ARQII Publication
http://arqiipubl.com/ams
APPLICATIONS OF
MODELLING AND SIMULATION
eISSN 2600-8084
VOL 4, 2020, 141-148

A Secure Chaotic Framework for Medical Image Encryption using a 3D Logistic Map

E. A. Adedokun[1], J. B. Akan[1*], H. Bello-Salau[1], I. J. Umoh[1], Nwosu R. I.[2] and Y. Ibrahim[3]

[1]Faculty of Engineering, Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria
[2]Department of Computer Science, Federal College of Forestry, Jos, Nigeria
[3]Department Computer Engineering, Hussanini Adamu Federal Polytechnic, Kazaure, Nigeria

[*]Corresponding author: akanbello@gmail.com

Submitted 20 March 2020, Revised 22 April 2020, Accepted 30 April 2020.
Copyright © 2020 The Authors.

Abstract: Information security and privacy are of utmost importance in transmitting, storing and preserving medical images. In this paper, a secure chaotic framework for medical image encryption is presented, in order to address existing defect in chaos-based image encryption algorithm. The proposed algorithm does the following: a 2D logistic adjusted sine map (2D-LASM) is utilized to generate random number with pixel format, the generated number are then inserted on a plain-image surrounding, which is then divided into non overlapping sub blocks. The scrambling sequence were generated using a 3D logistic map, before image pixel blocks scrambling and diffusion were performed on each sub-block of pixels using the generated scrambling sequence. To verify the efficiency of the proposed algorithm, a number of simulations were carried-out. Based on the results obtained, the algorithm recorded an average score of 7.9998 for information entropy while for number of pixel change rate (NPCR) and unified average changing intensity (UACI) 99.6261% and 33.4830% respectively on an average scale. The proposed algorithm showed high robustness, sensitivity and resistance to all forms of differential attack.

Keywords: Block-level scrambling; Image blocking; Image encryption; Medical image.

1. INTRODUCTION

Medical images contribute significantly to diagnosis and treatment process in healthcare industry. These images are highly confidential and sensitive, hence a lot of privacy need to be maintained either on transit or in storage. When illegal access occurs, it may results into disastrous and life threatening risk during diagnosis. A more direct and suitable approach to provide protection to such images against unauthorized information leakage is encryption [1-4]. Encryption requires transforming an image from its original form into an unrecognizable form called a cipher image by means of secret keys and utilizing an encryption algorithm thus, the process of converting the noise-like image (cipher image) back to its original image is referred to as decryption. This encrypted image can only be recovered using the correct keys [1, 4, 5]. However, in image/multimedia security traditional ciphering approaches such as DES, Triple-DES, AES and RSA does not provide the desired security for real time image encryption due to certain image properties such as high correlation of adjacent pixel and redundancy and it bulky size which may often lead to information leakage [5-11].

In addressing these weaknesses and preventing sensitive information leakage, numerous chaos-based image encryption algorithm has been proposed adopting the Fridrich permutation-diffusion structure to secure different types of images including medical images [11-13]. Among these includes [14, 15] and [17-20], whereas in [21] a new approach involving bit level manipulation was introduced for image encryption using a 2D logistic adjusted sine map. Furthermore, random data were randomly generated and inserted on the image before encryption in order to obtain a different cipher image whenever same pair of encryption keys are repeatedly used in the encryption algorithm. While [22] proposes a chaos-based image encryption algorithm with an orbit perturbation and dynamic state variable selection system using a two-dimensional logistic-adjusted-sine map to generate pseudo-random numbers. The map orbit are then perturbed continuously by the previously processed pixel and one of two state variables are selected to generate the key stream. Performance of the proposed encryption algorithm was evaluated and reported results indicates that the algorithm achieved a good performance.

In addition, [3, 23] in 2014 and 2018 respectively, present novel techniques for medical image encryption using multiple 1D chaotic maps and 3D Chen's chaotic system for both permutation and diffusion. Further to this, in the permutation phase a new shuffling mechanism was also introduced. Similarly, [24] presented an adaptive based medical image encryption scheme, while [1] proposes a high speed scrambling and pixel adaptive medical image encryption algorithm by introducing random data insertion. Two adaptive implementation mechanism called Bitwise XOR (BX) and modular arithmetic (MA) were

This article is distributed under a Creative Commons Attribution 4.0 License that permits any use, reproduction and distribution of the work without further permission provided that the original work is properly cited.

used to diffuse image pixel, although the authors claim that the scheme can achieve both high efficiency and strong robustness. However, [25] proposes a cryptanalysis for [24] claiming that under bad randomness the cipher image can be recovered completely without knowledge of the secret key used during encryption. Hence motivated by this, and exploring the rich properties of chaotic system we proposed a secure chaotic framework for medical image encryption using 3D logistic mapping. The remaining of this paper is structured as follows: Section 2 gives a description of the proposed image encryption algorithm, whereas in Section 3 experimental results and discussions are presented, an finally in Section 4 conclusion is drawn.

2. THE PROPOSED MEDICAL IMAGE ENCRYPTION ALGORITHM

In the proposed algorithm, based on the sensitivity of chaotic system to initial condition a two dimensional logistic adjusted sine map (2D-LASM) was used to generate random data with pixel format. Then, a 3D logistic map was equally used to generate a scrambling sequence and finally sum of permuted image row and column were computed and use interactively with the initial parameter of the logistic map to generate diffusion key stream. The proposed algorithm uses a 256 bit secure key length. Figure 1 shows the block diagram of the proposed algorithm. Hence the algorithm performance was evaluated, experimental results indicate that algorithm has high robustness, high sensitivity and achieve a high resistance to most cryptographic attacks.

Step (1): Generate chaotic key stream using 3D logistic map defined in Equation (1).

$$\begin{cases} a_{i+1} = \alpha a_i(1-a_i) + \beta {b_i}^2 a_i + \gamma {c_i}^3 \\ b_{i+1} = \alpha b_i(1-b_i) + \beta {c_i}^2 b_i + \gamma {a_i}^3 \\ c_{i+1} = \alpha c_i(1-c_i) + \beta {a_i}^2 + c_i + \gamma {b_i}^3 \end{cases} \quad (1)$$

where (α, β, γ) are the control/chaotic parameters and (a_i, b_i, c_i) are the initial conditions of the chaotic map. The 3D logistic map in Equation (1) exhibits chaotic behavior when $\alpha \in [0.35,3.8]$, $\beta \in [0,0.022]$ and $\gamma \in [0,0.015]$ while the initial value $a_i, b_i, c_i \in [0,1]$. Therefore in generating our chaotic key stream, we set the initial conditions as $a_i = 0.667$, $b_i = 0.172$, $c_i = 0.134$ and $\alpha = 3.7800$, $\beta = 0.0157$, $\gamma = 0.0125$. The first 20 iterates were discarded.

Step (2): Generation and insertion 2D-LASM pixel related random generation.
Four random vector of size 4×N and (M+4) ×4 were generated using 2D-LASM given in Equation (2) and inserted to the plain image surrounding.

$$\begin{cases} a_{i+1} = \left(\pi\mu(b_i+3)a_i(1-a_i)\right) \\ b_{i+1} = (\pi\mu(a_{i+1}+3)b_i(1-b_i)) \end{cases} \quad (2)$$

Herein the values of (a, b, u) are all within [0,1].

Step (3): Image blocking.
The image size is obtained and plain-image is divided into block 8 non-overlapping block with 8-by-8, 16-by-16 and 32-by-32.

Step (4): Next we apply image block level scrambling.
(a) First, a scrambling matrix (D) of size $M \times N$ is generated using Equation 1.
(b) Sort the generated D and obtain an index matrix (IM).
(c) Assign each row to the index matrix.

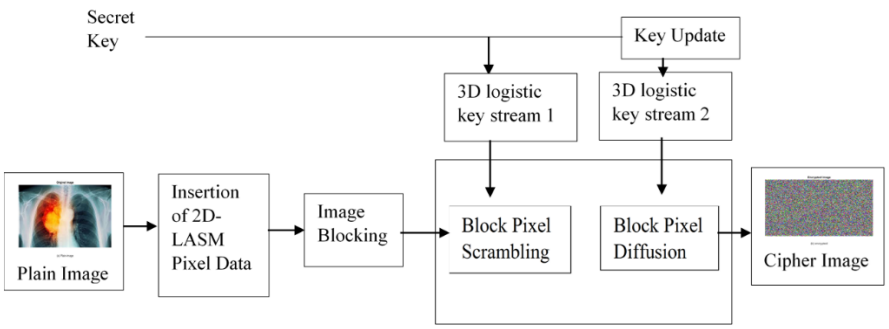


Figure 1. Block diagram of the proposed algorithm

(d) Shuffle each pixel position in each sub-block using the index matrix in this manner $\{(IM_{i,1}, 1), (IM_{i,2}, 2), \dots, (IM_{i,N}, N)\}$ using a shuffling function in Equation (3).

$$P_i = B_s(P, D) \tag{3}$$

where P_i represents the permuted image, B_s denotes block scrambling function, P denotes plain image while D is the generated scrambling sequence.

Step (5): Repeat permutation until $M - 1$ for $j = 2$.

Step (6): Return permuted image P_i.

Step (7): Block diffusion.
(a) Compute sum of row and column of permuted image in Step (6).
(b) Iterate 3D logistic map using Steps (1) and (7a) to obtain the diffusion key-stream k.
(c) Perform block level diffusion on the permuted image by masking the shuffled pixel in a chaotic manner with the chaotic diffusion key stream k using Equation (4).

$$c_n = D_E[P_n \oplus k_n] \tag{4}$$

(d) Repeat the whole process for all image pixel simultaneously for each sub-block.
(e) Return encrypted image.

From Equation (4), P_n denotes the current operated permuted pixel, c_n is the output ciphered pixel, and k_n represents the key stream. Similarly, the decryption is to perform a reverse encryption process.

3. EXPERIMENTAL RESULTS AND DISCUSSIONS

In this paper, a typical standard medical image of size 387-by-277 is used for the purpose of experimental demonstration. The entire standard medical images use for performance analysis were obtained from [26, 27]. Figures 2(a), (b), (c), (d) and (e) respectively show the plain image, cipher image, decrypted image and their corresponding histogram representation. From this figure, it can be seen that the plain image histogram in Figure 2(b) has different patterns whereas the encrypted image histogram in Figure 2(d) are uniformly distributed proving that the proposed cryptosystem has the ability to resist histogram related attack. To further verify the efficiency of this cryptosystem in resisting other forms of attack, the following analysis were carried out: information entropy, pixel correlation, differential analysis, key sensitivity.

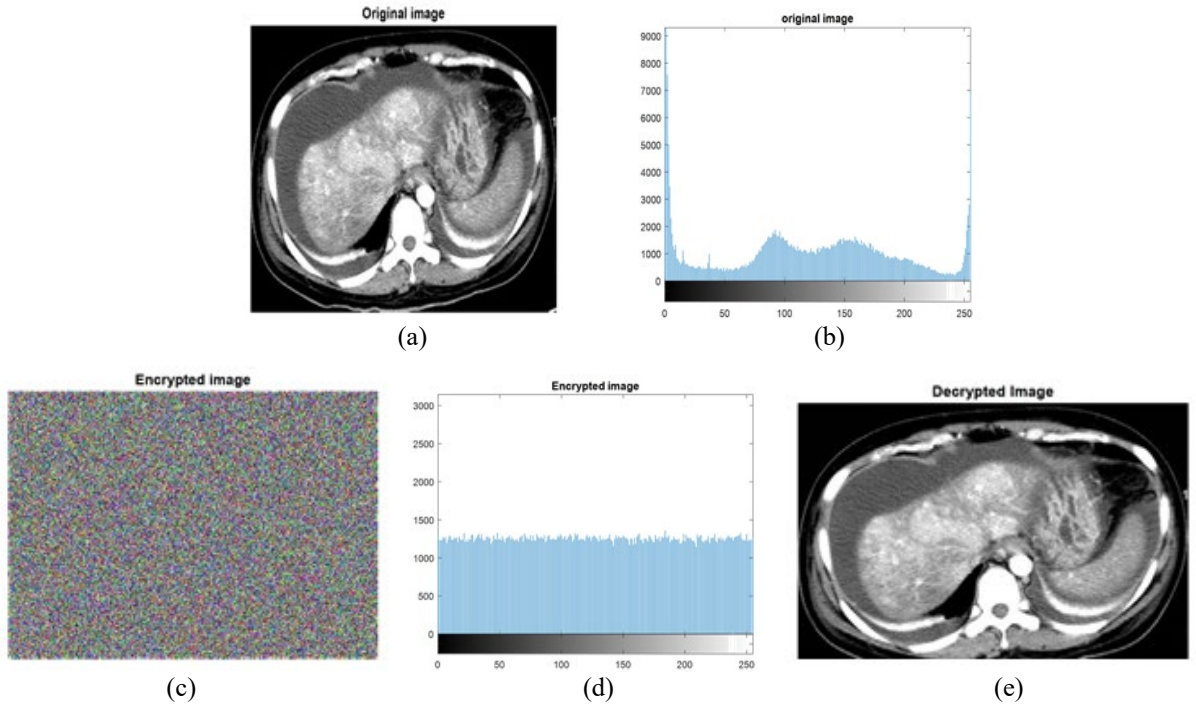


Figure 2. Illustration of encryption and decryption result

3.1 Information Entropy Analysis

Information entropy test is widely used to evaluate the degree of randomness exhibited in data sequence. Most times, it is express as the average number of bit required to store or communicate one symbol in a message. Mathematically it is defined as given in Equation (5).

$$IE = \sum_{i-1}^{L} P(k_i)\log_2 P(k_i) \tag{5}$$

where L is the gray level intensity and $P(k_i)$ denotes the probability occurrence of the i^{th} symbol k_i. As given in this equation, the entropy of a cipher image should ideally be $\log_2 L$ for all images with color intensity level L else, there exist some level of predictability, which may serve as a security threat to encrypted data. Table 1 presents the information entropy results obtained for six (6) medical images.

Table 1. Information entropy results

Information Entropy		
Test images	Plain images	Encrypted images
Chest-Xray	5.2145	7.9998
Abdomen CT	7.2377	7.9999
Pregnancy	6.0740	7.9998
Heart Cancer CT	4.3659	7.9999
Pancreas	5.5678	7.9998
Lungs CT	4.3451	7.9999
Average score	5.4675	7.99985

The entropy results for six different images having different sizes is as shown in Table 1. It can be seen that the proposed algorithm achieved a high entropy very close to the theoretical value for the encrypted images. Therefore, the level of information leakage is insignificant and it can be concluded that this scheme has high level of unpredictability which means it can efficiently resist entropy attack.

3.2 Pixel Correlation Analysis

As a result of high level of neighboring, pixel correlation in the plain image, at diagonal, horizontal and vertical direction. This analysis is performed to calculate pixel correlation coefficient for both plain and encrypted image. In order to perform this analysis 2000 pair of adjacent pixel in each direction were randomly selected. Presented in Figure 3, Figure 4 and Table 2 are the results obtained by the proposed algorithm. The assessments for both encrypted and plain image are calculated using Equations **(**6)-(8).

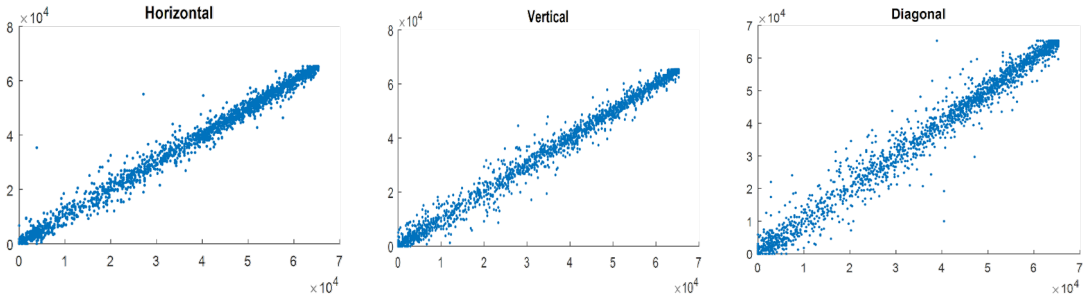
$$D(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)]^2 \tag{6}$$

$$cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)][y_i - E(y)] \tag{7}$$

$$R_{xy} = \frac{cov(x,y)}{\left(\sqrt{D(x)\sqrt{D(y)}}\right)} \tag{8}$$

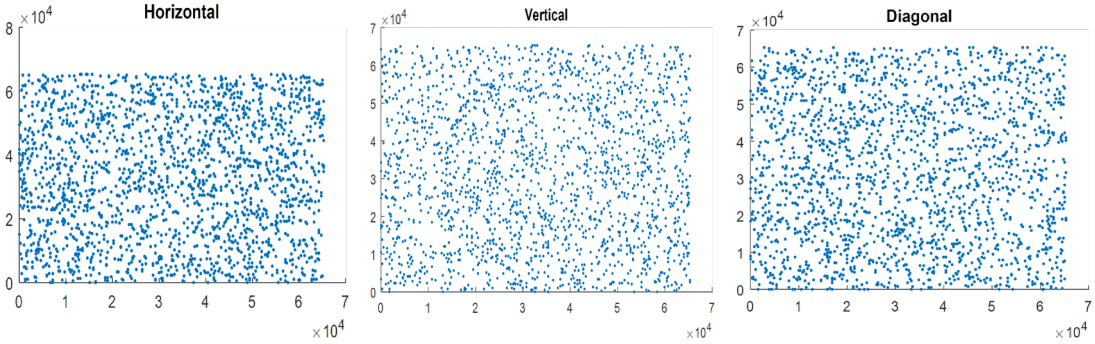
From Equations (6) to (8), n is defined as the number of pixel point, while $E(x)$ and $E(y)$ is the expectation of x and y whereas x and y are gray value for two adjacent pixel points, while $cov(x,y)$ is the covariance of x and y and R_{xy} is the pixel correlation coefficient for adjacent pixel values.

Illustrated in Figure 3 is the visual correlation distribution of adjacent neighboring plain-image pixel in horizontal, vertical and diagonal direction while Figure 4 is the visual correlation distribution of encrypted pixel in horizontal, vertical and diagonal direction. As shown in Figure 3, the plain-image neighboring pixels are clustered along a straight line meaning pixel values along each direction has high correlation. Meanwhile as shown in Figure 4 the encrypted image, it pixel values are scatter all over the entire space meaning the correlation of pixel values for each direction in the encrypted image drastically reduce.



(a) (b) (c)

Figure 3. Plain images of direction (a) Horizontal (b) Vertical (c) Diagonal



(a) (b) (c)

Figure 4. Encrypted images of direction (a) Horizontal (b) Vertical (c) Diagonal

As shown in Table 2, the pixel correlation for plain images is approximately 1 while their corresponding cipher image pixel correlation is practically 0. Thus, no useful information can be obtained from the encrypted image based on neighboring pixel correlation and therefore it indicated that the algorithm proposed can efficiently resist statistical attacks involving image pixel correlation.

Table 2. Adjacent pixel correlation coefficient results

Neighboring Pixel Correlation Coefficient			
Test images	Direction	Plain images	Encrypted images
Chest-Xray	Horizontal	0.9929	-0.0005
	Vertical	0.9923	-0.0021
	Diagonal	0.9872	0.0031
Abdomen CT	Horizontal	0.9744	-0.0008
	Vertical	0.9728	-0.0001
	Diagonal	0.9499	0.0026
Pregnancy	Horizontal	0.9659	0.0033
	Vertical	0.9801	0.0003
	Diagonal	0.9516	0.0057
Heart Cancer CT	Horizontal	0.9801	-0.0066
	Vertical	0.9762	0.0017
	Diagonal	0.9636	0.0027
Pancreas	Horizontal	0.9875	0.0006
	Vertical	0.9876	-0.0010
	Diagonal	0.9761	0.0011

3.3 Differential Attack Analysis

The differential analysis, verifies a cryptosystem diffusion effect that is its ability to generate a completely different cipher given a slight change in the plain image. To evaluate this encryption algorithm, two metric widely known as number of pixel change rate (NPCR) and unified average changing intensity (UACI) are used and define as given in Equations (9) and (10). The closer NPCR approaches 100% the more effective is the cryptosystem whereas the higher the UACI value the more effective the cryptosystem possesses the ability to resist differential attacks.

In performing this test, five (5) standard test medical images were used for NPCR and UACI for each image test case. A pixel values is modify in three positions namely upper right corner at pixel position (1,1), (20,20) and lower lifted corner. Thus, the two plain-image differing in a single pixel value were encrypted using the proposed algorithm with the same pair of secret key. Their values were computed and presented in Table 3. The values computed for both NPCR and UACI on an average scale is 99.6261 and 33.4830 respectively indicating higher resistance to differential attack.

$$NPCR(c_1, c_2) = \sum_{ij} \frac{D(ij)}{MN} \times 100\% \tag{9}$$

$$UACI(c_1, c_2) = \sum_{ij} \frac{|c_1(ij) - c_2(ij)|}{M \times N \times 256} \times 100\% \tag{10}$$

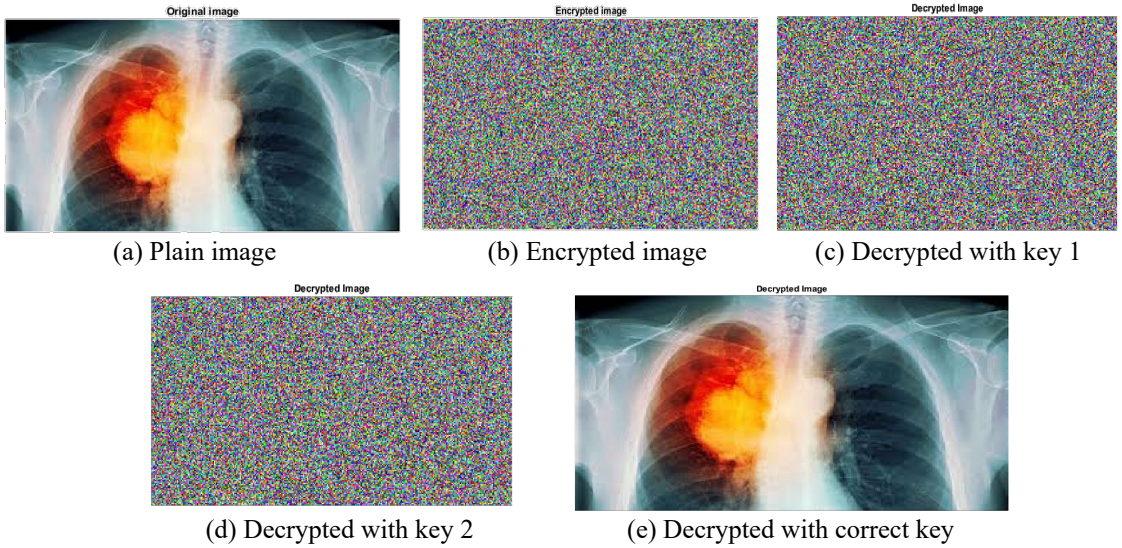
where c_1 and c_2 denote two different images and $M \times N$ is the image size, if $c_1(ij)$ is not equal to $c_2(ij)$, then $D(ij) = 1$, otherwise $D(ij) = 0$.

Table 3: NPCR and UACI results

Test Images	Kidney stone CT	Brain CT	Liver	Abdomen CT	Head CT	Average
NPCR	99.6330	99.6399	99.6258	99.6130	99.6188	99.6261
UACI	33.4624	33.5991	33.3784	33.4730	33.5022	33.4830

3.4 Key Sensitivity Analysis

In evaluating the sensitivity of keys for this algorithm, a pair of randomly generated secret key is utilized to encrypt a plain-image. Then, a slight modification is made to the key at decryption end differing by a single bit. This operation is performed repeatedly for all the key pairs. Figure 5 shows the sensitivity results. It is observed from Figure 5 that the proposed algorithm is highly sensitive to encryption keys. Therefore, the encrypted plain image can only be recover with the correct key. Finally presented in Table 4 is the performance comparison of the proposed algorithm with the work of [3, 23-25] using the following measures: information entropy, NPCR and UACI. Hence based on the average score obtained from each test as showed in Table 4, it can be concluded that the proposed algorithm offers better robustness and resistance against various cryptographic attacks.



(a) Plain image (b) Encrypted image (c) Decrypted with key 1

(d) Decrypted with key 2 (e) Decrypted with correct key

Figure 5. Key sensitivity results

Table 4. Performance comparison

	Our Scheme	[23]	[24]	[3]	[25]
Information Entropy	7.9998	7.9993	7.9891	7.9992	7.9973
NPCR	99.62	99.60	99.59	99.61	99.61
UACI	33.48	33.45	33.42	33.47	33.45

4. CONCLUSION

In this paper, a secure chaotic framework for medical image encryption algorithm using 3D logistic map for protecting the privacy of patient's medical images either on transit or storage is proposed. In the diffusion stage, by computing the row and column sum of the permuted image, the chaotic parameter for 3D logistic map were updated to increase the robustness and complexity of the proposed algorithm to attacks. The algorithm performance was then evaluated using information entropy, histogram analysis, adjacent pixels correlation coefficient, key sensitivity, NPCR and UACI as metric. The results obtained confirmed that the proposed algorithm exhibits a good encryption performance with high security level, better robustness and resistance to attacks on medical images.

REFERENCES

[1] Z. Hua, S. Yi and Y. Zhou, Medical image encryption using high-speed scrambling and pixel adaptive diffusion, *Signal Processing*, 144, 2018, 134–144.

[2] G. Alvarez, S. Li and L. Hernandez, Analysis of security problems in a medical image encryption system, *Computers in Biology and Medicine*, 37, 2007, 424–427.

[3] C. Fu, G.-y. Zhang, O. Bian, W.-m. Lei, and H.-f. Ma, A novel medical image protection scheme using a 3-dimensional chaotic system, *PloS One*, 9, 2014, 1–25.

[4] G. Ye, K. Jiao, C. Pan and X. Huang, An effective framework for chaotic image encryption based on 3D logistic map, *Security and Communication Networks*, 2018, 1–11.

[5] P. T. Akkasaligar and S. Biradar, Secure medical image encryption based on intensity level using chao's theory and DNA cryptography, *2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Chennai, India, 2016, 1–6.

[6] A. S. Nasim, *Chaos based cryptogrphy and image encryption*, M.Sc. Dissertation, Electrical and Computer Engineering, University of Applied Sciences, Luebeck, Germany, 2015.

[7] M. B. Hossain, M. T. Rahman, A. S. Rahman and S. Islam, A new approach of image encryption using 3D chaotic map to enhance security of multimedia component, *2014 International Conference on Informatics, Electronics & Vision (ICIEV)*, Dhaka, Bangladesh, 2014, 1–6.

[8] M. Machkour, A. Saaidi and M. L. Benmaati, A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher, *3D Research,* 6(36), 2015, 1–18.

[9] N. Mekki, M. Hamdi, T. Aguili and T.-h. Kim, A real-time chaotic encryption for multimedia data and application to secure surveillance framework for IoT system, *2018 International Conference on Advanced Communication Technologies and Networking (CommNet)*, Marrakech, Morocco, 2018, 1–10.

[10] H. Oğraş and M. Türk, A secure chaos-based image cryptosystem with an improved sine key generator, *American Journal of Signal Processing*, 6(3), 2016, 67–76.

[11] W. Zhang, H. Yu, Y.-l. Zhao and Z.-l. Zhu, Image encryption based on three-dimensional bit matrix permutation, *Signal Processing*,118, 2016, 36–50.

[12] L. Xu, Z. Li, J. Li and W. Hua, A novel bit-level image encryption algorithm based on chaotic maps, *Optics and Lasers in Engineering*, 78, 2016, 17–25.

[13] A.-V. Diaconu, V. Ionescu, G. Iana and J. M. Lopez-Guede, A new bit-level permutation image encryption algorithm, *2016 International Conference on Communications (COMM)*, Bucharest, Romania, 2016, 411–416.

[14] N. K. Pareek, V. Patidar and K. K. Sud, Image encryption using chaotic logistic map, *Image and Vision Computing*, 24, 2006, 926–934.

[15] J.-Q. Cao, H.-R. Xiao and Z.-L. Lan, Chaos encryption algorithm based on dual scrambling of pixel position and value, *Computer Engineering and Applications*, 46, 2010, 192–195.

[16] W. Zhen, H. Xia, L. Yu-Xia and S. Xiao-Na, A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system, *Chinese Physics B*, 22(1), 2013, 010504.

[17] J.-x. Chen, Z.-l. Zhu, C. Fu and H. Yu, An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism, *Optics Express*, 21, 2013, 27873–27890.

[18] Y. Zhang and D. Xiao, An image encryption scheme based on rotation matrix bit-level permutation and block diffusion, *Communications in Nonlinear Science and Numerical Simulation*, 19, 2014, 74–82.

[19] Y. Li, C. Wang and H. Chen, A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, *Optics and Lasers in Engineering*, 90, 2017, 238–246.

[20] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang and S. W. Baik, Secure surveillance framework for IoT systems using probabilistic image encryption, *IEEE Transactions on Industrial Informatics*, 14, 2018, 3679–3689.

[21] Z. Hua and Y. Zhou, Image encryption using 2D Logistic-adjusted-sine map, *Information Sciences*, 339, 2016, 237–253.

[22] H. Li, Y. Wang and Z. Zuo, Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms, *Optics and Lasers in Engineering*, 115, 2019, 197–207.

[23] C. Fu, Y.-F. Shan, M.-Y. He, Z.-Y. Yu and H.-L. Wu, A new medical image encryption algorithm using multiple 1-D chaotic maps, *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Miyazaki, Japan, 2018, 2055–2060.
[24] X. Chen and C.-J. Hu, Adaptive medical image encryption algorithm based on multiple chaotic mapping, *Saudi Journal of Biological Sciences*, 24(8), 2017, 1821–1827.
[25] Y. Chen, C. Tang and R. Ye, Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion, *Signal Processing*, 167, 2019, 107286.
[26] M. Levoy, The Stanford volume data archive, 2001. https://graphics.stanford.edu/data/voldata, 2009. (accessed 15.07.2019).
[27] SPIE-AAPM Lung CTchallenge. https://scidm.nchc.org.tw/en/dataset/spieaapmlungctchallenge/resource/1a37c6c8-10aa-4a9f-8db3-6e632bf788d7 (accessed 05.09.2019).