J. Inst. Eng. India Ser. B (April 2024) 105(2):183–190
https://doi.org/10.1007/s40031-023-00962-4

ORIGINAL CONTRIBUTION

A Parallel DNA Crypto Algorithm for Medical Image

Sumangala Biradar[1] · Prema T. Akkasaligar[2] · Sunanda Biradar[3]

Received: 16 October 2021 / Accepted: 17 November 2023 / Published online: 21 December 2023

Abstract In health care, due to COVID-19 pandemic, doctors and patients are preferring online tele consultancy. In online tele consultancy, diagnosis of the disease is on the basis of online communication and digital images. Wireless communication is good, but the security breach is a crucial problem. To prevent a security breach, various cryptography algorithms are used. The computational complexity of these algorithms is excessive. Hence, the major research issue in health care is the embellishment of security with lowered time complexity. In this paper, we proposed a parallel DNA crypto algorithm to afford substantial security with decline in time complexity. The parallel task processing and parallel instructions processing with multithreads are exercised for parallel process. The medical image is segregated into four subparts, and parallelly, each subpart is remodelled into DNA strands using bit-level dynamic DNA coding pattern selection. Parallelly, all DNA strands pixels are scuffled by sequences of four-dimensional Chen's and Lorenz chaos theories to get confusion matrices. The DNA XOR is applied to obtain transform matrices. All transform matrices are concatenated to conquer a encipher image. Our algorithm's simulation exhibits incredible enhancement in the operational speedup. The findings of experiment also proved that the proposed security-level methodology is higher than other conventional algorithms.

Keywords Parallel computation · Multiple chaos theories · Multiple DNA operations · Multithreads

Introduction

The medical emergency has initiated everywhere due to COVID-19 epidemic. The clinicians are leaning towards teleconsultation. In teleconsultation, diagnosis of disease is based upon detailed images of the body organs. These images are broadcasted via open-source communication channels. Hence, the hackers can infringement the disease related data. For the clinicians, interpreting the accurate diseases from the penetrated information is impractical. So, substantial security is crucial for teleconsultation. Several cipher models using chaotic systems are existing. These model's computational efficiency is high and fail to fulfil security constraints of medical images. Thus, the major issue is how to fulfil security constraints with fast processing.

The parallel processing is a technique which processes multiple tasks simultaneously using multicore computer system. Hence, parallel encryption or decryption methods process the image faster than the sequential encryption or decryption methods.

In [1], the discretized Kolmogorov flow map parallel algorithm is presented. The mask transformation transforms the image into encipher image. In [2], parallel 3D

✉ Sumangala Biradar
biradarsumangala@gmail.com

Prema T. Akkasaligar
premasb@rediffmail.com

Sunanda Biradar
sunanda_biradar@rediffmail.com

[1] Department of Information Science and Engineering, BLDEA's V.P. Dr. P. G. Halakatti College of Engineering and Technology, Vijayapur, Karnataka 586103, India

[2] Department of Computer Science and Engineering, KLE Technological University's Dr. M.S. Sheshgiri College of Engineering and Technology, Belagavi Campus, Belgaum, Karnataka 590006, India

[3] Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning), BLDEA's V.P. Dr. P. G. Halakatti College of Engineering and Technology, Vijayapur, Karnataka 586103, India

hyperchaos and zigzag ordering transformation is developed to accomplish a encipher image. In [3], parallel cipher model is presented employing 1D and 2D hybrid logistic map. In [4], pixel-level parallel processing is implemented to speed up the run time of chaotic theory. In [5], a compressed sensing and chaos theory are proposed to encrypt images simultaneously.

In [6], the image is segregated into segments and each segment is encoded using AES (Advanced Encryption Standard) method. In [7], the author proposed encryption algorithm using a hyperchaotic system, pixel-level dynamic filtering, DNA and 3D Latin cubes operations. In [8], a "Two-dimensional Hénon-Sine map" (2D-HSM), DNA coding and XOR procedures are proposed to develop a encipher image.

In [9], three channels, namely red, green and blue, are excerpted from colour image. The simultaneous intra–inter-element rearrangement is presented to create the encipher image. In [10], image is altered into DNA strand. The random phase mask of Lorenz chaotic map is combined with DNA strand. The fractional Fourier transform is exploited for encrypting normal images. It is inadequate for medical images because of its large volume and contains very sensitive disease-oriented information. Hence, for medical images the computational complexity is extremely high. This problem can be resolved by taking benefit of parallel processing.

The summary of some more existing methods is highlighted in Table 1. The majority of cryptographic methods are [11, 12] either focus on to bring down the run time or enrich the security. The major research issue is to upgrade the security with lowered run time. Therefore, this survey motivates us to implement a parallel DNA crypto algorithm to maximize the security and to minimize the time complexity.

The substantial contributions of the proposed DNA crypto algorithm are specified below:

i. Reducing computational time

Minimizing the time complexity by developing parallel cipher model.

ii. Increase in key size

To enlarge the key size, individual keys are generated in each layer leading to multiple keys.

iii. Enrich the security

Implementing multiple DNA operations, 4D Chen's and Lorenz chaos theories to offer the substantial security for the medical images.

The further segment of the paper is systematized as: Sect. 2 is about the description of the proposed parallel DNA cipher model. The cryptanalysis is perpetrated in Sect. 3. The comparison work is perpetrated in Sect. 4. The conclusion part is covered in Sect. 5.

Proposed System

In the proposed DNA system, to maximize the security, the four-dimensional chaos theories and DNA functions are proposed as illuminated in Fig. 1. To minimize time complexity, parallel DNA crypto algorithm is proposed. The detail explanation of the cipher model is shown in Algorithm 1.

Algorithm 1: Parallel DNA cipher model.

//Input: The medical image I (m, n) of size $m \times n$.

//Output: The encipher image C(m, n) of size $m \times n$.

Start

Step 1: The medical image I (m, n) is subdivided into four subparts I1, I2, I3 and I4.

$$\mathrm{I1} = \mathrm{I}\,(1 : m/2, 1 : n/2);$$

$$\mathrm{I2} = \mathrm{I}((m/2) + 1 : m, 1 : n/2);$$

$$\mathrm{I3} = \mathrm{I}\,(1 : m/2, (n)/2 + 1 : n);$$

$$\mathrm{I4} = \mathrm{I}((m)/2) + 1 : m, (n/2) + 1 : n);$$

Step 2: Multithreads are generated to minimize the encryption time. One thread for a row is initiated, i.e. "m" threads for "m" rows. The co-workers of local cluster are assigned for parallel processing.

Step 3: Row-wise each subpart is renewed as a binary matrix by multithreads.

Table 1 Summary of existing methods

Author and Year	Method	Remarks
Habibpour et al. 2016 [11]	The 1D chaos theory reorders the image pixel. The parallelism features of GPU and CPU are developed to encrypt image	Overhead is low key space
Hu, Ting et al. 2017 [12]	A DNA cycle operation and multiple chaos theories are presented to modify and confuse the image pixels	Overhead is high computational speed

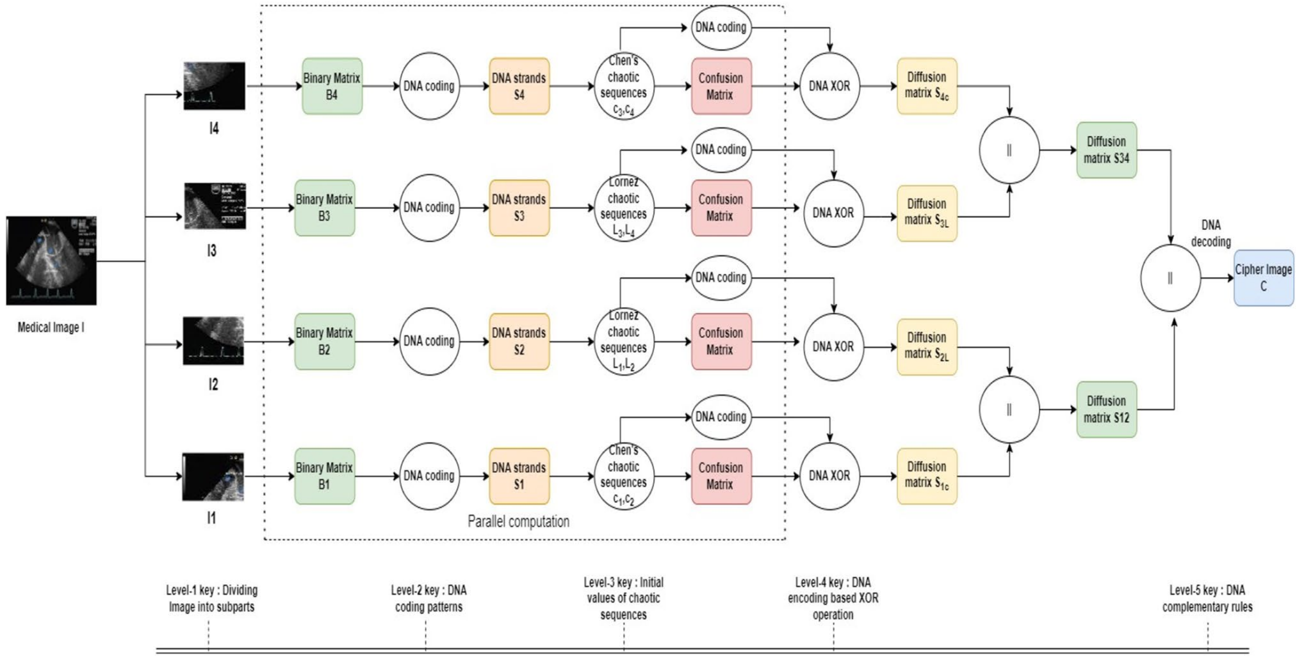

Fig. 1 Architectural design of parallel DNA encryption

$$\mathrm{B1} = \mathrm{dec2bin}\ (\mathrm{I1});$$

$$\mathrm{B2} = \mathrm{dec2bin}\ (\mathrm{I2});$$

$$\mathrm{B3} = \mathrm{dec2bin}\ (\mathrm{I3});$$

$$\mathrm{B4} = \mathrm{dec2bin}\ (\mathrm{I4});$$

Step 4: All DNA coding patterns specified in [13] are mapped to produce DNA stands for binary matrices simultaneously. The binary matrix 4-bit MSB are considered to opt DNA coding patterns dynamically as detailed in below table.

$$\mathrm{S1} = \mathrm{reshape\ B1};$$

$$\mathrm{S2} = \mathrm{reshape\ B2};$$

$$\mathrm{S3} = \mathrm{reshape\ B3};$$

$$\mathrm{S4} = \mathrm{reshape\ B4};$$

Step 5: The four-dimensional Chen's sequences c_1, c_2, c_3 and c_4 as indicated in [13] are sorted.

$$\overline{x} = \mathrm{sort}\left(\mathrm{c}_1\right);$$

$$\overline{y} = \mathrm{sort}\left(\mathrm{c}_2\right);$$

$$\overline{z} = \mathrm{sort}\left(\mathrm{c}_3\right);$$

$$\overline{w} = \mathrm{sort}\left(\mathrm{c}_4\right);$$

Step 6: The sorted sequences $\overline{x}$ and $\overline{y}$ positions are considered for transpose of S1, row by row and column by column, respectively. The sorted sequences $\overline{z}$ and $\overline{w}$ positions are considered for transpose of S4, row by row and column by column correspondingly by multithreads.

Step 7: The four-dimensional Lorenz's sequences L_1, L_2, L_3 and L_4 as indicated in [14] are sorted.

$$\overline{p} = \mathrm{sort}\left(\mathrm{L}_1\right);$$

$$\overline{q} = \mathrm{sort}\left(\mathrm{L}_2\right);$$

$$\overline{u} = \mathrm{sort}\left(\mathrm{L}_3\right);$$

$$\overline{v} = \mathrm{sort}\left(\mathrm{L}_4\right);$$

Step 8: The sorted Lorenz sequences $\overline{p}$ and $\overline{q}$ positions are considered for transpose of S2, row by row and column by column, respectively. The sorted Lorenz sequences $\overline{u}$ and $\overline{v}$ positions are considered for transpose of S3, row by row and column by column correspondingly by multiple threads.

Step 9: The sorted sequences are reconstructed as a DNA strands S*xy*, S*zw*, S*pq* and S*uv* by means of DNA coding patterns. DNA coding patterns are dynamically chosen as formulated in Table 2.

Step 10: The DNA XOR mentioned in [13] is utilized to modify the pixels of S1, S2, S3 and S4 individually.

$S_1c = \mathrm{S1\ DNA\ XOR\ S}xy;$

$S_{2L} = \mathrm{S2\ DNA\ XOR\ S}pq;$

$S_{3L} = \mathrm{S3\ DNA\ XOR\ S}uv;$

$S_{4c} = \mathrm{S4\ DNA\ XOR\ S}zw;$

Step 11: Modified DNA strands S_{1c}, S_{2L}, S_{3L} and S_{4c} are joined.

$S12 = S_{1c} || S_{2L};$

$S34 = S_{3L} || S_{4c};$

Step 12: The concatenated S12 and S34 are merged.

$S = S12 || S34;$

Step 13: Parallelly row-wise, DNA strand "S" is refurbished as a binary image "B" by DNA complementary patterns. The DNA strand 2-bit LSB are involved to select the DNA complementary patterns dynamically, as illuminated in Table 3.

Step 14: Binary image is altered into greyscale image to conquer a encipher image

C = bin2dec (B);

Stop

The decryption is the reversal of the encryption. At receiver end, parallel decryption algorithm is implemented to recover the medical image.

In this proposed parallel DNA encryption technique, a set of parallel pools are established. These parallel pools are called clusters. In each set of parallel pool, a group of workers are assigned to accomplish assigned task. The workers represent the multiple instances, which will run on individual cores. In MATLAB, we can run a local cluster of workers on the client machine itself. The local cluster means without server the task is performed on the same computer.

The mechanism of parallel instruction processing of the proposed DNA cipher model is illuminated in Fig. 2. The medical image is segregated into four subparts as explained in step 1 of Algorithm 1. For each subpart as shown in Fig. 2a, one parallel pool is assigned. The medical image subparts are transmuted as a matrix form in Fig. 2b. For each matrix, threads are produced row-wise and workers are allocated to run these threads parallelly in Fig. 2c. The DNA strand is conquered by referring DNA coding patterns in Fig. 2d. The four-dimensional Chen's and Lorenz sequences are exploited to transpose the DNA strands row by row in Fig. 2e. In Fig. 2f, the transposed DNA strands are amended row-wise by DNA XOR. The DNA complementary patterns are considered for conversion of modified DNA strands into binary matrix. The binary matrix is induced to construct a encipher image in Fig. 2g. The same procedure is performed parallelly for remaining subparts of the medical image. This parallel encryption takes place on the same computer, i.e. local cluster.

Experimental Results

The experiment is performed on ninth-generation Intel CoreT M i7 7500U CPU. The PubMed provided dataset for research purposes in "National Library of Medicine's Open Access Biomedical Images Search Engine" [15]. From the dataset, the 400 medical images of size 512 × 512 of four distinct types like ultrasound, MRI, X-ray and CT are considered for implementation. The 100 ECG images are contemplated from "ecgeducator.blogspot.com". The MATLAB (R2020b) parallel computing toolbox is exercised for the implementation of the proposed parallel DNA crypto algorithm. The medical image is unveiled in Fig. 3a and encipher image obtained using the proposed parallel DNA cipher model is unveiled in Fig. 3b. The decoded medical image is acquired by executing converse of parallel DNA cipher model and is unveiled in Fig. 3c.

Table 2 DNA coding patterns selection

MSB	1101 | 0010	1001 | 1010	1100 | 0110	0111 | 1000	1110 | 0101	0000 | 0001	0100 | 1111	0011 | 1011
DNA coding patterns	1	2	3	4	5	6	7	8

Table 3 DNA complementary patterns selection

LSB	TC|AG	CG|CC	GC|AT	TG|AC	TT|GA	GT|GG	CT|AA	TA|CA
DNA coding patterns in [14]	1	2	3	4	5	6	7	8

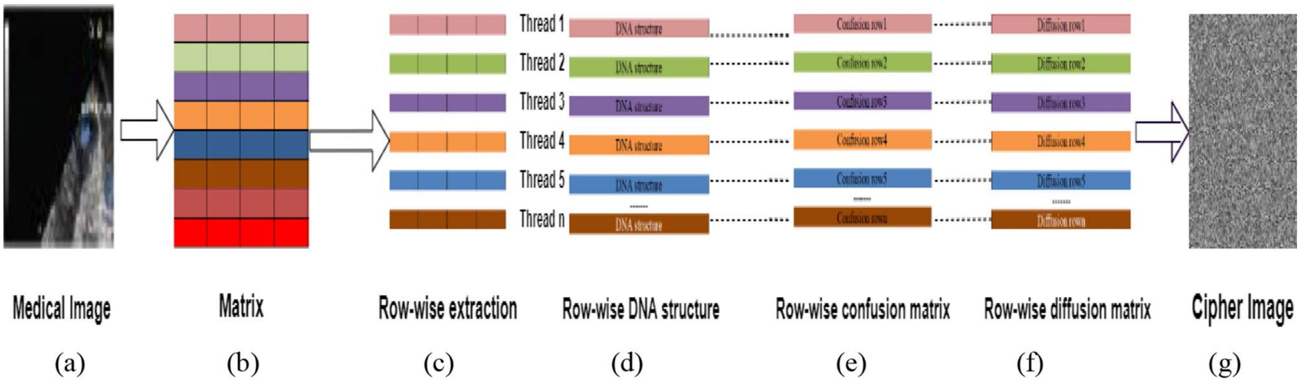

Fig. 2 Parallel compute mechanism of the proposed algorithm

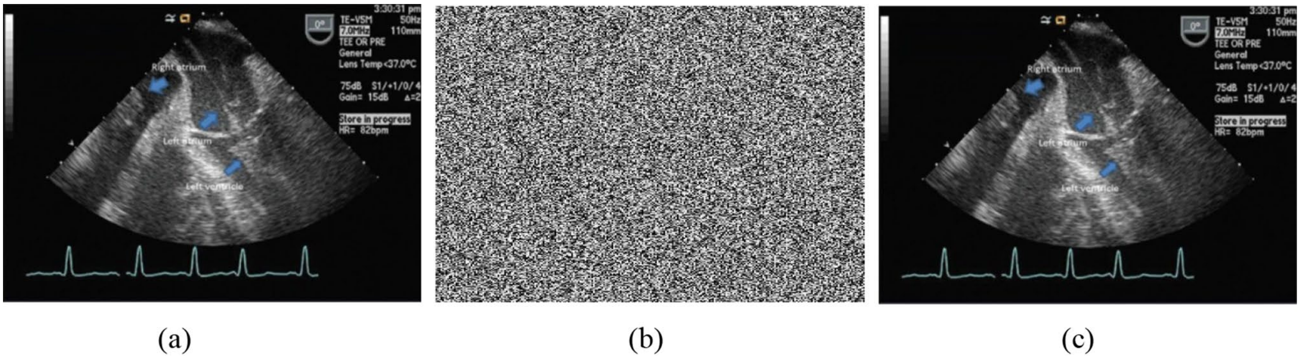

Fig. 3 **a** Sample medical image, **b** encipher image and **c** decipher image

Table 4 Performance of the proposed method

Medical image type	NPCR (%)	UACI (%)	Entropy	MSE	PSNR (dB)
MR	99.998	39.87	7.9999	5.9987e+04	3.4567
CT	99.997	35.79	7.9998	6.8528e+04	5.0100
X-ray	99.999	39.98	7.9999	5.9678e+04	4.0340
Ultrasound	99.995	39.96	7.9989	5.9987e+04	3.8998
ECG	99.996	37.99	7.9999	5.8976e+04	3.9956
Average	99.997	38.72	7.9997	6.14312e+04	4.07922

The proposed parallel algorithm is assessed by verifying the resistance against several attacks for example exhaustive attacks and differential attacks. The key space analysis specified in [14] is performed to prove thwarting against exhaustive attack.

The parameters “number of pixels change rate” (NPCR) and “unified average changing intensity” (UACI) are exploited to prove thwarting against differential attack. The “mean square error” (MSE), “peak signal-to-noise ratio” (PSNR) and entropy specified in [14, 16] are exploited to indorse quality of cipher model. The performance measurements are formulated in Table 4. The comparison work of the proposed method with state-of-the-art methods is detailed in Table 5. The comparative review evidenced that the proposed parallel DNA crypto algorithm is relevant to fulfil the security constraints of medical images.

Computational Complexity

The medical images are huge in dimensions, pixels are extremely consistent and contains very sensitive evidence

Table 5 Comparative review of the proposed method

Method	Entropy	NPCR (%)	UACI (%)	PSNR (dB)	Key Space	Encryption time (s)
Ref. [17]	7.9973	99.61	33.43	–	–	0.25
Ref. [18]	7.9995	99.62	33.63	7.74	2^{300}	1.53
Proposed Parallel DNA crypto method	7.9997	99.667	33.42	4.08	2^{400}	0.09

Table 6 Comparative review of the proposed algorithm using serial and parallel method

Medical image	Time taken in seconds			
	Serial computing		Parallel computing	
	Cipher image	Decipher image	Cipher image	Decipher image
MR	38	36	0.16	0.15
CT	37	35	0.12	0.10
X-ray	33	30	0.10	0.07
Ultrasound	32	29	0.09	0.08
ECG	40	37	0.19	0.17

of diseases [19]. Hence, the security constraint of medical images is varying from normal images. The enrichment of security is fundamental constraint for medical images. To fulfil this fundamental constraint, the computational complexity is high, which is drawback for tele interaction. To defeat this challenge, as an alternative for consecutive process, a parallel process is implemented in the proposed system to bring down the time complexity and attain the security constraint of the medical images.

In the proposed method, for high-level security, multi-level, i.e. five-level, encryptions are performed, and in each level, several distinct secret keys are used. If we run the proposed algorithm sequentially, time complexity of one level is O(mn); then, for five levels it is O(5mn). The medical image is subdivided into four equal subparts, then for one subpart it is O(5mn). For four parts, it is O(5*4(mn)), i.e. O(20mn), which is extremely high. If we run the proposed method parallel, then it is O(5mn) because each part is running parallel. Hence, complexity is reduced with fulfilled security constraints of medical images in this cipher model. The comparative review of run time for serial and parallel processing of the proposed method is exposed in Table 6.

The time taken for parallel processing of the proposed system is drastically reduced from the range 30s–40s to 0.1s–0.2s, which is proved in Fig. 4.

The assessment of run time of the proposed parallel cipher method with ancient methods is detailed in Table 7. The run time of the proposed parallel cipher model is lesser than other methods. Thus, the proposed cipher model is significant to extend substantial security with lowered time complexity. The proposed cipher model

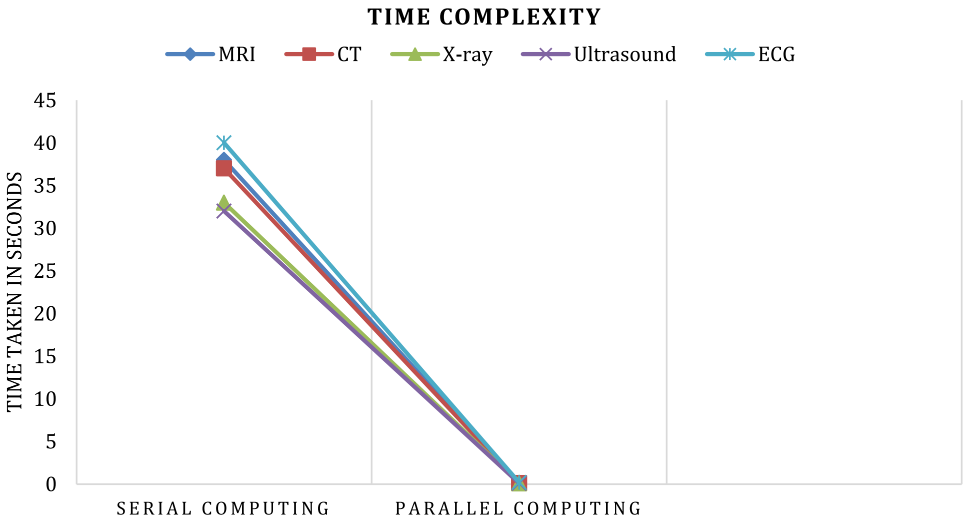

Fig. 4 Comparison of serial and parallel processing of the proposed system

Table 7 Comparison of encryption time in seconds

Koala image of size	Proposed System	Ref. [2]	Lena image of size	Proposed System	Ref. [3]	Medical image of size	Ref. [20]	Proposed System
256×256	**0.09**	0.53	256×256	**0.16**	2.54	MR 512×512	1.21	**0.09**
512×512	**0.19**	–	512×512	**0.99**	13.54	X-ray 1024×1024	5.09	**0.32**

The proposed system values are highlighted in bold

induces to a high throughput which is applicable to real-time systems.

Conclusion

In this paper, the parallel DNA crypto method using 4D Chen's and 4D Lorenz chaotic map, DNA functions and parallel processing is proposed. The medical image is segregated into four equal subparts. The multithreads are generated and allocated to multiple workers for parallel process. These threads are assigned for row by row conversion of the binary matrix into DNA strands using DNA coding patterns. For DNA strands the confusion strands are spawned using Chen's and Lorenz chaotic sequences. The confusion strands are modified into diffusion strands in multilayers by operating DNA XOR. The diffusion strands referred DNA complementary rules to create a encipher image. The experimental findings substantiate that, the proposed DNA crypto method is invulnerable against all possible crypto attacks. The proposed method is relevant for electronic healthcare and teleconsultation applications. The comparative review shows that implementation speed reaches its top state, when multicore CPU is utilized. The real-time clinical image set can be experimented further with the implemented parallel encryption algorithm.

Funding The research work has received a grant under "Research Scheme for Scientists/Faculty (RGS/F) GRD No.851/315" from "Vision Group of Science and Technology, Government of Karnataka".

Declarations

Conflict of interests The authors declared that they do not have the conflict of interest.

References

1. Q. Zhou, W. Kwok-wo, L. Xiaofeng, X. Tao, H. Yue, Parallel image encryption algorithm based on discretized chaotic map. Chaos Solitons Fractals **38**(4), 1081–1092 (2008)
2. K. Hussein, A.M. Sadiq, A.H. Salam, Image encryption based on parallel algorithm via zigzag manner with a new chaotic system. J. Southwest Jiaotong Univ. **54**(4), 1–9 (2019)
3. You, L., Y. Ersong, W. Guangyi, A novel parallel image encryption algorithm based on hybrid chaotic maps with OpenCL implementation. Soft Comput., pp. 1–15, (2020).
4. A.M. Abbas, A.A. Ayman, I. Saleh, A novel parallelizable chaotic image encryption scheme based on elliptic curves. IEEE Access **9**, 54978–54991 (2021)
5. Yu, J., L. Chao, S. Xiaomeng, G. Shiyu, W. Erfu, Parallel mixed image encryption and extraction algorithm based on compressed sensing. Entropy **23**(3), 278 (2021).
6. Raghu, M, E., K. Ravishankar, Encryption and decryption of an image data—a parallel approach. Int. J. Eng. Technol. **7**, 674–677 (2018).
7. Li, T., S. Jiayi, L. Xinsheng, W. Jiang, P. Fan, Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin cubes. Entropy **21**(3), 319, pp.1–21 (2019).
8. J. Wu, L. Xiaofeng, Y. Bo, Image encryption using 2D Hénon-Sine map and DNA approach. Signal Process. **153**, 11–23 (2018)
9. X. Chai, F. Xianglong, G. Zhihua, L. Yang, C. Yiran, A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Process. **155**, 44–62 (2019)
10. Farah, M. A., R. G. Ben, A. Kachouri, M. Samet, A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Opt.& Laser Technol. **121**(105777), 1–8 (2020).
11. L. Habibpour, S. Yousefi, M.Z. Lighvan, H.S. Aghdasi, 1D chaos-based image encryption acceleration by using gpu. Indian J. Sci. Technol. **9**(6), 19–25 (2016)
12. T. Hu, L. Ye, G. Li-Hua, O. Chun-Juan, An image encryption scheme combining chaos with cycle operation for DNA sequences. Nonlinear Dyn. **87**(1), 51–66 (2017)
13. P. T. Akkasaligar, B. Sumangala, Medical image compression and encryption using chaos based DNA cryptography. In: *2020 IEEE Bangalore Humanitarian Technology Conference (B-HTC)*, pp. 1–5 (2020).
14. Prema T. A., B. Sumangala, Multilevel security for medical image using heterogeneous chaotic map and deoxyribonucleic acid sequence operations. In: *Concurrency and Computation: Practice Experience*, **34**(20/10), 1–21 (2022).
15. National Library of Medicines Open Access Biomedical Images Search Engine, https://openi.nlm.nih.gov. Last accessed December 2019.
16. Hiremath P.S, P. T. Akkasaligar, S. Badiger, An optimal wavelet filter for despeckling echocardiograph images". In: *Proceedings of International Conference on Computational Intelligence and Multimedia Applications, ICCIMA*, pp. 245–249 (2007).
17. Md Siddiqur Rahman, T. , K. Md. Rokibul Alam, M. Yasuhiko, A multi-stage chaotic encryption technique for medical image. Inform. Security J. A Global Perspect., 1–19, (2021).

18. Masood, F., D. Maha, B. Wadii, A. Jawad, U. R. Sadaqat, U. J. Sana, Q. Abdullah, J. B. William, A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wireless Personal Commun. pp. 1–28 (2021).
19. Manohar, M., S. Giraddi, G. Bharamagoudar, M. S. Madhur, Brain tumor classification and segmentation using deep learning. In: *Smart Computing Techniques and Applications: Proceedings of the Fourth International Conference on Smart Computing and Informatics*, Volume 2, pp. 201–208. Springer, Singapore (2021).
20. Li, S., Z. Li Z., Y. Na, Medical image encryption based on 2D zigzag confusion and dynamic diffusion. Security Commun. Netw., pp. 1–23 (2021).

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