2, convert into
a DNA-coded matrix.
            $B_1(a \times 4, b \times 4)$ = DNA-coded Matrix of $D_{i1}(a \times 8,b \times 8)$;
            $B_2(a \times 4, b \times 4)$ = DNA-coded Matrix of $D_{i2}(a \times 8,b \times 8)$;
Step 5: Intertwining chaos maps are utilized to produce the chaotic sequences x,
y, and z given in Section 2.1.
            $x = [x_0,x_1,x_2,x_3,\ldots\ldots x_N]$;
            $y = [y_0,y_1,y_2,y_3,\ldots\ldots y_N]$;
            $z = [z_0,z_1,z_2,z_3,\ldots\ldots z_N]$;
            $\bar{x}$ = sort (x);
            $\bar{y}$ = sort (y);
            $\bar{z}$  = sort (z);
Step 6: To jumble the pixels of an image, the sorted chaos sequences index values
are x, y, and z is utilized by Section 3.2
            $B_1(a \times 4, b \times 4)$;
Step 7: Section 3.3 dealt with fusing DNA-coded matrices:
            $B_d(a \times 4, b \times 4) = B_1(a \times 4, b \times 4)$ DNA-XOR $B_2(a \times 4, b \times 4)$;
Step 8: Follow Section 3.4 to permutate DNA-coded matrix
            $C8 = 6\left(7n^2 - 98n + 342\right)$ otherwise 0 for $n \leq 7$
Step 9: Using the DNA decoding methods described in Section 3.5, convert a DNA-
coded matrix into an 8-bit binary image.
            $D_{i12}(a \times 8, b \times 8) = B_d(a \times 4, b \times 4)$;
Step 10: Shear 8-bit binary image to affine transform principle r, s, and t given
in Section 3.6
            $A_T(r, s, t) = A_T(\bar{r}, \bar{s}, \bar{t})$;
Step 11: Creating cipher image from binary image
            $m_{ie}(a, b)$= bin2dec($A_T(\bar{r}, \bar{s}, \bar{t})$);
Step 12: Stop
```

To perform the decryption strategy, the proposed DMIES is reversed. Section 2.2 describes DNA encoding principles, while Section 3.5 describes all DNA decoding rules are used in the proposed DMIES to increase security. Computational time is a significant issue in DNA cryptography. Instead of shuffling all pixels, chosen pixels are scrambled using an intertwining chaotic sequence to minimize it. Because of the intertwining chaos map's strong confusion quality and randomization (see Section 3.2, 3.3) with knight's travel (see Section 3.4) and affinity transform (see Section 3.6), attackers will have difficulty guessing the pixel sequence. As a result, the proposed DMIES provides adequate security while reducing computing time.

RESULTS AND DISCUSSION

This test has conducted on a machine with 4 GB of RAM and a processor clocked at 2.70 GHz running an Intel Core i5. Five types of 500 medical Digital Imaging and Communications in Medicine (DICOM) images (100 of each type) were evaluated, including Computerized Tomography (CT), Magnetic Resonance Imaging (MRI), ultrasound, and X-ray images, with a size of 512 × 512 pixels. The images were sourced from the Open Access Biomedical Images Search Engine of the National Library of Medicine (http://openi.nlm.nih.gov). In addition, the 256 × 256 and 512 × 512 pixels

Electrocardiogram (ECG) image has obtained from ecg_educator.blogspot.co.uk. With the help of the R2015b-Matlab tool, the proposed DMIES of encrypting medical images has been implemented. Figure 3a shows an example original medical image.

Pixels are picked from the original medical image in the proposed DMIES using PCT Algorithm 1. Matrix A_1 is used to store these pixels, whereas Matrix A_2 keeps the remaining pixels. Both matrices are transformed to a binary image of 8-bits. To get 4-bits DNA-coded matrices of B_1 and B_2, a binary image of 8-bit is encoded using all eight DNA coding patterns in Section 2.2. The initial conditions of the parameters $x_n = 1, y_n = 0.5, z_n = 0.2$, and the control parameter $\mu = 3.586$ are used to generate chaotic sequences in the intertwining chaos map. As stated previously, the sequences are sorted, and the sorted sequence index is used to encrypt the DNA-coded matrix B_1 chosen pixels. As shown in Table 3, DNA-XOR was utilized to combine the two matrices B_1 and B_2. This DNA-XORed matrix is permutated with the knight's travel map in L form traverse. Now, the traversed pixels are sheared using affine transform. After all fusion, the mid cipher image is acquired. Using all decoding DNA procedures in Section 3.5, mid cipher images are transformed into cipher images for creating final images, as illustrated in Figure 3b. Inverse encoding is used to decode the cipher image generated by the proposed encrypting DMIES. Figure 3c depicts the decrypted image.

To compute the efficacy of the proposed technique of DMIES, different attacks are used. They are statistical attacks, cropping attacks, noise attacks, exhaustive attacks, and differential attacks. A medical image's error rate is directed by the Mean Square Error (MSE), entropy, and Peak Signal-to-Noise Ratio (PSNR).

Analysis of Statistical Attacks

Using grey-level diffusion in the encrypted image, intruders attempt to anticipate the original image and secret keys in a statistical attack. A chi-square test, histogram analysis, and correlation coefficient are analyzed for verification of the statistical attack.

Histogram Analysis

It is feasible to calculate the regularity of encrypted images by evaluating the variance of the histogram. A lower variance number signifies a more uniform cipher image. Equation 8 is used to determine the variance of the histogram:

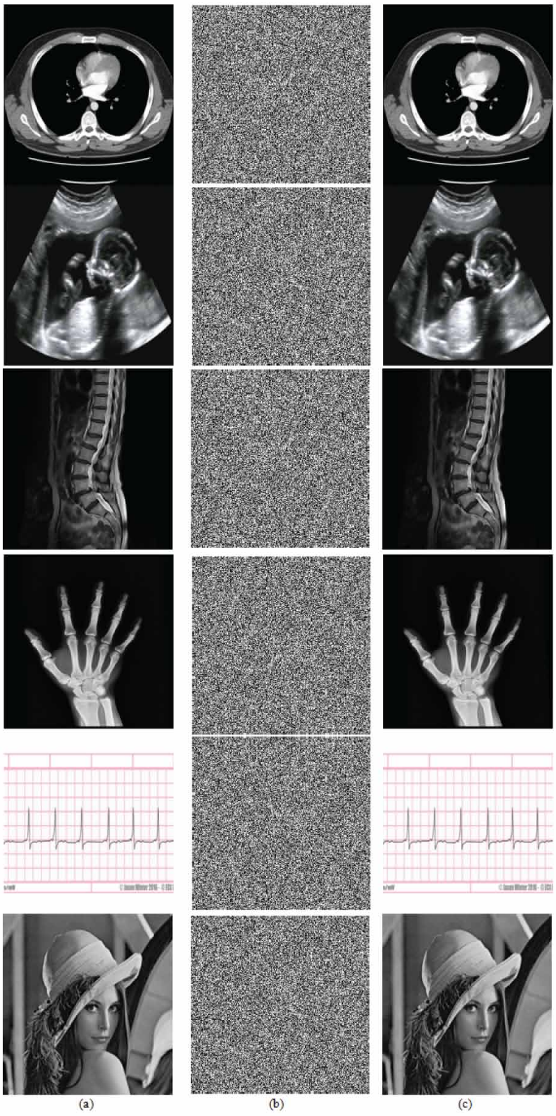
$$\mathrm{var}\left(L\right) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}\left(l_i - l_j\right)^2 \tag{8}$$

where L is the histogram value vector, with $L = l_1, l_2, \ldots, l_{256}$, where l_i and l_j are the number of pixels equal to i and j, respectively. The graphical distribution of pixels is known as histogram analysis. The pixels histogram in the original medical image is scattered irregularly can be seen in Figure 4(a,b). Figure 4c illustrates the distribution of pixels in an encrypted image. Figure 4c shows that the

Table 3. DNA-XOR

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

Figure 3. Sample of (a) Original image-[CT, Ultrasound, MRI, X-ray, ECG, Lena] (b) Encrypted image-[CT, Ultrasound, MRI, X-ray, ECG, Lena] (c) Decrypted image-[CT, Ultrasound, MRI, X-ray, ECG, Lena]

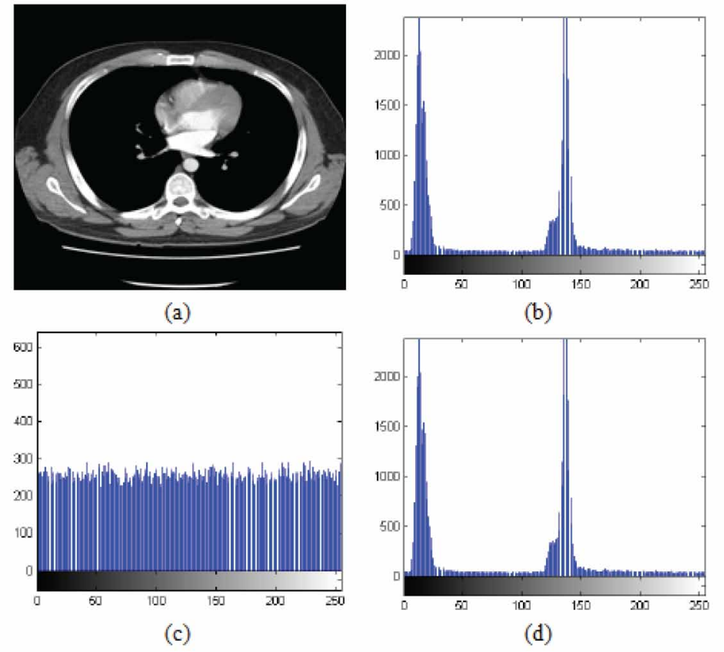


encrypted image's graphical distribution of pixels differs significantly from the original image. The decrypted medical image's histogram can be seen in Figure 4d. Based on Figure 4d, it is relatively easy to differentiate the graphical distribution of pixels between the encrypted and original images. According to these images, the proposed DMIES exhibits a consistent distribution of pixel values within the encrypted image.

Analysis of Chi-Square Test

Statistics is a method of evaluating encryption schemes based on a collection of anticipated and actual values. The pixels are equally encrypted when the chi-square value is less than the theoretical table value. Equation 9 is used to determine the chi-square parameter W^2 :

Figure 4. (a) Original image-[CT scan] and Histogram of (b) original image (c) encrypted image (d) decrypted image



$$W^2 = \sum_{0}^{255} \frac{\left(u_i - v_i\right)^2}{v_i} \tag{9}$$

The predicted and actual values are v_i and u_i, respectively, where i is the grayscale values. Table 4 shows the chi-square estimate for several test images. The calculated chi-square values for the degrees of freedom of 255 are lower than the theoretical table value. As a result, the proposed DMIES encrypted image pixels have evenly spread over the grayscale region.

Table 4. Chi-square test histogram analysis

	Size	W^2		Results
		Original image	Encrypted image	
CT-image	512 x 512	244.6436	228.9187	Pass
Ultrasound-image	512 x 512	242.8363	257.1996	Pass
MRI-image	512 x 512	262.2244	254.1319	Pass
X-ray-image	512 x 512	270.1796	250.3889	Pass
ECG-image	256 x 256	265.7355	255.1254	Pass
Lena-image	256 x 256	262.4697	252.3569	Pass

Analysis of Correlation Coefficient

To conduct the correlation study, the encrypted image and the original image of two pixels must be diagonally adjacent, horizontally adjacent, and vertically adjacent. In cryptography, the correlation coefficient has sometimes used as a measure of quality. Optimal cryptography can hide the image's original characteristics and make it appear random and uncorrelated (Elashry et al., 2007). Thus, the encrypted and original image is identical when the correlation coefficient remains one. The encrypted and the original image are entirely different if the correlation coefficient is near zero or zero (Gleick, 1987; Elashry et al., 2007; Ye, 2011). Correlation coefficient analysis is performed using the Equation (10-13):

$$E\left(op\right)=\frac{1}{n}\sum_{i=1}^{n}op_i \tag{10}$$

$$D\left(op\right)=\frac{1}{n}\sum_{i=1}^{n}\left(op_i-E\left(op\right)\right)^2 \tag{11}$$

$$co\left(op,tu\right)=\frac{1}{n}\sum_{i=1}^{n}\left(op_i-E\left(op\right)\right)\left(tu_i-E\left(tu\right)\right) \tag{12}$$

$$f_{op.tu}=\frac{co\left(op,tu\right)}{\sqrt{D\left(op\right)\times D\left(tu\right)}} \tag{13}$$

Two adjacent pixel values in the grayscale image are represented by o*p* and t*u*, where E(op) is the mean, and D(op) is the variance, co(op, tu) is the co-variance. The encrypted and original images randomly calculate the vertical, diagonal, and horizontal correlation coefficients of six thousand (6000) pairs of adjacent pixels. However, as you can see in Figure 5, the proposed DMIES effectively removes the connections between neighboring pixels, making it impossible to attack statistically.

Analysis of Information Entropy

The unpredictability and randomness of information are reflected in information entropy (Shannon, 1949). It is calculated by Equation 14:

$$H\left(O\right)=\sum_{i=0}^{2^n-1}pb\left(o_i\right)\log_2\frac{1}{pb\left(o_i\right)} \tag{14}$$

where $pb\left(o_i\right)$ is the probability of symbol o_i and *n* is the total number of symbols $o_i \in O$, will appear. It determines the encryption's unpredictability. If there are 256 different 8-bit message *O* outputs with equal probability, the message source will become random. This is the ideal condition, in which H(O)=8. An entropy comparison of the lena image can be found in Table 5, while in Table 6, the entropy of other

Figure 5. Analysis of correlation coefficient for original and encrypted images-[CT, Ultrasound, MRI, X-ray, ECG, Lena]

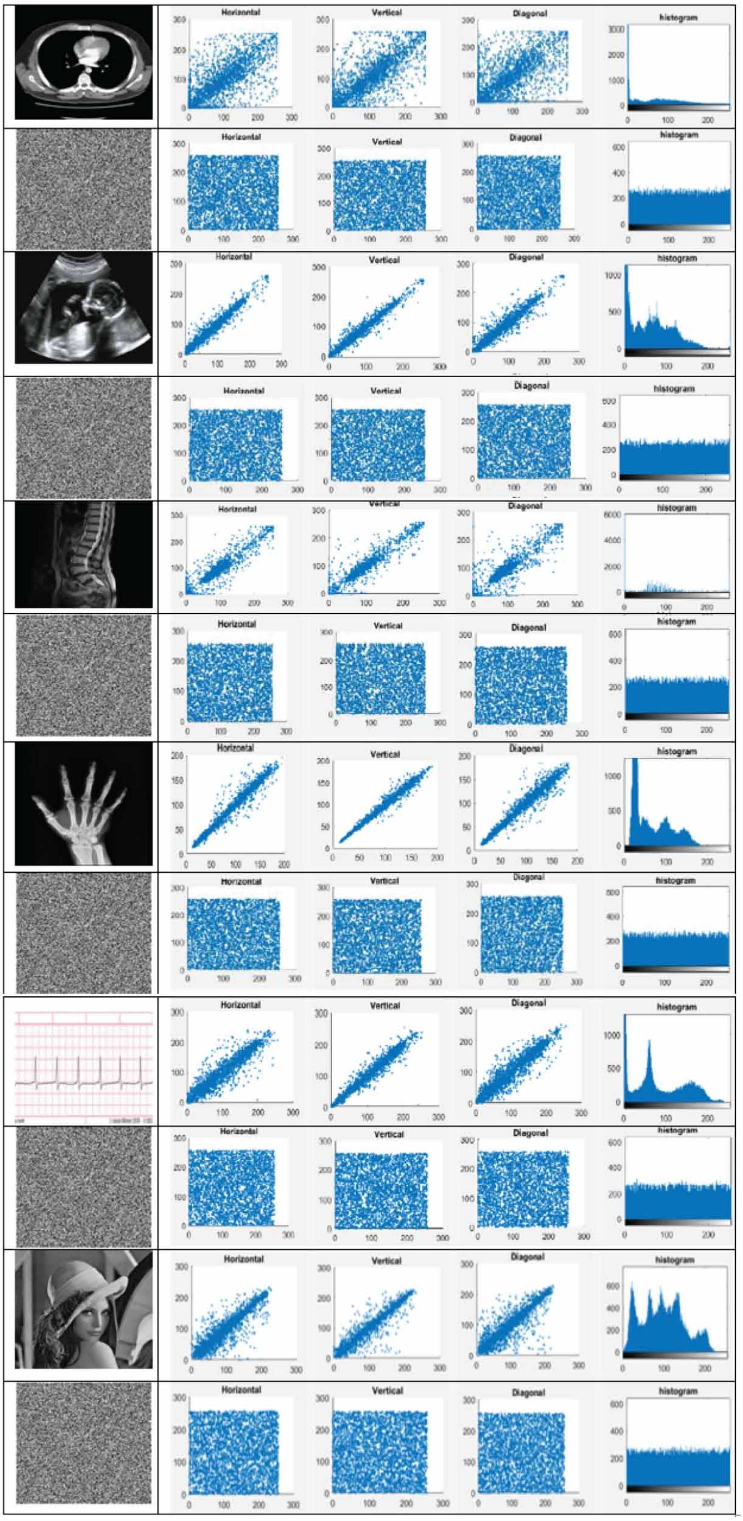


Table 5. Comparison of Lena-image entropy analysis

	Proposed DMIES	Zhang et al., 2017	Sujarani & Manivannan, 2017	Sathishkumar et al., 2011	Liu et al., 2018	Chai et al., 2017	Zhang et al., 2014
Lena-image	7.9976	7.9896	7.990	7.9634	7.9972	7.9974	7.9973

Table 6. Comparison of medical image global entropy analysis

	CT-image	Dagadu et al., 2019	Ultrasound-image	Dagadu et al., 2019	MRI-image	Dagadu et al., 2019	X-ray-image	Dagadu et al., 2019	ECG-image
Original image	3.9854	3.9854	7.0329	7.0329	5.6047	5.6047	7.3326	7.3326	3.6270
Encrypted image	7.9975	7.9973	7.9994	7.9993	7.9977	7.9974	7.9996	7.9993	7.9971

medical images can be seen. As shown in Table 6, all of the original images' entropy values are extremely near to the ideal value, implying very little information loss during encryption and strong resistance to entropy attacks.

Global entropy can occasionally fail to show the randomness of a partially encrypted image. Shannon entropy on a local scale addresses the flaws in global Shannon entropy. Splitting the encrypted image into non-overlapping segments and determining the global entropy can be used to compute it. Table 7 represents the predicted local Shannon entropies for encrypted and original medical images.

Analysis of Differential Attack

The encrypted image is examined in a differential attack to determine the image's origin. The differential attack is proved based on the Unified Average Changed Intensity (UACI) and Number of Changing Pixel Rate (NPCR) analysis. The proposed DMIES to assess image encryption techniques' resistance to differential analysis examines how sensitive an encrypted image consists of minor changes in the original image. The two measures used are NPCR and UACI, which are calculated using Equation (15-17):

$$NPCR = \frac{\sum_{a,b} D_1\left(a,b\right)}{WE_1 \times HE_1} \times 100\% \tag{15}$$

The height and width of the medical image are HE_1 and WE_1, respectively, while $D_1\left(a,b\right)$ is specified as:

Table 7. Comparison of medical image local entropy analysis

	CT-image	Ultrasound-image	MRI-image	X-ray-image	ECG-image
Original image	3.9854	7.0329	5.6047	7.3326	6.9311
Encrypted image	7.8795	7.8738	7.8971	7.8996	7.8394

$$D_1\left(a,b\right)=\left\{\begin{matrix} 0, \; if\, m_{iee}\left(a,b\right)=m_{ie}\left(a,b\right) \\ 1, \qquad if\, m_{iee}\left(a,b\right)\neq m_{ie}\left(a,b\right) \end{matrix}\right\} \tag{16}$$

where m_{iee} and m_{ie} are encrypted and ten-pixel values are changed from the original image.

UACI is specified as:

$$UACI=\frac{1}{WE_1+HE_1}\left[\sum_{a,b}\frac{\left|m_{iee}\left(a,b\right)-m_{ie}\left(a,b\right)\right|}{255}\right]\times 100\% \tag{17}$$

Tables 8, 9, and 10 show the results of both NPCR and UACI testing. The proposed DMIES alters the original image by ten pixels during the encryption process. The demonstrated testing result values in the proposed DMIES cryptosystem can withstand differential attacks and stabilize the presented scheme. Table 10 displays the UACI results, with all values passing, and demonstrating the rigor of the proposed DMIES.

Table 8. Lena-image UACI and NPCR analysis

	Proposed DMIES	Sathishkumar et al., 2011	Liu et al., 2018	Chai et al., 2017	Zhang et al., 2014	Hu et al., 2016
UACI	33.574	32.212	33.347	33.49	33.419	33.457
NPCR	99.643	98.475	99.621	99.62	99.6041	99.6077

Table 9. Medical image NPCR analysis

	CT-image	Ultrasound-image	MRI-image	X-ray-image	ECG-image
NPCR	99.789	99.781	99.843	99.809	99.668

Table 10. Medical image UACI analysis

<table>
<tr><th rowspan="4"></th><th colspan="3">UACI critical theoretical value</th><th rowspan="4">UACI</th></tr>
<tr><th colspan="3">UA*+0.001=33.7567% UA*-0.001=33.1495%
UA*+0.01=33.7026% UA*-0.01=33.2255%
UA*+0.05=33.6336% UA*-0.05=33.2625%</th></tr>
<tr><th colspan="3">Test outcomes of UACI</th></tr>
<tr><th>0.001-level</th><th>0.01-level</th><th>0.05-level</th></tr>
<tr><td>CT-image</td><td>Pass</td><td>Pass</td><td>Pass</td><td>33.487</td></tr>
<tr><td>Ultrasound-image</td><td>Pass</td><td>Pass</td><td>Pass</td><td>33.483</td></tr>
<tr><td>MRI-image</td><td>Pass</td><td>Pass</td><td>Pass</td><td>33.598</td></tr>
<tr><td>X-ray-image</td><td>Pass</td><td>Pass</td><td>Pass</td><td>33.423</td></tr>
<tr><td>ECG-image</td><td>Pass</td><td>Pass</td><td>Pass</td><td>33.447</td></tr>
</table>

Analysis of Exhaustive Attack

An exhaustive attack is a kind of brute-force attack. First, attackers perform an exhaustive search to discover the secret key. Then, by analyzing key sensitivity and key space, the exhaustive attack is validated.

Analysis of Key Space

The initial states and control parameters needed for the intertwining chaos map to create the pseudorandom bits constitute the key space set. A 128-bit external input key has been used to generate the first condition. According to the IEEE standard floating-point, a 64-bit double-accuracy integer has a computational accuracy of approximately 10^{-15} (Floating Point Working Group et al., 1985). To resist brute-force attacks, a successful encryption system must have a size of at least 2^{100} key space (Alvarez & Li, 2006). The designed method has a secret key space of 2^{128} bits, which is sufficient to withstand brute-force attacks if accuracy of 10^{-16} bits is used approximately.

Analysis of Key Sensitivity

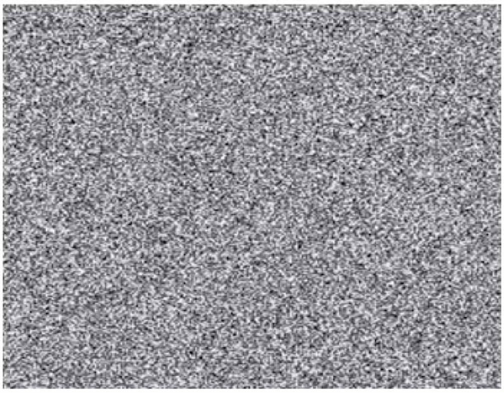
The intertwining chaotic map is extremely sensitive to early control factors and system evaluation metrics. Even minor changes in initial values in the decryption approach make retrieving the original medical image very difficult. For analysis of key sensitivity, the encrypted image is decoded with the erroneous key $x_n = 0.00000002$ in place of $x_n = 1$. As a result, the decoded medical image in Figure 6 differs significantly from the original medical image. The remaining secret key variables are also highly sensitive.

Analysis of PSNR and MSE

In evaluating the quality of a medical image, two metrics are used: Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The encrypted medical image and the original medical image are compared during the MSE analysis. In general, a value nearer to zero signifies greater similarity, whereas a number above zero indicates less similarity. For the original m_i and ciphered medical image m_{ie}, the MSE generates an estimated average squared error. Equation (18) defines the MSE where the size of the image is represented as *SI*:

$$MSE = \frac{\sum_{SI}\left[m_i\left(a,b\right) - m_{ie}\left(a,b\right)\right]^2}{SI} \tag{18}$$

Figure 6. Medical image was decrypted using an invalid key



$$PSNR = 10\log_{10}\frac{\left(256-1\right)}{MSE} \tag{19}$$

The PSNR ensures that noise during transmission does not affect the digitalized medical image's significance. The lower the PSNR number, the better the encryption method. Equation (19) defines the PSNR. Table 11 shows that the proposed DMIES have a low PSNR compared to the original medical images but a high MSE value. This implies that the proposed DMIES will have a high degree of performance and security.

Analysis of Cropping Attack

Cropping attack analysis may be calculated by cropping the encrypted image and then running the decryption method to get the original image. Figure 7 shows the image cropped by 10%, 5%, and 3%, respectively. The decoded images of data loss are shown in Figure 7. Even after cropping, original medical images could not be recovered, demonstrating the resilience of the proposed DMIES cryptosystem.

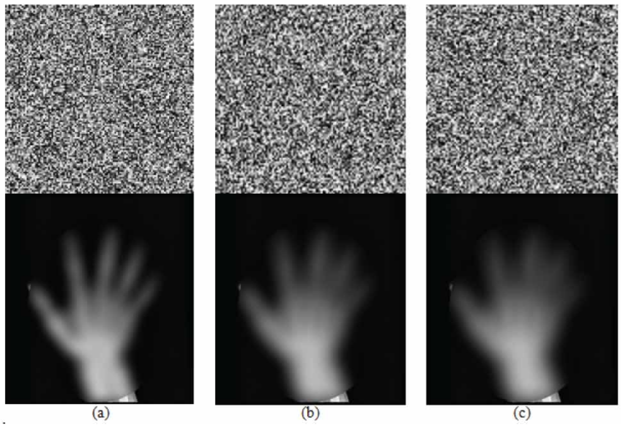
Analysis of Noise Attack

As a result of transmission over a noisy channel, the encrypted image has been subjected to interference. Therefore, an algorithm's quality has been determined by the amount of noise it can handle and the

Table 11. MSE and PSNR results

	MSE	PSNR
CT-image	15145.68	6.36
Ultrasound-image	12820.64	7.09
MRI-image	16814.41	5.91
X-ray-image	12077.12	7.35
ECG-image	11671.33	7.49
Lena-image	9130.17	8.56

Figure 7. Decrypted medical image-[X-ray] with data loss (a) 10% (b) 5% (c) 3%



capacity to identify the encoded image with a reliable receiver. In test cases, the proposed DMIES encrypts the encrypted image with a mean of zero and a Gaussian noise variation of 0.01. It also decrypts the image with the appropriate key using the salt and pepper noise density of 0.05. An encrypted sample image with salt-pepper noise and Gaussian noise is shown in Figure 8.

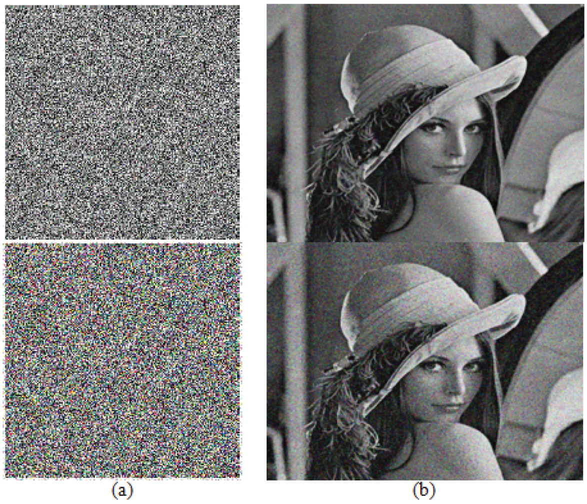
Performance Analysis

The value of NPCR is estimated to be around 99.78%, whereas the value of UACI is estimated to be approximately 33.59%. Thus, the findings are almost comparable to the optimum UACI » 33% and NPCR > 99% values (Ravichandran et al., 2017). Furthermore, the proposed DMIES MSE value is near 12077.12, and the PSNR value is near 7.91 dB, showing that the encryption system is of high quality. An entropy value indicates the uniformity of gray levels. For example, encrypted images are comparable to the 7.9975 entropy value, close to the 8.0 value of optimum entropy. Accordingly, the proposed DMIES provides a high level of security for encrypting medical images. In addition, the proposed DMIES cryptosystem requires 0.233s and 0.243s of processing time, respectively, to perform encryption and decryption. Six thousand pixels from a medical image have been chosen diagonally, horizontally, and vertically to assess the correlation coefficient of neighboring pixels. In each category, the average correlation coefficient is calculated for 100 images. According to the proposed DMIES, neighboring pixels in a decrypted medical image have substantially associated, whereas adjacent pixels in an encrypted medical image are less correlated. A medical image encrypted with a key is correlated with 0.0013, while a decoded image has a correlation coefficient of 0.9951. As a result, the proposed DMIES can use to send medical images over insecure networks.

Computational Complexity Analysis

DNA principles are used to encode all pixels in medical images for encryption. In level 1 for DNA encoding, this DMIES necessitates a runtime complexity of $O\left(n^2 \times 4\right)$. In level 2, a chaotic map is used to rearrange all pixels with an absolute runtime complexity of $O\left(n^2 \times 4\right)$. In level 3, all shuffled pixels are permutated using the knight's travel map with a runtime complexity of $O\left(n^2 \times k\right)$. The

Figure 8. Cipher Image-[Lena] (A) Salt-Pepper Noise And Gaussian Noise And (B) Decrypted Image With Salt-Pepper Noise And Gaussian Noise



proposed DMIES has a runtime complexity that is almost equivalent to $O\left(\left(n^2/3\right)\times 4\right)$. In the proposed DMIES algorithm, rather than shuffling all pixels of medical images in a permutation round, only chosen pixels are rearranged.

CONCLUSION

A new medical image encryption cryptosystem is introduced based on the intertwining chaotic maps, knight's travel map, DNA sequencing, and affinity transforming. The original medical image is first split into the B_1 pixel DNA-coded matrix. The rest of the pixels DNA-coded matrix B_2 deploy on the pixel index value selection using DNA rules. Then, in the intertwining chaotic map, the system parameters and control parameters produce chaotic sequences. It is used to confuse the encoded DNA matrix B_1 chosen pixels. Besides, the scrambled DNA-coded B_1 and B_2 matrices are combined using DNA-XOR. Then, the knight's travel map permutates the DNA-coded matrix to dislocate the pixel values. Furthermore, the permutated pixel value is decoded into a binary image and then transformed into a grayscale image. Finally, the grayscale image is transformed by affinity to produce the encrypted image. The findings of the performance study demonstrate that the proposed DMIES significantly enhances security while preventing differential, cropping, exhaustive, noise, and statistical attacks. The proposed DMIES is suited for smart health, telemedicine, and e-health applications since it requires less processing time of 0.243s.

FUNDING AGENCY

Publisher has waived the Open Access publishing fee.

REFERENCES

Al-Husainy, M. A. F. (2012). A novel encryption method for image security. *International Journal of Security and its Applications*, *6*(1), 1-8.

Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, *16*(8), 2129–2151. doi:10.1142/S0218127406015970

Anusudha, K., Venkateswaran, N., & Valarmathi, J. (2017). Secured medical image watermarking with DNA codec. *Multimedia Tools and Applications*, *76*(2), 2911–2932. doi:10.1007/s11042-015-3213-1

Askar, S. S., Karawia, A. A., & Alshamrani, A. (2015). Image encryption algorithm based on chaotic economic model. *Mathematical Problems in Engineering*, *2015*, 1–10. Advance online publication. doi:10.1155/2015/341729

Bai, S., Zhu, G., & Huang, J. (2013). An Intelligent Algorithm for the (1,2,2)-Generalized Knight's Tour Problem. *Ninth International Conference on Computational Intelligence and Security*, 583-588. doi:10.1109/CIS.2013.129

Bechikh, R., Hermassi, H., El-Latif, A. A. A., Rhouma, R., & Belghith, S. (2015). Breaking an image encryption scheme based on a spatiotemporal chaotic system. *Signal Processing Image Communication*, *39*, 151–158. doi:10.1016/j.image.2015.09.006

Belazi, A., Abd El-Latif, A. A., & Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, *128*, 155–170. doi:10.1016/j.sigpro.2016.03.021

Chai, X., Gan, Z., Lu, Y., Chen, Y., & Han, D. (2017). A novel image encryption algorithm based on the chaotic system and DNA computing. *International Journal of Modern Physics C*, *28*(05), 1750069. Advance online publication. doi:10.1142/S0129183117500693

Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos, Solitons, and Fractals*, *21*(3), 749–761. doi:10.1016/j.chaos.2003.12.022

Dagadu, J. C., Li, J., Aboagye, E. O., & Deynu, F. K. (2019). Medical image encryption scheme based on multiple chaos and DNA coding. *International Journal of Network Security*, *21*, 83–90.

Elashry, I., Faragallah, O. S., Abbas, A. M., & El-Rabaie, E. M. (2007). Homomorphic image encryption. *Journal of electronic*. *Engineering (London)*, *18*(3), 033002. doi:10.1117/1.3167847

Enayatifar, R., Sadaei, H. J., Abdullah, A. H., Lee, M., & Isnin, I. F. (2015). A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. *Optics and Lasers in Engineering*, *71*, 33–41. doi:10.1016/j.optlaseng.2015.03.007

Floating Point Working Group. (1985*). IEEE standard for binary floating-point arithmetic.* IEEE Std, 754-1985.

Fu, C., Li, W. J., Meng, Z. Y., Wang, T., & Li, P. X. (2013). A symmetric image encryption scheme using chaotic baker map and Lorenz system. In *2013 Ninth International Conference on Computational Intelligence and Security* (pp. 724–728), Leshan, China. IEEE. doi:10.1109/CIS.2013.158

Gao, H., Zhang, Y., Liang, S., & Li, D. (2006). A new chaotic algorithm for image encryption. *Chaos, Solitons, and Fractals*, *29*(2), 393–399. doi:10.1016/j.chaos.2005.08.110

Ghosh, D., & Bhaduri, U. (2017). A simple recursive backtracking algorithm for knight's tours puzzle on standard 8×8 chessboard. *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 1195-1200. doi:10.1109/ICACCI.2017.8126004

Gleick, J. (1987). *Chaos Making a New Science*. Viking Books.

Hu, T., Liu, Y., Gong, L., & Ouyang, C. (2016). An image encryption scheme combining chaos with cycle operation for DNA sequences. *An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems*, *87*(1), 51–66. doi:10.1007/s11071-016-3024-6

Hu, T., Liu, Y., Gong, L. H., & Ouyang, C. J. (2017). An image encryption scheme combining chaos with cycle operation for DNA sequences. *Nonlinear Dynamics*, *87*(1), 51–66. doi:10.1007/s11071-016-3024-6

Jin, C., & Liu, H. (2017). A color image encryption scheme based on arnold scrambling and quantum chaotic. *International Journal of Network Security*, *19*(3), 347–357.

Kanso, A., & Ghebleh, M. (2015). An efficient and robust image encryption scheme for medical applications. *Communications in Nonlinear Science and Numerical Simulation*, *24*(1–3), 98–116. doi:10.1016/j.cnsns.2014.12.005

Krishnamoorthi, R., & Murali, P. (2014). Chaos based image encryption with orthogonal polynomials model and bit shuffling. In *2014 International Conference on Signal processing and Integrated Networks (SPIN)* (pp. 107–112). Noida, India. IEEE. doi:10.1109/SPIN.2014.6776931

Li, J., Xing, Y., Qu, C., & Zhang, J. (2015). An image encryption method based on tent and Lorenz chaotic systems. In *6th International Conference on Software Engineering and Service Science (ICSESS'15)* (pp. 582-586). IEEE. doi:10.1109/ICSESS.2015.7339125

Li, X., Zhou, C., & Xu, N. (2018). A secure and efficient image encryption algorithm based on dna coding and spatiotemporal chaos. *International Journal of Network Security*, *20*(1), 110–120.

Liang, H. R., Tao, X. Y., & Zhou, N. R. (2016). *Quantum image encryption based on generalized affine transform and logistic map*. Quant Info Proc. doi:10.1007/s11128-016-1304-1

Lin, Z., & Wang, H. (2010). Efficient image encryption using a chaos-based PWL memristor. *IETE Technical Review*, *27*(4), 318–325. doi:10.4103/0256-4602.64605

Liu, Y., Lin, T., Wang, J., & Yuan, H. (2018). Bit image encryption algorithm based on hyper chaos and DNA sequence. *Journal of Computers*, *29*, 43–55.

Lokeshwari, G., Susarla, S., & Kumar, S. U. (2015). A modified technique for reliable image encryption method using Merkle-Hellman cryptosystem and RSA algorithm. *Journal of Discrete Mathematical Sciences and Cryptography*, *18*(3), 293–300. doi:10.1080/09720529.2014.968367

Mao, Y., & Chen, G. (2005). Chaos-based image encryption. Handbook of Geometric Computing, 231-265.

Norouzi, B., Mirzakuchaki, S., & Norouzi, P. (2017). Breaking an image encryption technique based on neural chaotic generator. *Optik (Stuttgart)*, *140*, 946–952. doi:10.1016/j.ijleo.2017.04.103

Parvin, Z., Seyedarabi, H., & Shamsi, M. (2016). A new secure and sensitive image encryption scheme based on new substitution with chaotic function. *Multimedia Tools and Applications*, *75*(17), 10631–10648. doi:10.1007/s11042-014-2115-y

Priyanka & Maheshkar, S. (2017). Region-based hybrid medical image watermarking for secure telemedicine applications. *Multimedia Tools and Applications*, *76*, 3617-3647.

Ravichandran, D., Praveenkumar, P., Rayappan, J. B. B., & Amirtharajan, R. (2016). Chaos based crossover and mutation for securing DICOM image. *Computers in Biology and Medicine*, *72*, 170–184. doi:10.1016/j.compbiomed.2016.03.020 PMID:27046666

Ravichandran, D., Praveenkumar, P., Rayappan, J. B. B., & Amirtharajan, R. (2017). DNA chaos blend to secure medical privacy. *IEEE Transactions on Nanobioscience*, *16*(8), 850–858. doi:10.1109/TNB.2017.2780881 PMID:29364129

Sam, I. S., Devaraj, P., & Bhuvaneswaran, R. S. (2012). An intertwining chaotic maps based image encryption scheme. *Nonlinear Dynamics*, *69*(4), 1995–2007. doi:10.1007/s11071-012-0402-6

Sankpal, P. R., & Vijaya, P. A. (2014). Image encryption using chaotic maps: A survey. *Fifth International Conference on Signal and Image Processing (ICSIP'14)*, 102-107. doi:10.1109/ICSIP.2014.80

Sathishkumar, G. A., Bagan, K. B., & Sriraam, N. (2011). Image Encryption Based on Diffusion and Multiple Chaotic Maps. *International Journal of Network Security & Its Applications*, *3*, 181– 194.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Labs Technical Journal*, *28*(4), 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x

Souyah, A., & Faraoun, K. M. (2016). An image encryption scheme combining chaos-memory cellular automata and weighted histogram. *Nonlinear Dynamics*, *86*(1), 639–653. doi:10.1007/s11071-016-2912-0

Srichavengsup, W., & San-Um, W. (2016). Data encryption scheme based on rules of cellular automata and chaotic map function for information security. *International Journal of Network Security*, *18*(6), 1130–1142.

Sujarani, R., & Manivannan, D. (2017). A non linear two dimensional henon_sine chaotic map based image cryptosystem. *International Journal of Pure and Applied Mathematics*, *115*, 215–221.

Tang, Z., Zhang, X., & Lan, W. (2015). Efficient image encryption with block shuffling and chaotic map. *Multimedia Tools and Applications*, *74*(15), 5429–5448. doi:10.1007/s11042-014-1861-1

Wang, Q., Zhang, Q., & Zhou, C. (2009). A multilevel image encryption algorithm based on chaos and DNA coding. *Fourth International on Conference on Bio-Inspired Computing*, 1–5. doi:10.1109/BICTA.2009.5338154

Wang, X. Y., Zhang, Y. Q., & Zhao, Y. Y. (2015). A novel image encryption scheme based on 2-d logistic map and DNA sequence operations. *Nonlinear Dynamics*, *82*(3), 1269–1280. doi:10.1007/s11071-015-2234-7

Yap, W. S., Phan, R. C. W., Yau, W. C., & Heng, S. H. (2015). Cryptanalysis of a new image alternate encryption algorithm based on chaotic map. *Nonlinear Dynamics*, *80*(3), 1483–1491. doi:10.1007/s11071-015-1956-x

Ye, R. (2011). An Image Encryption Scheme with Efficent Permutation and Diffusion Processes. *CCIS*, *202*, 32–39.

Younus, Z. S., & Younus, G. T. (2019). Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data. *Journal of Intelligent Systems*, *29*(1), 1–10. doi:10.1515/jisys-2018-0225

Zhang, L. Y., Hu, H., Liu, Y., Wong, K., & Gan, J. (2014). A chaotic image encryption scheme owning temp-value feedback. *Communications in Nonlinear Science and Numerical Simulation*, *19*(10), 3653–3659. doi:10.1016/j.cnsns.2014.03.016

Zhang, X., Han, F., & Niu, Y. (2017). Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding. *Computational Intelligence and Neuroscience*, *2017*, 1–11. Advance online publication. doi:10.1155/2017/6919675 PMID:28912802