Taylor & Francis
Taylor & Francis Group

Information Security Journal: A Global Perspective

ISSN: 1939-3555 (Print) 1939-3547 (Online) Journal homepage: https://www.tandfonline.com/loi/uiss20

Selective medical image encryption using DNA cryptography

Prema T. Akkasaligar & Sumangala Biradar

To cite this article: Prema T. Akkasaligar & Sumangala Biradar (2020) Selective medical image encryption using DNA cryptography, Information Security Journal: A Global Perspective, 29:2, 91-101, DOI: 10.1080/19393555.2020.1718248

To link to this article: https://doi.org/10.1080/19393555.2020.1718248

Published online: 01 Feb 2020.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
2020, VOL. 29, NO. 2, 91–101
https://doi.org/10.1080/19393555.2020.1718248

Selective medical image encryption using DNA cryptography

Prema T. Akkasaligar[a] and Sumangala Biradar[b]

[a]Department of Computer Science & Engineering, BLDEA's V.P. Dr. P. G. Halakatti College of Engineering and Technology, Vijayapur, India; [b]Department of Information Science & Engineering, BLDEA's V.P. Dr. P. G. Halakatti College of Engineering and Technology, Vijayapur, India

ABSTRACT

In the medical field, advanced techniques like e-health, smart health, and telemedicine applications are in use. These techniques transmit a digital medical image via open-source networks. The digital medical image contains confidential and sensitive information of patients. The transmitted digital medical images are used for diagnosis in the remote center. Hence, providing security and maintaining the confidentiality of the medical image is a major apprehension. In this paper, DNA cryptography and dual hyperchaotic map techniques are proposed to provide high-level security for a digital medical image. The digital medical images are very large in size and require more computational time. To reduce computational time, the selective digital medical image encryption algorithm is proposed. In the proposed cryptosystem, the permutation and diffusion process are performed on selected pixels of digital medical images. To construct theDNA structure for digital medical images, all DNA encoding rules based on the pixel position of the digital medical image are used. The cipher image is attained by using all DNA decoding rules based on the pixel value of the digital medical image. The proposed cryptosystem is resistant to different types of attacks.

KEYWORDS

DNA cryptography; digital medical image encryption; digital medical image decryption; dual hyperchaos map

1. Introduction

In the medical field, e-health, smart health, and telemedicine are advanced systems. These systems utilize digital medical information for end-to-end communication. This digitalization reduces time, but it is open source. Hence, hackers can tamper the digital medical image during transmission. In medical diagnosis, the diagnosis of exact disease from the tampered digital medical image is difficult. Hence, providing security and maintaining the confidentiality of a medical image and reducing the computational time of the encryption algorithm are the major issues for researchers. Several image encryption techniques are available using cryptography, steganography, and watermarking. These traditional methods are not enough to provide high-level security for medical image. The DNA cryptography and chaotic system are advanced techniques in the existing literature. These techniques are in a premature stage and detail literature survey is carried out as follows.

Due to the sensitive nature of a modular cosine number transform (CNT), the CNT is used to encrypt medical image (Lima, Madeiro, & Sales, 2015). The CNT is effective for the low-frequency nature of an image but not for high-frequency nature. Kanso & Ghebleh (2015) have proposed selective medical image encryption using a 2D chaotic cat map. In a digital medical image, only sensitive information is masked with a synthetic image. The 2D chaotic cat map is not resisted against brute force attack due to limited key space. Kester et al. (2015) used mean and entropy technique for encryption of the digital medical image. Sebastian and Delson (2016) have proposed the Rivest, Adi Shamir and Leonard Adleman (RSA) algorithm for encryption of magnetic resonance imaging (MRI) images. Further, the K-means and watershed segmentation is used to extract details of the tumor. The RSA is very slow for large size medical images. Anusudha, Venkateswaran, and Valarmathi (2017) proposed logistic map and DNA sequence rules to create a DNA mask. The best DNA mask is obtained by using a genetic algorithm. The digital watermarked image is obtained by embedding the electronic patient record into the DNA mask. The computation cost of the method is very high. Hence,

CONTACT Sumangala Biradar, Assistant Professor ✉ biradarsumangala@gmail.com Information Science and Engineering B.L.D.E.A's V.P.Dr.P.G. HALAKATI College of Engineering and Technology, Ashram road, Vijayapura-586103, Karnataka, India

a simple computational method with sufficient security is required. The piecewise linear memristor and the chaotic map are used for encryption (Lin & Wang, 2010). The hyperchaotic map, pseudo-random generator, and DNA sequences are used for multilevel encryption of the image (Wang, Zhang, and Zhou (2009)). But it takes more computational time due to multilevel encryption. The baker map, tent map, and Lornez system are used to encrypt the image (Fu, Li, Meng, Wang, and Li 2013; Krishnamoorthi and Murali 2014). The chaotic maps are very sensitive to initial condition and security depends on initial condition. Due to limited key space, not resist against exhaustive search attack.

The literature survey shows that encryption techniques cannot survive every possible attack and not enough to provide high-level security with less computational time. Due to the unique nature of DNA cryptography and very complex confusion property of chaotic map, it is suitable to provide high-level security. But, they require more computational time. Hence, reducing the computational time of encryption of medical image is a big challenge in the research area. The main objective of the proposed system is to reduce computational time along with efficient security. To reduce computational time and to provide high-level security for the digital medical image, selective medical image cryptosystem is proposed using dual hyperchaos map and DNA sequences.

The objectives of the proposed system are as follows: (1) The confusion and diffusion process of chaotic system are performed on selected pixels of digital medical images. (2) The randomness of dual chaotic system is used to provide high-level security. (3) All DNA encoding and decoding rules are used to generate unique DNA structure and cipher image instead of using a specific one. The selection of DNA encoding and decoding rules is depending on pixels of the digital medical image hence for every medical image will get unique DNA structure.

The rest of the paper is organized as follows: In Section 2, digitized medical image encryption schemes are introduced. Section 3 describes the proposed selective medical image cryptosystem. Section 4 illustrates experimental results and security analysis. The conclusion is presented in Section 5.

2. Digitized medical image encryption schemes

The digitized medical image encryption schemes namely, dual hyperchaos map and DNA sequence operations are explained. The dual hyperchaos map is the combination of Taylor chirikov map and Chen's hyperchaotic map. The Taylor chirikov map has a very complex confusion property. It presents the straightforward and most precise means to envisage the behavior of conventional systems with two degrees of liberty. It is two-dimensional chaotic maps; hence, it is not sufficient to provide security for digitized chaotic map. The Chen's hyperchaotic map is a high dimensional chaotic map with dynamic uniqueness and good confusion property. Hence to provide security, the combination of Taylor chirikov map and Chen's hyperchaotic map is used as a dual hyperchaos map. Due to the uniqueness of DNA, it is used to enhance the security of digitized medical image.

2.1. Dual hyperchaos map

The dual hyperchaos map is the combination of Taylor Chirikov map and Chen's hyperchaotic map. The Taylor Chirikov Map is a discrete map. This map explains the poincare surface of the fraction of a straightforward involuntary system and is represented as the kicked rotator. The kicked rotator is composed of a gravitational force and a free stick. It frictionlessly rotates around the axis of a plane on one tip and kicked periodically on the further tip.

The Chen's hyper chaotic map has spatiotemporal complexity and mixture property due to the more than one positive Lyapunov exponent. The chaotic sequences obtained by the hyperchaotic map are extremely complex, difficult to predict and explore. The dual hyperchaos map is represented by Eqs. (1–6).

$$\mathrm{x}_{n+1} = \frac{(\mathrm{x}_n + Ksin(\mathrm{y}_n))}{2} \tag{1}$$

$$\mathrm{y}_{\mathrm{n}+1} = (\mathrm{y}_{\mathrm{n}} + \mathrm{x}_{\mathrm{n}+1}(\mathrm{mod}2\pi)) - 0.4 \tag{2}$$

$$x^{`} = a(y_{n+1} - x_{n+1}) \tag{3}$$

$$y^{`} = -x_{n+1}z + dx_{n+1} + cy_{n+1} - x_n \tag{4}$$

$$z^{`} = x_{n+1}y_{n+1} - bz \tag{5}$$

$$q^{`} = x_{n+1} + l \tag{6}$$

where the variable x_n is the angular position of the stick and y_n is its angular momentum after the nth kick. The constant K is the intensity of the kicks on the kicked rotator. The value of K controls the degree of chaos. Where a, b, c, and d are control factors. The value of l varies from −0.7 to 0.7. The x, y, and z represent a chaotic sequence. In dual chaos map, the Taylor Chirikov map is used to provide initial values for system parameters of Chen's hyper chaotic map. The chaotic sequence of Chen's is used to shuffle the pixels of the digital medical image.

The degree of chaos provides very complex confusion property and highly sensitive to the initial condition. Hence, it is suitable to provide security for digitized medical images. To enhance the security of a digital medical image, the dual hyperchaos map is used along with DNA cryptography.

2.2. *DNA sequence operations*

The DNA cryptography is a fresh domain in cryptography and is used as an information carrier. In DNA cryptography, unique DNA structure is generated for every digital image using different DNA sequences. The basic DNA structure consists of four nucleotide elements namely, Guanine (G), Adenine (A), Cytosine (C), and Thymine (T) (Wang et al., 2009). It is composed of two chains which are put together due to the key hydrogen. The double helix structure is formed by putting chains together. One chain is complementary to the other in the base sequence, that is, C is the complement of G and A is the complement of T.

Similarly, in a binary representation, 0 and 1 are opposite; therefore 01 and 10 are opposite, 00 and 11 are opposite. Hence, the nucleic acid bases G, C, A, and T are encoded as 10, 01, 00; and 11, respectively. By using this theory we can get 4! = 24 different encoding patterns. But only eight patterns of DNA base encoding and decoding rules satisfy the opposite pairing base, which is specified below:

Rule_1: 00=A 11=T 01=G 10=C
Rule_2: 00=A 11=T 10=G 01=C
Rule_3: 01=A 10=T 00=G 11=C
Rule_4: 01=A 10=T 11=G 00=C
Rule_5: 10=A 01=T 00=G 11=C
Rule_6: 10=A 01=T 11=G 00=C
Rule_7: 11=A 00=T 01=G 10=C
Rule_8: 11=A 00=T 10=G 01=C

These encoding rules are used to generate a DNA structure for the digital medical image. For each image, a unique DNA structure will be obtained. Hence, it is used to provide high-level security for the digitized medical image in a proposed selective digitized medical image cryptosystem.

3. Selective digitized medical image cryptosystem

In the proposed selective digitized medical image cryptosystem, the dual hyperchaos map and DNA sequence operations are used to provide security for medical images is shown in Figure 1. In the proposed model, the pixels are selected from the original digitized medical image using Pixel_selection method represented in Algorithm 1.

Algorithm 1: Pixel_selection

```
//Input: The original digitized medical image $I_o$ (m, n), where m is
  row size and n is column size
//Output: Selected pixels are stored in matrices $M_1$ and $M_2$
    for i = 0 to m do
        for j = 0 to n do
        a = $I_o$ (i, j) % 3;
        b = floor (a);
        w = b-a;
        if (w < 0) then
            $M_1$(i,j) = $I_o$(i,j);
        else
            $M_2$(i,j) = $I_o$(i,j);
        end
    end
  end
```

The selected pixels are stored in matrix M_1 and remaining pixels in matrix M_2. Both matrices are converted into an 8-bit binary image. All the eight patterns of DNA bases are employed on an 8-bit binary image to obtain 4-bit DNA-encoded matrix

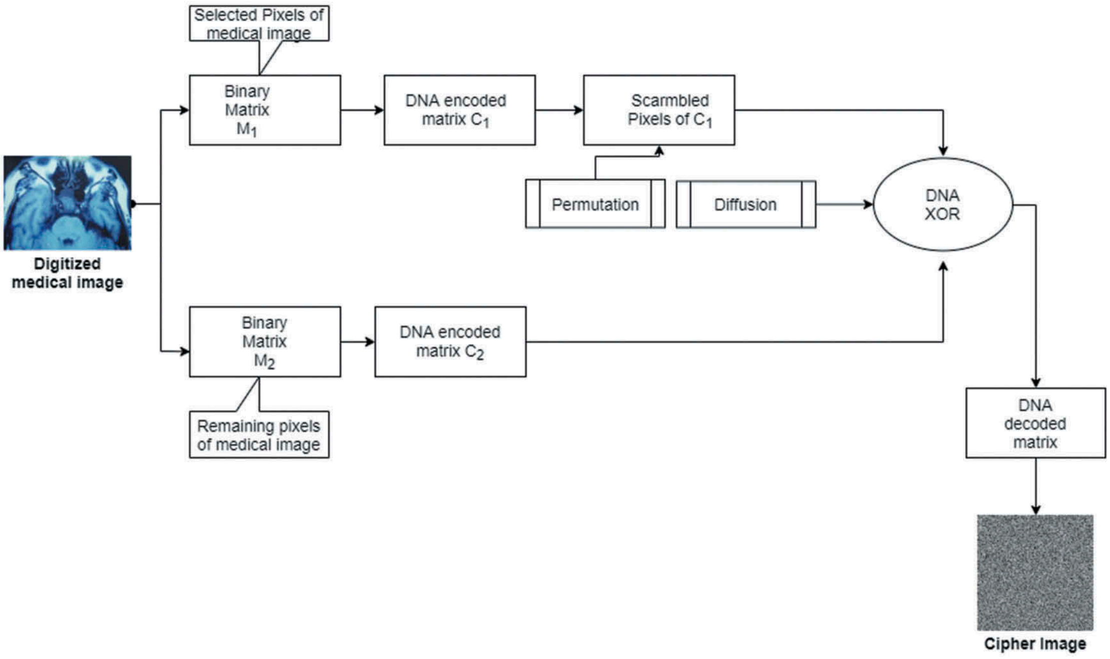


Figure 1. Proposed SDMIE method.

C_1 and 4-bit DNA-encoded matrix C_2. The selection of DNA encoding rules depends on the pixel index of the binary image.

3.1. Selection of DNA rules

The DNA-encoded matrix is attained by using different DNA encoding rules based on pixel index, instead of using the specific encoding rule. Selection of DNA rules is defined in Eq.(7).

$$\text{Rule\_n} = (\text{Index}(I_o(i, j))\text{mod } 8) + 1 \tag{7}$$

where (Index I_o (i, j)) is a pixel index of the digitized medical image. Assume that the pixel index is 131, 131 mod 8 is equal to 3 + 1 = 4. The Rule_4: 01 = A, 10 = T, 11 = G and 00 = C is used to convert 8-bit {01101100} into 4-bit {ATGC}. In this way, for each pixel different DNA rules are used to generate a unique DNA-encoded matrix.

3.2. Permutation process

The permutation process of the chaotic system is the shuffling of pixels. The DNA-encoded matrix C_1 pixels are shuffled using a dual hyperchaos map. The chaotic sequences are produced using the dual hyperchaos map method. The chaotic sequences are arranged in order to shuffle the pixels in the permutation process. Based on ordered sequences, the index values are changed and based on index value, the DNA-encoded matrix C_1 pixels are shuffled. For example, if chaotic sequence is $P = \{1.2, 0.8, 0.98, 1.4\}$ with index P [0 1 2 3], then sorted sequences is $P = \{0.8, 0.98, 1.2, 1.4\}$ with index P [1 2 0 3]. This index is used to shuffle the pixels of C_1. In this way, the DNA-encoded matrices pixels are shuffled.

3.3. Diffusion process

The diffusion process of the chaotic system is the changing of pixel values. The DNA-encoded matrix pixel values are changed using DNA XOR operation. For example, the DNA-encoded matrix C_1 has DNA sequence as {A T G C} and {G A C T} in the DNA-encoded matrix C_2. These two sequences are combined using XOR and the new sequence obtained is {G T T G} which is totally different.

3.4. DNA decoding rules

The DNA decoding means converting DNA-encoded matrix into binary image. After permutation and diffusion process, DNA-encoded matrix is converted into binary image using DNA decoding rules. The selection of decoding rules depends on the last two bits of each pixel of the DNA-encoded matrix. It is shown below:

AA | GA: Rule_1: A=00 T=11 G= 01 C=10
AT | GT: Rule_2: A=00 T=11 G=10 C=01
AG | GG: Rule_3: A=01 T=10 G=00 C=11
AC | GC: Rule_4: A=01 T=10 G=11 C=00
TA | CA: Rule_5: A=10 T=01 G=00 C=11
TG | CG: Rule_6: A=10 T=01 G=11 C=00
TC | CC: Rule_7: A=11 T=00 G=01 C=10
TT | CT: Rule_8: A=11 T=00 G=10 C=01

For example, in DNA-encoded matrix, if the pixel value is ATGC then based on the last two bits, i.e., GC Rule_4 is used to convert the DNA-encoded matrix into a binary medical image. The binary image is converted into a grayscale medical image to obtain a cipher image. For better understanding, the detail steps of selective encryption technique are shown in Algorithm 2.

The decryption technique is performed using a reverse process of the SDMIE algorithm.

In the proposed SDMIE methodology, the security level is enhanced by using all DNA encoding rules specified in Section 2.2 and all DNA decoding rules specified in Section 3.4. The big challenge in DNA cryptography is computational time. To reduce it, selected pixels are shuffled using dual hyperchaos sequence instead of shuffling all pixels. Due to good confusion property and randomness of dual hyperchaos map, guessing of pixel sequence is highly impossible for attackers. Hence, the proposed system provides sufficient security along with reduced computational time.

4. Experimental results and security analysis of SDMIE

The experimentation is conducted on Intel core i7 system with 8 GB RAM and 2.70 GHz processor. The 500 digital medical images of five categories (each type 100) like MRI, CT, X-Ray, and Ultrasound images of size 512 × 512 are tested. These images are collected from "National Library of Medicine's Open Access Biomedical Images Search Engine" (https://openi.nlm.nih.gov). The ECG image of size 512 × 512 collected from ecg_educator.blogspot.co.uk. The Matlab (R2015b) tool is employed to implement the proposed SDMIE method. The sample original digitized medical image is shown in Figure 2a. In the proposed model, the pixels are selected from

Algorithm 2: Selective_Digitized_Medical_Image_Encryption (SDMIE)

```
//Input: The original digitized medical image $I_o(m, n)$
//Output: Cipher image $I_e(m, n)$
    Step 1: Start
    Step 2: Divide into two matrices
            $M_1(m,n)$ = Selected pixels of $I_o$ (m, n) using Pixel_selection Algorithm 1;
            $M_2(m,n)$ = Remaining pixels of $I_o$ (m, n);
    Step 3 : Convert into binary images
            $B_1(m \times 8, n \times 8) = dec2bin(M_1(m,n))$;
            $B_2(m \times 8, n \times 8) = dec2bin(M_2(m,n))$;
    Step 4 : Convert into DNA-encoded matrix using DNA base encoding rules specified in Section2.2
            $C_1(m \times 4, n \times 4)$ = DNA-encoded Matrix of $B_1(m \times 8, n \times 8)$
            $C_2(m \times 4, n \times 4)$ = DNA-encoded Matrix of $B_2(m \times 8, n \times 8)$
    Step 5: The chaotic sequences x, y are generated using dual hyperchaos map
            $x = [x_0, x_1, x_2, x_3, \ldots\ldots x_N]$;
            $y = [y_0, y_1, y_2, y_3, \ldots\ldots y_N]$;
            $\bar{x}$ = sort (x);
            $\bar{y}$ = sort (y);
    Step 6 : The index value of sorted chaotic sequences $\bar{x}$ and $\bar{y}$ are used to jumble the pixels of
            $C_1(m \times 4, n \times 4)$.
    Step 7: Fusion of DNA-encoded matrices is:
            $C_{12}(m \times 4, n \times 4) = C_1(m \times 4, n \times 4)$ DNA XOR$C_2(m \times 4, n \times 4)$
    Step 8 : Transform DNA-encoded matrix into 8-bit binary image using DNA decoding rules specified in Section 3.4.
            $B_{12}(m \times 8, n \times 8) = C_{12}(m \times 4, n \times 4)$
    Step 9 : Convert binary image into cipher image
            $I_e(m, n) = bin2dec(B_{12}(m \times 8, n \times 8))$
    Step 10 : Stop
```

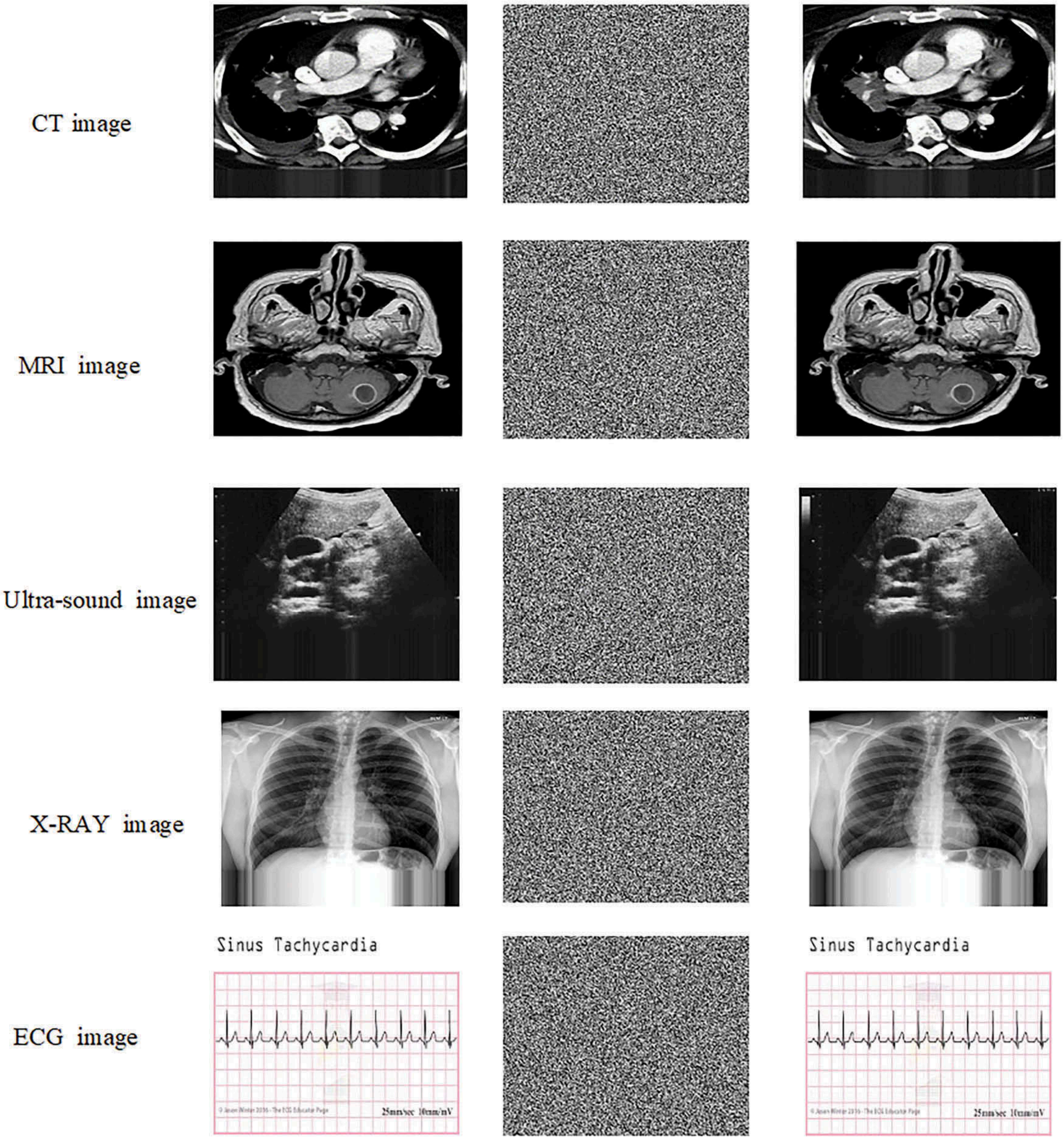


Figure 2. Samples of (a) Original digitized image, (b) Cipher image, and (c) Decrypted digitized medical image.

Table 1. DNA XOR operation.

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

the original digitized medical image using Pixel_selection Algorithm 1. These pixels are stored in matrix M_1 and remaining pixels in matrix M_2. Both matrices are converted into an 8-bit binary image. All the eight patterns of DNA encoding rules explained in Section 2.2 are employed on 8-bit binary image to obtain 4-bits DNA-encoded matrix C_1 and 4-bits DNA-encoded matrix C_2. In dual hyperchaos map the initial values of parameters $x_n = 1$, $y_n = 0.5$, $K = 0.8$, $z = K + 0.4$ and control parameters $a = 36$, $b = 3$, $c = 28$, $d = 16$, and $l = 0.2$ are considered to produce chaotic sequences. These sequences are arranged in order and index of the ordered sequences are employed to scramble the selected pixels of DNA-encoded matrix C_1. The DNA XOR procedure represented in Table 1 is employed to merge the two matrices C_1 and C_2. The intermediate cipher image is obtained after fusion. All DNA decoding rules specified in Section 3.4 are used to convert intermediate cipher image into cipher image as shown in Figure 2b. The cipher image is decrypted using the inverse process of SDMIE algorithm. The decrypted image is shown in Figure 2c.

The crypto investigation such as differential attacks, exhaustive attacks, and statistical attacks are performed to analyze the performance of proposed SDMIE technique. The peak signal-to-noise ratio (PSNR), mean square error (MSE) and entropy are employed to verify the error rate of a digital medical image.

4.1. Statistical attack

In statistical attack, invaders try to predict plain image and secret keys based on the distribution of gray levels in cipher image. The correlation coefficient analysis and histogram analysis are employed to verify the statistical attack.

4.1.1. Correlation coefficient analysis

The correlation coefficient is used to determine correlation between the adjoining pixels in the given digital medical images. The correlation measures the degree of correspondence between two pixels. The lower degree between adjoining pixels indicates that the encryption technique is the best technique. Pearson's correlation coefficient is given below (Hiremath, Prema, & Sharan, 2013).

$$r = \frac{S\sum I_O\overline{I_O} - \left(\sum I_O\right)\left(\sum \overline{I_O}\right)}{\sqrt{S\left(\sum I_O^2\right) + \left(\sum I_O\right)^2\sqrt{N\left(\sum \overline{I_O^2}\right) + \left(\sum \overline{I_O}\right)^2}}} \tag{8}$$

where $\mathrm{I_o}$ and $\overline{\mathrm{I}}_\mathrm{o}$ are the gray-level values of the original digitalized medical image and adjoining pixels of the digitalized medical image, respectively. The S is the size (m × n) of an medical image. The degree value +1 of r indicates positively correlated and degree value −1 indicates negatively correlated. A zero value indicates no correlation. If P_1 is current pixel and P_2 is adjoining pixel, in positive correlation, if the value of P_1 increases then the value of P_2 also increases means both move in the same direction. In negative correlation, if the value of P_1 increases then the value of P_2 decreases means both move in the opposite direction.

4.1.2. Histogram analysis

The histogram analysis is the graphical distribution of pixels. The pixels are distributed unevenly in original digitized medical image as shown in Figure 3a. In the cipher image, pixels are distributed uniformly as shown in Figure 3b. From Figure 3b, it is observed that the graphical distribution of pixels of cipher image is totally different from that of original digitized medical image. The histogram of the decrypted medical image is shown in Figure 3c. From Figure 3c, it is observed that the graphical distribution of the pixels is similar in both the original digitized medical image and decrypted digitized medical image.

4.2. Differential attack

In differential attack, attackers study the cipher image to extract information about the plain image. The unified average changed intensity (UACI) and a number of changing pixel rate (NPCR) methods are used to verify differential attack.

4.2.1. NPCR and UACI

In differential attacks, the NPCR and UACI are decisive factors employed to determine the resist against pixel change rate. During transmission of digitalized medical image, the attacker can access cipher image and try to get keys and plain medical image. But in the proposed method, only ten-pixel values of the medical image are modified and encrypted. The cipher image of the changed pixel value is totally different from the original cipher image. This pixel change rate is calculated using NPCR is defined in (9).

$$NPCR = \frac{\sum_{m,n} D_1(m,n)}{W_1 \times H_1} \times 100\% \tag{9}$$

where W_1 and H_1 are width and height of the digital medical image and D_1(m, n) is defined as

$$D_1(m,\ n) = \begin{cases} 0, & if\, I_{ee}(m,\ n) = I_e(m,\ n) \\ 1, & if\, \mathrm{I}_{ee}\,(m\ \ n) \neq I_e(m,\ n) \end{cases} \tag{10}$$

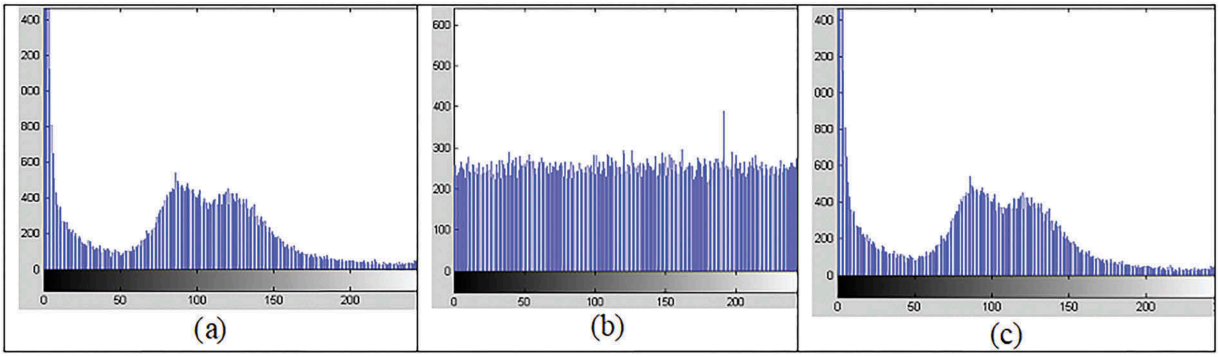


Figure 3. Histogram of (a) Original digitized image, (b) Cipher image, and (c) Decrypted digitized medical image.

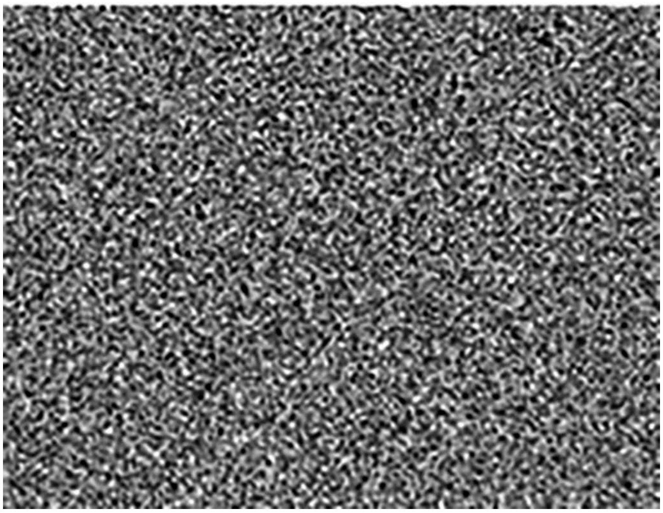


Figure 4. Decrypted digitized image using wrong key.

The UACI is defined in Eq. (11)

$$UACI = \frac{1}{W_1 + H_1}\left[\sum_{m,n}\frac{|I_{ee}(m,\ n) - I_e(m,\ n)|}{255}\right] \times 100\,\% \tag{11}$$

where I_e and I_{ee} are two ciphered images obtained from an original digitized image and ten-pixel value changed original digitized medical image, respectively.

4.3. MSE and PSNR

The quality of the digital medical image is checked using PSNR and MSE metrics. The MSE measures the resemblance among the original digitized medical image and encrypted digitalized medical image. The value close to zero represents more similarity and higher value means less similarity. The MSE calculates approximately the average of squared errors between the original digital medical image 'I_o' and ciphered medical digitalized image 'I_e'. The MSE is defined in Eq. (12).

$$MSE = \frac{\sum_S [I_O(m,\ n) - I_e(m,\ n)]^2}{S} \tag{12}$$

The PSNR is used to verify that the addition of noise during transmission affects the importance of the digitalized medical image. The lowest value of PSNR indicates a better encryption technique. The PSNR is defined in Eq. (13).

$$PSNR = 10\log_{10}\frac{(256 - 1)}{MSE} \tag{13}$$

where S represents a size $(m \times n)$ of the digitized medical image.

4.4. Entropy

The quality of the encryption algorithm is measured by entropy value. The entropy is the measurement of the probability distribution of gray levels all through the image. The higher value of entropy indicates a uniform distribution of gray levels. The gray levels distributed uniformly means, pixels are shuffled in such a way that it is highly impossible for invaders to predict a small part of the plain medical image. Hence, the higher value of entropy indicates good confusion property. The entropy is defined by (14).

$$\mathrm{H(U)} = \sum_{i=0}^{255} \mathrm{p}(u_i) log_2 \mathrm{p}(u_i) \tag{14}$$

where $\mathrm{p}(u_i)$ represents the probability of distribution of gray level of the encrypted digitized medical image.

4.5. Exhaustive attack

The exhaustive attack is also known as a brute force attack. The attackers try to reveal the secret keys using the exhaustive search. The keyspace analysis and key sensitivity analysis are used to verify the exhaustive attack.

4.5.1. Key space analysis

In the SDMIE algorithm, the initial values of control factors and system parameters of dual hyperchaos map are used as a secret key. In the proposed algorithm, eight secret keys (K, $\mathrm{x_n}$, $\mathrm{y_n}$, a, b, c, d, l) are used. According to IEEE floating-point standard, the computational precision of the 64 bit double data is 10^{-15}. The keyspace of the proposed scheme is $(10^{15})^8 = 10^{120} \approx .2^{399}$. The space of the security key is vast enough to validate the exhaustive attack.

4.5.2. Key sensitivity analysis

The dual hyperchaos map is very perceptive to preliminary conditions of control factors and system parameters. The small alteration in initial values leads to highly impossible in recovering original digitalized medical image in decryption technique. To verify the key sensitivity analysis, cipher image is deciphered with incorrect key $\mathrm{x_n}$ = 0.00000001 as a substitute for $\mathrm{x_n}$ = 1. The deciphered digital medical image is entirely diverse than the original digitized medical image as shown in Figure 4. The remaining parameters of secret keys are also extremely sensitive.

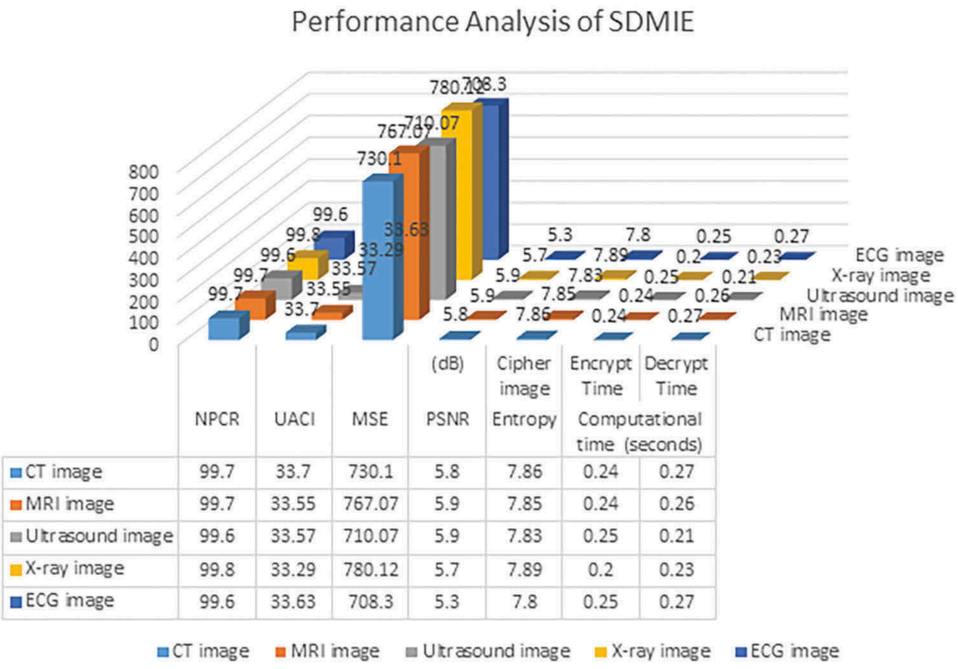
4.6. Performance analysis

The performance analysis of the SDMIE method is shown in Figure 5. From Figure 5, it is found that the value of NPCR is near to 99.68% and the value of UACI is close to 33.55%. The values are almost equal to the ideal value of NPCR >99% and UACI ≈ 33% (Ravichandran, Praveenkumar, Rayappan, and Amirtharajan (2017)). In the proposed SDMIE method, the value of MSE is near to 739.132 and the value of PSNR is near to 5.72 dB, which means the quality of encryption technique is good. The entropy value shows the uniform distributions of gray levels. For ciphered image, it is approximately equal to 7.8466, near to ideal entropy value of 8.0. The proposed SDMIE method provides efficient security. We have calculated computational time, the time required for encryption and decryption process as 0.236, 0.248 seconds respectively.

The 3000 pixels of a digitized medical image is selected horizontally, vertically and diagonally to verify the correlation coefficient of adjacent pixels. Table 2 shows the average correlation coefficient value for 100 images of each category. From Table 2, it is found that adjacent pixels are highly correlated in decrypted digitized medical image and less correlated in an encrypted medical image. The average correlation coefficient value for an decrypted digitized image is 0.9946 and the encrypted medical image is 0.00154. Hence, the proposed SDMIE algorithm is appropriate to transmit the digital medical image through timid channels.

4.7. Comparative analysis of SDMIE method

The proposed SDMIE algorithm is compared with some of the methods discussed in the literature survey. The comparative analysis is shown in Table 3. From Table 3, it is observed that the NPCR, UACI, and correlation coefficient of SDMIE system are almost equal or greater than other methods. The comparative analysis proves that it is impossible for attackers to decrypt the



	NPCR	UACI	MSE	(dB) PSNR	Cipher image Entropy	Encrypt Time	Decrypt Time
						Computational time (seconds)	
■ CT image	99.7	33.7	730.1	5.8	7.86	0.24	0.27
■ MRI image	99.7	33.55	767.07	5.9	7.85	0.24	0.26
■ Ultrasound image	99.6	33.57	710.07	5.9	7.83	0.25	0.21
■ X-ray image	99.8	33.29	780.12	5.7	7.89	0.2	0.23
■ ECG image	99.6	33.63	708.3	5.3	7.8	0.25	0.27

Figure 5. Performance analysis of SDMIE method.

Table 2. Correlation coefficient for SDMIE method.

		Correlation coefficient	
Medical image		Encrypted image	Decrypted image
CT image	**Horizontal**	0.0196	0.996
	Vertical	0.0178	0.999
	Diagonal	0.0169	0.997
MRI image	**Horizontal**	0.0159	0.995
	Vertical	0.0162	0.992
	Diagonal	0.0168	0.996
Ultrasound image	**Horizontal**	0.0153	0.994
	Vertical	0.0153	0.992
	Diagonal	0.0146	0.992
X-ray image	**Horizontal**	0.0194	0.995
	Vertical	0.0195	0.995
	Diagonal	0.0195	0.996
ECG image	**Horizontal**	0.0121	0.993
	Vertical	0.0135	0.996
	Diagonal	0.0181	0.991

Table 3. Comparative analysis of NPCR, UACI, and correlation coefficient for encrypted Lena image.

	NPCR	UACI	Correlation coefficient		
Methods	(%)	(%)	Horizontal	Vertical	Diagonal
Meng, Z.Y et al.	99.61	33.46	−0.0013	−0.0274	−0.0199
Krishnamoorthi, R et al.	99.62	27.38	0.038	0.019	0.065
SDMIE (proposed method)	**99.87**	**33.29**	**0.0198**	**0.0213**	**0.0187**

original digitized medical image and identify secret keys after studying the cipher image. Hence, the proposed SDMIE provides efficient security for digitized medical image.

To reduce the computational time in the SDMIE algorithm, selected pixels obtained using Pixel_selection Algorithm 1 are scrambled instead of shuffling all pixels. The time required for encryption and decryption of the proposed SDMIE method is compared with other methods in Table 4. From Table 4 it is observed that the proposed SDMIE algorithm takes less computational time compared with other methods in the literature.

In (Akkasaligar & Biradar, 2016) for encryption, all pixels of digital medical images are encoded using DNA rules. This method requires absolutely time complexity of O(n^2 × 4) for DNA encoding in level-1. All pixels are shuffled using a chaotic map in level-2 requires absolutely time complexity O(n^2 × 4). The proposed SDMIE algorithm requires less time complexity almost equal to O((n^2/2) × 4)). Because in the proposed SDMIE algorithm, instead of shuffling all pixels of the digital medical images only selected pixels are shuffled in permutation round.

5. Conclusion

In this paper, a selective digitalized medical image encryption using dual hyperchaos map and DNA sequencing is proposed. Initially, the original medical digitized image is renovated into selected pixel

Table 4. Comparison of computational time of SEDMI with other methods.

Methods	Encryption time (seconds)	Decryption time (seconds)
SDMIE (proposed method)	**0.22**	**00.36**
One-time pad (Gehani, LaBean, & Reif, 2003)	2.00	10.00
GSCS (Santoshi, Kranthi, Gowripushpa, & Mishra, 2016)	4.16	22.93
Zaslavsky chaotic system (Hamza and Titouna (2016))	0.32	–

DNA-encoded matrix C_1 and remaining pixel DNA-encoded matrix C_2 using all DNA rules based on the pixel index value. The chaotic sequences are produced using parameters and system factors of the dual hyperchaotic map. The dual hyperchaotic map is employed to muddle the selected pixels of encoded DNA matrix C_1. The DNA XOR method is employed to merge the scrambled DNA-encoded matrix C_1 and DNA-encoded matrix C_2. The combined DNA-encoded matrix is converted into binary image using all DNA decoding rules and is converted into grayscale image to get cipher image. The performance analysis illustrates that a proposed SDMIE algorithm enhances the security level and also inhibits differential, exhaustive and statistical attacks. The proposed SDMIE method takes less computational time (i.e., 0.236 s) and is suitable for telemedicine, smart health, and e-health applications.

ORCID

Sumangala Biradar http://orcid.org/0000-0002-6261-5495

References

Akkasaligar, P. T., & Biradar, S. (2016, December). Secure medical image encryption based on intensity level using Chao's theory and DNA cryptography. In *Computational* Intelligence *and Computing* Research *(ICCIC), 2016 IEEE International Conference on* (pp. 1–6), Chennai, India. doi:10.1109/ICCIC.2016.7919681

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

Fu, C., Li, W. J., Meng, Z. Y., Wang, T., & Li, P. X., (2013, December). 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

Gehani, A., LaBean, T., & Reif, J. (2003). DNA-based cryptography. In Natasa, Jonoska Gheorghe, Paun Grzegorz, Rozenberg (Eds.), *Aspects of Molecular Computing* (pp. 167–188). Berlin, Heidelberg: Springer. doi:10.1007/978-3-540-24635-0_12

Hamza, R., & Titouna, F. (2016). A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. *Information Security Journal: A Global Perspective*, *25* (4–6), 162–179. doi:10.1080/19393555.2016.1212954

Hiremath, P., Prema, T. A., & Sharan, B. (2013). *Speckle noise reduction in medical ultrasound images, Advancements and breakthroughs in ultrasound images*. Crotria, England and Wales: InTech Publishers.

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

Kester, Q. A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., & Quaynor, N. N. (2015). A cryptographic technique for security of medical images in health information systems. *Procedia Computer Science*, *58*, 538–543. doi:10.1016/j.procs.2015.08.070

Krishnamoorthi, R., & Murali, P. (2014, February). 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

Lima, J. B., Madeiro, F., & Sales, F. J. R. (2015). Encryption of medical images based on the cosine number transform. *Signal Processing: Image Communication*, *35*, 1–8. doi:10.1016/j.image.2015.03.005

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

National library of medicine's open access biomedical images search engine. Retrieved from https://openi.nlm.nih.gov

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

Santoshi, G., Kranthi, T., Gowripushpa, G., & Mishra, T. K. (2016). Novel approach of DNA sequencing algorithm to image security. 2016 *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)* (pp. 1501–1505), Paralakhemundi, India. doi:10.1109/SCOPES.2016.7955690

Sebastian, A., & Delson, T. R. (2016). Secure magnetic resonance image transmission and tumor detection techniques. *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT*) (pp. 1–5), Nagercoil, India. doi:10.1109/ICCPCT.2016.7530277

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