EasyChair Preprint

№ 8539

2D-CTM and DNA-Based Computing for Medical Image Encryption

Mobashshirur Rahman and Piyush Kumar

July 25, 2022

2D-CTM and DNA-based Computing for Medical Image Encryption

Mobashshirur Rahman[1] and Piyush Kumar[2]

[1] National Institute of Technology Patna
mobashshirurrahman@gmail.com*
[2] National Institute of Technology Patna
piyush.cs@nitp.ac.in

Abstract. Medical imaging plays an important role in the proper treatment of a patient's disease. Nowadays, the virtual diagnosis of patients is becoming popular, so these images are sent from one place to another via the network for diagnosis purposes. So, the medical images need to be secured from any illegal access and modification. To handle this situation, a novel key generation with medical image encryption and decryption algorithms is proposed based on chaos, DNA computing, and Mersenne Twister (MT). The key is generated using a proposed new 2D-Chaotic Tan Map (2D-TCM). Then, the image is passed through two levels of confusion and diffusion based on DNA computing, chaos, and MT to get a final, highly secured encrypted image. Extensive comparative evaluation of the results is performed on X-ray images and MRI images using different security metrics, such as key space, key sensitivity, histogram analysis, entropy and correlation analysis. The results show that the proposed model achieved a better result in comparison to other related techniques.

Keywords: DNA · chaotic map · Medical image · encryption · Security

1 Introduction

Nowadays, after the breakthrough of the novel covid-19, the treatment of patients virtually is of utmost popularity. When examining the patient virtually the medical image plays an important role in the proper diagnosis of the patient's disease. Medical images are also important for analysis and research purposes. There are many modalities of medical images which are currently popular, such as Magnetic Resonance Imaging (MRI), X-ray, Computed Tomography (CT), and ultrasound. However, it is also important to protect these medical images from cyber attackers. The attackers may use medical images to leak the privacy of patients or also alter the data, which may lead to false diagnoses. Another concern related to medical image is its increasing size day by day. Due to its large size, there is a need to handle storage costs efficiently. Therefore, there are many schemes related to securing the medical images that are proposed, such as image steganography [1], image watermarking [2], and image encryption [3].

In all of these schemes, currently, the encryption method is the most popular for securing the data. In the encryption technique, the data is changed into some unreadable or unrelated data using a private key, then it is sent over the internet to the receiver side. On the receiving end, the receiver also required the private key to decrypt the data. DNA computing [4], Chaos and cryptography are frequently used together to provide security. The chaotic maps are used for generating different sequences, which are subsequently used in the confusion and diffusion processes in cryptography. The chaotic map can have different types based on the number of space dimensions, space domains, and time domains.

A number of technique is proposed for securing the medical image using encryption process. Ravichandran et al. [5] proposed DNA and chaos-based image encryption. In this paper, two levels of confusion and diffusion are performed. The shuffling of block-level with row and column level pixel values followed by a DNA-based XOR operation is performed to get the encrypted image. Belazi et al. [6] have proposed a novel medical image security algorithm based on DNA encoding, SHA-256 and bit-level pixel confusion and diffusion. The logistic-Chebyshev chaotic map and sine-Chebyshev chaotic map are used for generating key streams. Extensive result analysis is carried out using different security metrics. The algorithm has achieved better time complexity as well in comparison to other existing algorithms. However, the author has not considered the issue related to the storage cost of medical images. Y. Zhang [7] proposed a new DNA and chaos-based image encryption algorithm. In this paper the author has used piecewise linear chaotic map (PWLCM) to generate key sequences. Two levels of DNA-based confusion and diffusion are performed to get the final encrypted image.

Traditional approaches have several disadvantages: high algorithm complexity, lack of propoer evaluation, and encryption time. A novel model based on Deoxyribo Nucleic Acid (DNA), Mersenne Twister (MT), and 2D-chaotic Tan map is proposed to efficiently secure the medical image from cyber attacks. In this approach, two levels of confusion and diffusion are performed based on the proposed 2D-Chaotic Tan Map (2D-CTM) equation, and DNA computing is performed to get the final cipher image.

The major contribution of this proposed approach can be summarized as:

- A new 2D chaotic map is proposed for generating private keys for confusion and diffusion processes.
- In the proposed method, a private key is employed for confusion, followed by DNA-based diffusion with the private key. Finally, MT-based confusion is performed to get the final encrypted image.
- Comparative result analysis is carried out using different security measures, such as entropy, key space, differential attack, correlation analysis, and robustness analysis. The result showed that the proposed model outperforms the other existing related models.

The paper has 4 sections. The next section is the proposed methodology section. Section 3 has the results and discussion part. And finally, the paper is concluded in section 4.

2 Methodology

Medical images are sent over the internet and kept on servers for diagnosis and analysis purposes. However, there is a need to secure medical images from unauthorized access or modification. Therefore, a novel algorithm is proposed for efficiently securing digital images on the internet from cyber-attacks. In this approach, two levels of confusion and diffusion of the original image are performed using a new 2D-chaotic map, DNA computing, and MT, to get a highly secure encrypted image.

2.1 Key Generation

Key generation is the most important step for getting a secure encrypted form of the original image. In this approach, a new 2D-chaotic map is designed to generate the key stream. The 2d-Chaotic Tan Map (2d-CTM) is given by the following equation.

$$\begin{cases} p_{n+1} = k + p_n * tan(m) \ mod \ 1, \\ q_n = k + m * (1 - p_{n+1} * tan(m)) \ mod \ 1, \end{cases} \tag{1}$$

where p_n, k and m is the initial control parameter value.

In the above equation, the first initial value for p_n, k, and m is chosen to obtain the initial sequence. Using this map, two sequences are generated, named as X1 and Y1. The X1 is used for the diffusion process and the Y1 is used for the confusion process in this algorithm. The algorithmic steps for the key generation are shown in Algorithm 1.

Algorithm 1: Proposed key Generation steps.

Input : s, k, and m are initial control parameter. Also, give desired size of the key as parameter

Output: Secret keys sequences, X1 and Y1 *key* of given size

Function `GenerateKey(`M_i`):`

- X1 ← *initialize empty array for key sequence 1*
- Y1 ← *initialize empty array for key sequence 2*
- **for** *i in range(size)* **do**
  - $s = k + ((s) * tan(m)) \ \% \ 1$
  - $X1.append(int((s * pow(10, 10)) \ \% \ (256)))$
  - $s = k + (m * (1 - s * sin(m))) \ \% \ 1$
  - $Y1.append(int((m * pow(10, 10)) \ \% \ (256)))$
- **end**
- return X1, Y1

2.2 Encryption

The Encryption is the final step for generating the cipher image from its original form. So, after the successful generation of the private key, the encryption is

performed. First, a pixel level shuffling of the original image is performed using the Y1 sequence generated using 2D-CTM.

$$S\_image[Y1[i]] = Original\_image[i]$$

where S_image denote modified image, Original_image is the original image, and i denotes the index value.

After getting the shuffled image, encode the pixels of the image into DNA sequences using rule Rule 1. Also, encode the value of key X1 into the DNA sequence.

$$Rule\ 1 \leftarrow (Key[i]\%8) + 1$$

$$Rule\ 2 \leftarrow (i\%8) + 1$$

where, i $\in$ integer and key is private encryption key. After converting the values of

Table 1: DNA BASED RULE FOR ENCODING AND DECODING

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

both images and keys to DNA sequences, perform a DNA-based XOR operation to obtain a diffused image.

Table 2: RULE FOR XOR OPERATION OF DNA SEQUENCES

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

Now, after the diffusion process, decode the DNA sequence back to the integer values. Now, perform MT-based confusion of the cipher image [8]. Finally, the XOR operation is performed among the sum of pixels of the original image, X1 and the cipher image to get a highly secured final encrypted image. The complete block diagram of encryption process is shown in Fig. 1.

2.3 Decryption

The reverse step of encrytion needs to be followed to recover the original image from its encrypted form. First, reshuffling of pixels is performed based on the Y1 sequence. Then perform DNA-based encoding of pixels. The DNA-based XOR operation is carried out with the X1 key. After that, decode the pixels of the image into integers. Now, reshuffle using the MT-based sequence used during encryption. Finally, perform an XOR based operation between the image, X1, and the sum of pixels of the original image to get back the original image.

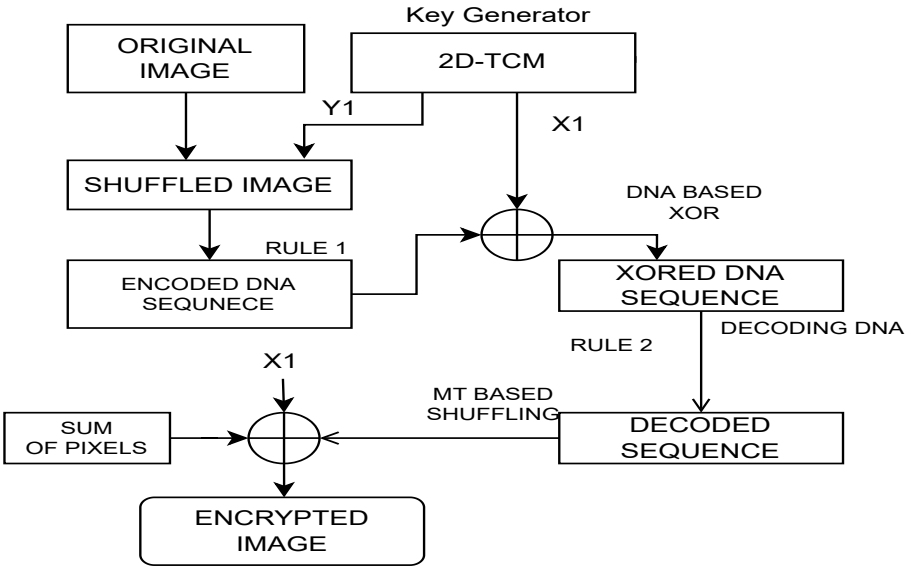

Fig. 1: Proposed Encryption flow

3 Performance Analysis

A novel medical image encryption technique is proposed based on chaos, MT, and DNA computing. The 2D-CTM is used for key generation, and a DNA-based operation is performed to get the final encrypted image. The performance of the proposed model is evaluated thoroughly using different security evaluation metrics.

3.1 Experimental Setup And Dataset Details

The proposed scheme is tested on an Asus laptop with an Intel Core i5 processor, 8GB of RAM, a 512 GB SSD hard disk, and a 4GB Nvidia graphics card. The result evaluation is performed using different madalities of medical images, namely, X-ray and MRI images. All these images are taken from the Medpix website [9].

3.2 Results and Discussion

2D-Chaotic Tan Map (2D-TCM) In this subsection the discussion of 2D-TCM and related chaotic map is performed.
The Sine map [10] is chaotic 1D map which can be described by the following equation.

$$S_{n+1} = \mu sin(\pi S_n) \tag{2}$$

where $\mu \in [0.87, 1]$ for chaotic behaviour.

Algorithm 2: Image Encryption

Input : Medical images M_i, where $i = 1, 2, 3...n$, and Key X1,Y1 along with their DNA encoded values

Output: Encrypted images C_i, where $i = 1, 2, 3...n$.

Function `Encrypt_Image(`M_i`)`**:**

- $Y1, X1 = 2D - CTM()$
- $sequence_2 = Mersenne\_Twister()$
- sum $\leftarrow$ *sum of pixels of original image*
- $R_1 \leftarrow (Key[i]\%8) + 1$
- $R_2 \leftarrow (i\%8) + 1$
- $DNA_{Ri} \leftarrow$ *Encodepixel with rule* R_i
- $Decode_{Ri} \leftarrow$ *DecodeDNA with rule* R_i
- size = M*N
- $X1_{DNA} \leftarrow$ *DNA based encode form of key X1*
- **for** *i from 0 to size)* **do**
  - $S\_image\,[Y1[i] - 1] = M_i[i]$
- **end**
- **for** *i from 0 to size* **do**
  - Encode_dna[i] = DNA_{R1}
- **end**
- **for** *i from 0 to size* **do**
  - Encode_dna[i] = Encode_dna[i] *XOR* $X1_{DNA}[i]$
- **end**
- **for** *p in Encoded_dna* **do**
  - Enc_dna= $Decode_{R2}$
- **end**
- **for** *j from 0 to size* **do**
  - $Encrypted\_image\,[sequence_2[j] - 1] = Enc\_dna[j]$
- **end**
- **for** *j in range(M*N)* **do**
  - $Cipher\_image\,[j] = Cipher\_image\,[j] \oplus X1 \oplus (Sum\,\%\,256)$
- **end**
- return C_i

A new 2D map is proposed which also based on trignometry $tan(x)$, which is given by the following equation.

$$\begin{cases} p_{n+1} = k + p_n * tan(m)\ mod\ 1, \\ q_n = k + m * (1 - p_{n+1} * tan(m))\ mod\ 1, \end{cases} \tag{3}$$

where p_n, k and m is the initial control parameter value.

Here, each time initial value p_n get updated and added to the key sequence. Now, the bifurcation diagram is drawn for the Sine map and the 2D-CTM in Fig. 2(a) and Fig. 2(b) respectively. It can be seen that the proposed 2D-CTM has no pattern as compared to the Sine map. Thus, the 2D-CTM is very sensitive

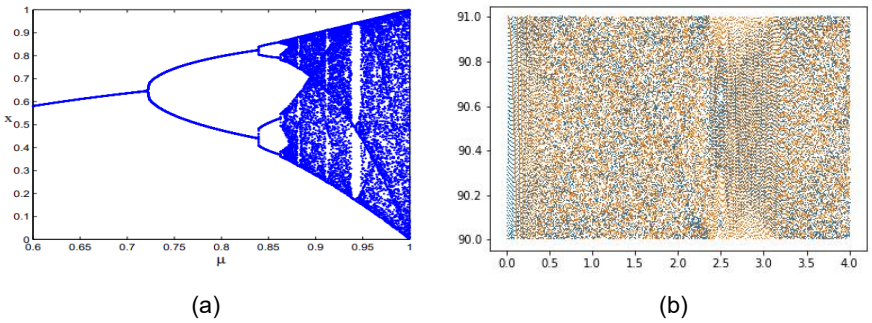

Fig. 2: Bifurcation diagram of (a) Sine map and (b) 2D-CTM

to initial conditions as well. Now the Lyapunov Exponent (LE) is calculated for 2D-CTM and it is shown in Fig. 3.

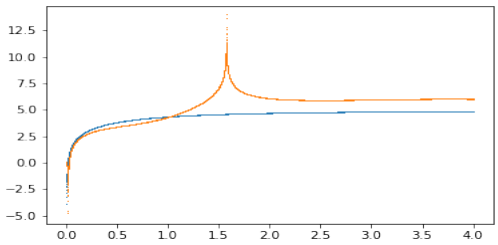

Fig. 3: Lyapunov exponent diagram of 2d-CTM in range [0,4]

The LE of 2D-CTM has a positive value just above 0 and is positive. And a positive LE means the map is chaotic at that point. So, the proposed map has a large range of chaotic behaviour from $(0 - \infty)$. Thus, the sequence generated using 2D-CTM has more chaotic behavior and an unpredictable trajectory. So, it can be perfectly used for the key generation process.

Key space Key space is defined as the total size of the key used for the encryption process. It determines the restiveness of the model against exhaustive search attacks. In the 2D-CTM based key generation process, the initial parameters p_n, k, and m have a precision of at least 2^{14}. So, the resulting key space becomes $(10^{14})^3 = 10^{42}$, which is large enough to prevent exhaustive search attacks [10]. Thus, the key generated by the proposed model has a restiveness towards exhaustive search attacks.

Key Sensitivity The key sensitivity shows the susceptible algorithm with a slight modification in key value. The 2D-CTM is highly sensitive to a minute change in the initial parameters of the key. For evaluation of 2D-CTM towards

key sensitivity, a secret key is generated with an initial parameter of $p_n = 0.93$, k = 90, and u = 4. And the given image is encrypted. Now, again the decryption key is generated, keeping all the parameters the same except slightly modifying the value of p_n from 0.93 to 0.930000000000001. Now, with this key, the decryption is carried out. The result of decryption is shown in Fig. 4. And it is clearly visible that with a slight modification to the initial parameters, the decryption process completely failed.

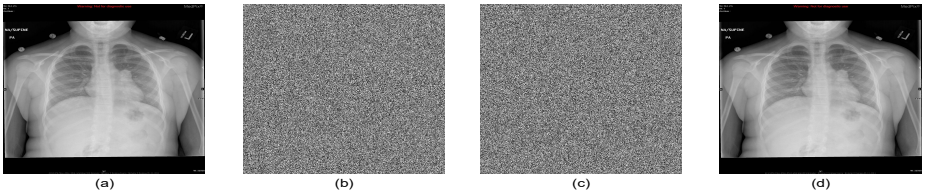

Fig. 4: (a) Original image, (b) encrypted image with p = 0.93, (c) decrypted image with slight modification in p value as 0.930000000000001, and (d) decrypted image with correct p value

Histogram Analysis The histogram analysis shows the frequency of different pixel values. If the pixel distribution of the cipher image is uniform, this means that the cipher image can prevent statistical attacks as the attackers are not able to find any pattern in the image. Fig. 5 shows the histograms of original images and their corresponding cipher images.

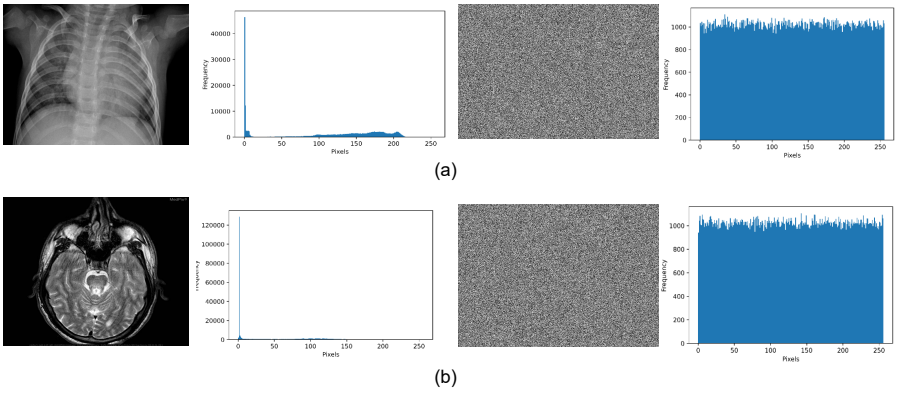

Fig. 5: Histogram of original image and its corresponding cipher image for (a)x-ray image, and (b) MRI image

Entropy Information entropy measures the level of randomness present in the cipher image. It is calculated using Eq. 4. The ideal value of entropy is 8. The entropy value for the cipher images of X-ray and MRI is calculated as 7.9992 and 7.9993, which is very close to the ideal value. Table 3 shows the comparative

analysis of the information entropy of the proposed scheme with other related schemes.

$$IE(x) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i). \tag{4}$$

where IE stands for Infomation Entropy, and p(xi) is probability of pixel x_i in the image.

Table 3: INFORMATION ENTROPY COMPARATIVE ANALYSIS FOR CIPHER IMAGES

Method	Guan et al.[11]	T. Akkasaligar and S. Biradar [12]	2D-CTM
Entropy	7.992	7.890	7.999

Correlation Analysis Corrlation analysis determines the way in which adjacent pixels are related to each other. If there is a pattern among pixels, then the attackers may launch an attack using this pattern. So, ideally the correlation coefficient should be 0, i.e., it means there is no correlation between adjacent pixels. The correlation of the X-ray and MRI images is calculated and the comparative result is shown in Table 4.

Table 4: PERFORMANCE COMPARISON FOR CORRELATION COEFFICIENTS

Methods	**Correlation**		
	Horizontal	**Diagonal**	**Vertical**
Guan et al.[11]	0.0011	0.0001	-0.0002
T. Akkasaligar and S. Biradar [12]	0.0194	0.0195	0.0195
2D-CTM	0.0009	-0.0002	-0.0021

4 Conclusion

A novel algorithm based on DNA computing, chaotic map, and Mersenne twister is proposed for securing medical images from cyber attacks. In the proposed algorithm, a new chaotic map, 2D-CTM, is proposed to generate a private key for the confusion and diffusion process. After key generation, the encryption process is carried out by performing confusion based on sequences generated by 2D-CTM followed by DNA encoding. The DNA based XOR operation is carried out between the key and the DNA encoded image. Then, the image is decoded and MT-based shuffling is performed. Finally, the XOR-based encryption is performed among the image, key, and sum of pixels of the original image, to get a highly-secured encrypted image. The comparative result evaluation is performed on X-ray images and MRI images considering different security metrics, such as key space, histogram analysis, key sensitivity, entropy, and correlation analysis. The result of the proposed model achieves a better result than other existing models.

Bibliography

[1] V. K. Sharma, P. C. Sharma, H. Goud, and A. Singh, "Hilbert quantum image scrambling and graph signal processing-based image steganography," Multimedia Tools and Applications, vol. 81, no. 13, pp. 17817–17830, 2022.

[2] M. S. Moad, M. R. Kafi, and A. Khaldi, "A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications," Microprocessors and Microsystems, vol. 90, p. 104490, 2022.

[3] A. Toktas and U. Erkan, "2D fully chaotic map for image encryption constructed through a quadruple-objective optimization via artificial bee colony algorithm," Neural Computing and Applications, vol. 34, no. 6, pp. 4295–4319, 2021.

[4] S. Namasudra, R. Chakraborty, A. Majumder, and N. R. Moparthi, "Securing multimedia by using DNA-based encryption in the Cloud Computing Environment," ACM Transactions on Multimedia Computing, Communications, and Applications, vol. 16, no. 3s, pp. 1–19, 2021.

[5] D. Ravichandran, A. Banu S, B. K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain," Medical amp; Biological Engineering amp; Computing, vol. 59, no. 3, pp. 589–605, 2021.

[6] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," IEEE Access, vol. 7, pp. 36667–36681, 2019.

[7] Y. Zhang, "The image encryption algorithm based on chaos and DNA computing," Multimedia Tools and Applications, vol. 77, no. 16, pp. 21589–21615, 2018.

[8] Matsumoto, M., and Nishimura, T, "Mersenne twister: a 623-dimensionally equidistributed uniform pseudorandom number generator" ACM Transactions on Modeling and Computer Simulation (TOMACS), vol.8, no.1, pp. 3-30, 1998.

[9] "MedPix," U.S. National Library of Medicine. [Online]. Available: https://medpix.nlm.nih.gov/home. [Accessed: 04-May-2022].

[10] A. Mansouri and X. Wang, "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme," Information Sciences, vol. 520, pp. 46–62, 2020.

[11] M. Guan, X. Yang, and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," IET Image Processing, vol. 13, no. 9, pp. 1535–1539, 2019.

[12] P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using DNA cryptography," Information Security Journal: A Global Perspective, vol. 29, no. 2, pp. 91–101, 2020.