An Enhanced Security in Medical Image Encryption Using Dynamic Chaotic Fuzzy Based Technique

Snehashish Bhattacharjee [1,*], Mousumi Gupta [2], and Biswajoy Chatterjee [3]

[1] Department of Computer Science & Engineering, University of Engineering & Management, Kolkata, India
[2] Department of Computer Application, Sikkim Manipal Institute of Technology, Majitar, India;
Email: mousumi.g@smit.smu.edu.in (M.G.)
[3] Department of Computer Science & Engineering, University of Engineering & Management, Jaipur, India;
Email: biswajoy.chatterjee@iemcal.com (B.C.)
*Correspondence: snehashishbhattacharjee@gmail.com (S.B.)

***Abstract*—As IoT and cloud computing have grown in popularity, medical images are now often transmitted between devices or accessed directly from the cloud. With this, the security is always a concern as these images are prone to many types of attack. We have proposed a proven method that is efficient in terms of security, time complexity, and integrity in order to be cloud-friendly so that it may be launched into the cloud and made accessible to users at any time. The goal of the work is to create a dynamic key that, depending on fuzzy values, alters the reproduction rate parameters with each repetition. By applying the last chaotic value created from the previous iteration, the fuzzy triangular membership function has been used in this manner to generate the reproduction rate parameter. The uniqueness and major benefit of the suggested strategy are that it can increase the security of the algorithm that makes use of a chaotic map and a static key. The method has been put forth when designing algorithms so that it should not only demonstrate security against different attacks but also provide efficiency towards computational complexity. The technique has been tested against a set of images and an existing algorithm using a variety of security metrics, including the correlation coefficient, Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), and entropy. It has been determined from the comparative analysis that the proposed approach can make the existing algorithm more secure.**

***Keywords*—fuzzy, encryption, chaos, logistic map, correlation, Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI)**

I. Introduction

The emergence of cloud computing and IOT encourages users to keep images for quick access, whether for business purposes or personal ones. The security of these images, which include sensitive images, cannot be compromised. Every business, from banking to healthcare, spends a lot of money each year to protect the information of its clients. Cloud computing has made it possible for healthcare professionals to effectively store, access, and safeguard patient data so that it is always accessible. The major goals of the various medically-based cryptography methods are to protect patient information from unwanted access and to fend off cipher attacks [1–3]. For safeguarding medical images, numerous encryption techniques have already been put forth in the literature. AES (Advanced Encryption Standard), RSA, and DES (Data Encryption Standard) are three examples of classic encryption methods that are excellent for text but not ideal for images due to their vast size and high pixel correlation [4–11]. Modern chaos-based encryption methods exhibit highly positive security results. In chaos-based encryption, the chaotic map is used to scramble the picture pixel values during encryption, and the opposite procedure is then done at the receiver's end to recover the original plain image. Numerous authors have put forth a variety of strategies, including bit map permutation, the Arnold Cat map, the 1 -D Tent map, the hybrid chaotic map (a combination of the sine map, the logistic map, and the tent map [12–16], the cubic logistic map, combination permutation with the diffusion method, and extended diffusion substitution [17–19]. There are other chaos-based encryption techniques recently proposed such as two-dimensional Logistic-adjusted-Sine map (2D-LASM), dynamic substitution box technique, 2-D Burgers chaotic map, combination of 3-D chaotic logistic map with DNA encoding and many more [20–31].

Image moments are a type of image characteristic that is employed in image encryption. Orthogonal moments are studied and continuous orthogonal moments are first implemented. Some disadvantages of continuous orthogonal moments include numerical approximation of continuous integrals, wide dynamic range values *etc*. To overcome these issues, there have been suggested Image encryption based on discrete orthogonal moment-based encryption methods [32], Fractional Discrete Meixner moments [33], Fractional discrete Tchebyshev

Manuscript received May 4, 2023; revised June 1, 2023; accepted July 5, 2023.

moments [34], multi-channel orthogonal Gegenbauer moments with fractional order (FrMGMs) [35], 3D fractional modified Henon map and the discrete fractional Krawtchouk moments [36].

Hyper chaotic systems are used due to their complex dynamic nature including hyper sensitivity and pseudo randomness in image encryption. The algorithm proposed in recent years include hyper-chaotic multi-attractors Chen system with time delay [37] for improving performances of encryption performances, hyper chaotic system with compressive sensing to improve the visual security[38], Three-dimensional (3D) orthogonal Latin cube transformation and RNA diffusion [39], hyper chaotic system with double parity alternate scrambling to resists differential and statistical attack [40], DNA strand displacement and four-dimensional multi-stable hyper chaotic system [41], chaos based encryption using four dimensional hyperchaotic map is proposed for better dynaic behavior [42].

In recent years, fuzzy based encryption technique emerges as an appealing alternative to encryption due to its complicated dynamic characteristics, which exhibit what appear to be random occurrences within a predetermined nonlinear system or Process. Fuzzy Cellular Neural Network (FCNN) has been used due to the properties of high non linearity [33–35]. Traditional FCNN has the issues of time varying delays for which Modified FCNN has been proposed to address the issues [10]. Among other techniques, Parallel Fuzzy Multi Modular Chaotic Logistic Maps (PFMM-CLM) has been introduced to overcome the issues in key space and security protection faced in Cascade Chaotic System (CCS) and Dynamic Parameter-Control Chaotic System (DPCCS) [1]. The substitution boxes (S-Boxes) which use features of the combination of Choquet Fuzzy Integral (CFI) and DNA techniques are applied in image encryption to add more security to ensure resistance against attacks [2]. In another study, 3D hybrid chaotic system and choquet fuzzy integral are introduced using B-spline functions as membership grades to confuse and diffuse the pixels [5].

In the various literature, it has been noticed that most of the algorithms use a static key, which is constant throughout the encryption and decryption processes. Any algorithm that uses a 1-D logistic map, which is very simple in its nature and easy to predict, On the contrary, a 2D logistic map is complex, but the computational cost is very high. To overcome all these issues, a method is proposed that not only increases the security of the existing algorithm but also has a minimal effect on the existing time complexity.. It is significant to highlight that this method is easily adaptable to any other chaotic system and may be further adjusted by taking into account various fuzzy number types, such as trapezoidal, Gaussian, quadratic, exponential, or their combination. The basic difference of the schemes having used only chaotic map and the schemes used combination of chaotic map and fuzzy logic is that fuzzy based chaotic maps reach a higher security in terms of Correlation coefficient, NPCR, UACI, Entropy *etc* and hence provide a good security against various types of attacks. This method can be easily adaptable in image hiding schemes, complex hyper chaotic system, in DNA cryptography etc which can further improve the security performances.

II. Materials and Methods

In Fig. 1, the architecture diagram is displayed. In this suggested approach, we have attempted to adapt the method [43] that makes use of a static key and two logistic maps. In the first iterative run, we generated the first parameter using the same static key. However, in the second iteration, the reproduction rate was altered using fuzzy logic, raising the level of security of the existing algorithm. The first logistic map uses the sort transformation to randomly shuffle all of the pixels. To defend against further statistical and differential attacks, the second logistic map is employed to completely diffuse the entire image. The initial parameter employed by both logistic maps was the same and remained constant throughout the entire encryption and decryption procedures. Despite the fact that the proposed scheme produces good results for medical images, there is still room to improve the technique and increase algorithmic security. In this case, the fuzzy numbers were created using a fuzzy membership function, and they were then utilized to change the logistic map's chaotic parameter reproduction. The reproduction rate parameter has values between [3.98, 4]. The membership function is shown in the Fig. 2. We adjust the reproduction rate in accordance with Eq. (2) every 100 iterations. As a result, the beginning value will change after each repetition by obtaining the final value from the previous iteration.

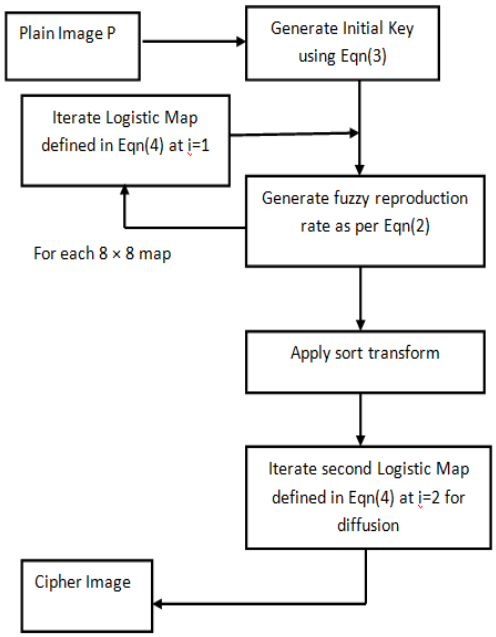


Figure 1. Block diagram

We have used the below equation to compute the membership values.

$$y=(x-3.98)/0.01 \quad (1)$$

$$x=\sum_{k=1}^{n}\binom{n}{k}x^k\,a^{n-k}\times 3.98+0.01y \quad (2)$$

Steps for Initial parameter generation:

First time, Iterate the logistic map defined in Eq. (4) with the initial parameter x_0 and b_0.

For each iteration, calculate the value of the reproduction rate ($b_1, b_2, \ldots, b_n$)by using Eq. (2).

For each iteration, the initial value ($x_1, x_2, \ldots, x_n$) is calculated by using the last iterated value obtained in the previous iteration.

This can be denoted as $x_i = LAST(ITR_i-1)$, where $i=1, 2, \ldots, n$ and $LAST(ITR_i)$ denotes the last value of the previous iteration.

So the below combined steps to be performed for the encryption technique.

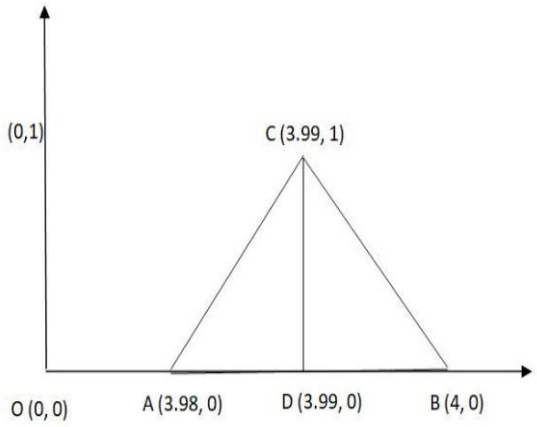


Figure 2. Fuzzy membership diagram.

Let us view the matrix as $(a_{ij})_{m\times n}$. We change the element names as b_j, where $b_{(i-1)n+j}=a_{ij}$.

Step 1: Key Generation

The gray level key generation steps defined in [1]. The initial parameter is generated by using the Eq. (3).

$$y_0=\frac{\sum_{i=1}^{2^{2n-1}}\sum_{j=1}^{4}k_{ij}\,2^{ij-1}}{4.2^{2n-3}} \quad (3)$$

where each k_{ij} is a four bit binary code generated from gray code.

Step 2: Reproduction rate parameter generation

In this approach, we have considered the two logistic map taken is the below equation.

$$y_{j+1}^{i}=a^i y_j^i(1-y_j^i),\ i=1,2\ j=0,1,2\ldots \quad (4)$$

The initial value y_0 is calculated using Eq. (3).

Step 3: Iterate the logistic map defined in Eq. (4) with the value i=1. For each iteration calculate the value of the reproduction rate ($b_1, b_2, \ldots, b_n$) by using Eq. (2). The initial values ($y_1, y_2, \ldots, y_n$) are calculated by using the last iterated value obtained in the previous iteration.

This can be denoted as $x_i = LAST(ITR_i-1)$ where $i=1, 2, \ldots, n$ and $LAST(ITR_i)$ denote the last value of the previous iteration.

Step 4: Now, we view the set as $B=\{(y_j^i, j, b_j): i=1,2,\ldots,m\times m\}$. Sort transformation is applied on B to get $y_{j1}<y_{j2}<\ldots<y_{jk}<\ldots$ and the corresponding set becomes $S=\{(y_{jk}^i, jk, b_{jk}): k=1,2,\ldots,m\times m\}$.

Step 5: Rearrange the pixels of the input image with the same order based on the position value obtained in the set S and calculate the average produced by the other chaotic map's iteration x_k^2.

Step 6: The second level diffusion is carried out by further modification of the average value obtained in the above step.

$$b_{jk}=\begin{cases} b'_{jk} & if\ \ jk\ is\ even \\ pb'_{jk} & if\ \ jk\ is\ odd \end{cases}$$

The image is encrypted e is the matrix $(e_{ij})_{m\times n}$.

III. Result and Discussion

The proposed algorithm has been implemented in Wolfram Mathematica 11. The processor is an Intel(R) Core (TM) i3-5005U CPU at 2.00 GHz with 4 GB of RAM. We have used medical images, which are available in [30]. In our experiment, five medical images are shown in Fig. 3 that were collected from a standard dataset. First, the proposed encryption algorithm is used. In Fig. 3, the input medical images are shown as a1–a5, the cypher images are shown as d1–d5, the image histograms for the original images are shown as b1–b5, and the equivalent image histogram for the cypher images is shown as c1–c5. These results show that the histogram of the encrypted images is extremely dispersed and distinct from the histogram of the original images. The only disadvantage is that the histogram is not flat and which can be improved further.

A. Correlation Coefficient Analysis

The correlation coefficient is one of the metrics used to assess the effectiveness of any encryption technique. It determines the correlation value between two neighboring pixels. Mathematically, the correlation coefficient is determined by the equation shown below. We have calculated the correlation coefficient for each of the medical images in Fig. 3, and it is tabulated in Table I. A graphical analysis of Table I is shown in Fig. 4. The correlation values are observed, and they are close to zero for all the directions in diagonal vertical and horizontal pixels for each of the cypher images, which indicates that the encryption technique is secured against statistical attack.

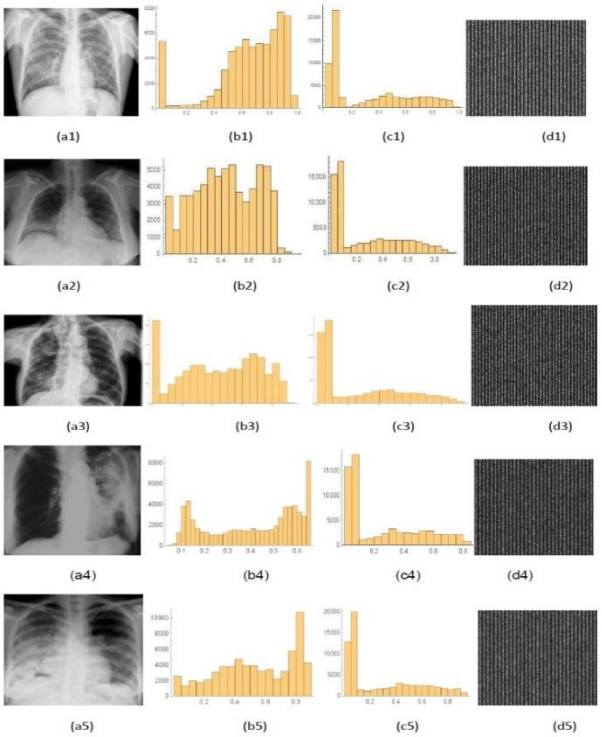


Figure 3. (a1–a5) are the medical Images taken as input. (b1–b5) are the histogram representation of the input images. (c1–c5) are the histogram of encrypted images. (d1-d5) are the respective encrypted Images.

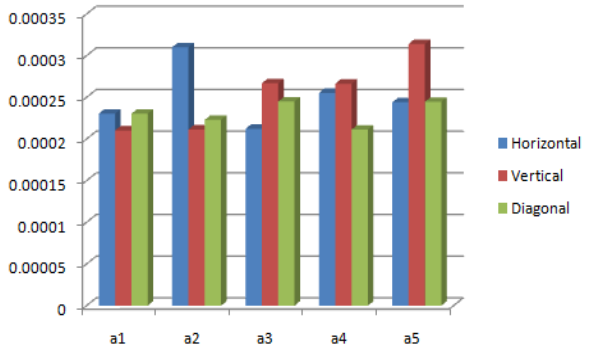


Figure 4. Graphical analysis of correlation coefficient in horizontal, vertical and diagonal adjacent pixels.

$$C_r = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{N\sum_{j=1}^{N} x_j^2 (\sum_{j=1}^{N} x_j)^2 \times (N\sum_{j=1}^{N} y_j^2 (\sum_{j=1}^{N} y_j)^2}} \quad (5)$$

For the horizontal, vertical, and diagonal pixels, the correlation coefficient is assessed. The findings of the coefficient result of each medical image along the horizontal, vertical, and diagonal directions are provided in Table I. The technique is verified with the Leena image, compared with [1], and documented in Table II. The experimental result demonstrates that, compared to other methods, encryption has a lower correlation coefficient than [1].

TABLE I. CORRELATION COEFFICIENT ANALYSIS IN HORIZONTAL, VERTICAL AND DIAGONAL ADJACENT PIXELS

Image Name	Size	Horizontal	Vertical	Diagonal
a1	256 × 256	0.0002305	0.0002103	0.0002304
a2	256 × 256	0.0003102	0.0002115	0.0002230
a3	256 × 256	0.0002123	0.0002669	0.0002449
a4	256 × 256	0.0002554	0.0002664	0.0002114
a5	256 × 256	0.0002441	0.0003142	0.0002447

TABLE II. CORRELATION CO-EFFICIENT IN HORIZONTAL, VERTICAL AND DIAGONAL DIRECTION WITH FUZZY BASED PROPOSED APPROACH AND WITHOUT FUZZY BASED APPROACH [1]

Lena Image	Bhattacharjee *et.al.* [1]	Proposed Algorithm
Horizontal	−0.0002167	−0.0001121
Vertical	0.0053385	0.0002122
Diagonal	0.0006699	0.0004122

In Table II, we have detailed the correlation coefficient in horizontal, vertical, and diagonal directions. We have taken the same 256×256 Leena image to check the difference. The horizontal co-efficient in this fuzzy-based proposed approach is −0001121, which is higher than the −0.0002167 obtained in [1]. Similarly, for the vertical and diagonal directions, the values obtained were 0.0053385 and 0.0006699, respectively.

B. NPCR

NPCR is one of the most commonly used metrics to test the performance of the encryption technique against differential attacks. It is used to quantify the performance of the algorithm in terms of being sensitive when the plain-text image is altered or modified by different attacks. NPCR calculates the rate of change in pixel count between two ciphered images, CIP1 and CIP2. The plain-text picture PTX2, a modified version of PTX1, is used to create the cypher-text image CIP2, and P1 is used to create the cypher-text image CIP1. An efficient cryptosystem produces very nearly 100 percent, indicating the highest level of resistance to differential attack. The NPCR values obtained for the images a1–a5 are 99.68, 99.62, 99.64, 99.65, and 99.69, which are captured in Table III. A graphical analysis of Table III is shown in Fig. 5. It is evident from Table III that with the proposed methodology, NPCR values are better obtained when we incorporate fuzzy in [1].

The Eq. (6) below yields the NPCR value

$$NPCR = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} p(a,b)}{H \times W} \quad (6)$$

$$where\ P(a,b) = 1\ if\ C1P1 \neq C2P2$$

$$= 0\ if\ C1P1 = C2P2$$

$$W\ is\ the\ width\ and\ H\ is\ the\ height$$

TABLE III. NPCR MEASURE BETWEEN THE PROPOSED AND EXISTING SCHEMES

Schemes	a1	a2	a3	a4	a5
Proposed algorithm	99.68	99.62	99.64	99.65	99.69
Bhattacharjee *et al.* [1]	99.66	99.42	99.30	99.28	99.42

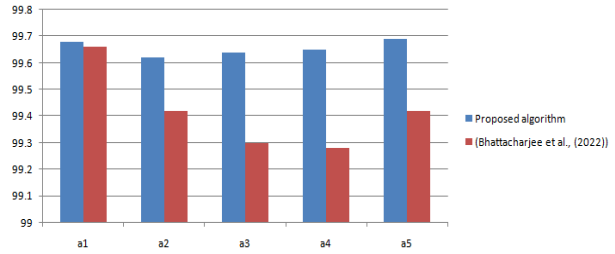


Figure 5. Graphical analysis of NPCR Measure between the proposed and existing scheme.

C. UACI

When applied to two versions of the input image, the number of average changed intensities is determined using UACI (Unified Averaged Changed Intensity). Let ENC1 and ENC2 represent the two cipher images that were created from the original image both before and after a change. The resulting UACI is calculated from the below equation

$$UACI = \sum \frac{ENC1(i,j) - ENC2(i,j)}{H \times W \times 255} \quad (7)$$

where H and W are the image's height and breadth and ENC1 and ENC2 are its two encrypted images. The UACI is calculated for the visual images and is formulated in Table IV. A graphical analysis of the Table IV is shown in Fig.6. It is observed that the UACI value is obtained around 33 percent which is quite good for the encryption technique. A comparison result has been carried out between the proposed by fuzzy based approach and the approach proposed by Bhattacharjee *et al*. [1]. The UACI value for the Leena image obtained in [1] is 33.6992 compared to the proposed technique is 33.6995. Similarly, the value obtained in USC-SIPI image by the proposed technique is higher than the value obtained in [1].

TABLE IV. THE USC-SIPI IMAGES DATABASE CONTAINS NPCR AND UACI VALUES FOR A VARIETY OF VISUAL IMAGERY

SL. No	Image	NPCR Proposed	UACI proposed	NPCR [1]	UACI [1]
1	Leena	99.6834	33.6995	99.6632	33.6992
2	5.1.09	99.5633	33.5223	99.5214	33.5125
3	5.1.10	99.2897	33.5228	99.5523	33.5221
4	5.1.11	99.2689	33.2261	99.6016	33.1921
5	5.1.12	99.5897	33.2964	99.5437	32.9918
6	5.1.13	99.6458	33.2982	99.5219	33.1582

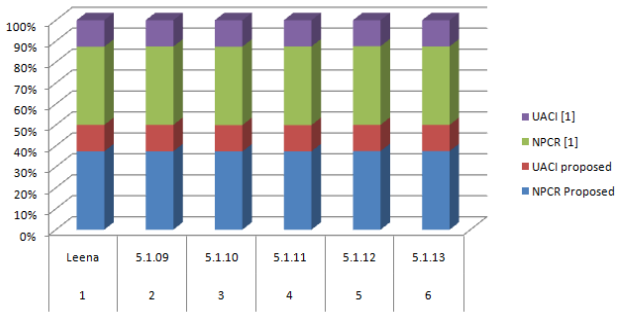


Figure 6. Graphical analysis of NPCR and UACI measures between the proposed and existing scheme.

D. Comparison Analysis with Other Techniques

For checking the efficiency, the security parameters like correlation coefficient, NPCR, UACI and entropy of the proposed approach is outlined and compared with Mohamed *et al*. [3], Gad *et al*. [2], Moysis *et al*. [4], Shafique *et al*. [22], Li *et al*. [24] and Qayyum *et al*. [26]. The results are formulated and captured in the Table V. It can be seen from Table V that the results are satisfactory from the other existing techniques.

TABLE V. NPCR AND UACI VALUE FOR DIFFERENT VISUAL IMAGES AVAILABLE IN USC-SIPI IMAGE DATABASE

Tehniques	Horizontal Corr.	Vertical Corr.	Diagonal Corr	NPCR	UACI	Entropy
Proposed System	0.0001121	−0.000212226	0.0004122	99.683426	33.6995	7.98992
[3]	0.00022	0.00045	0.00241	99.62	33.44	7.9829
[2]	−0.00501	−0.0012	0.00195	99.62	33.52	7.9972
[4]	0.0046	0.0063	0.0023	--	--	--
[22]	0.0259	−0.0690	−0.0617	--	--	7.9476
[24]	0.0016	0.0025	0.0003	--	--	--
[26]	--	--		99.61	33.49	7.9973
[34]	0.0060	0.0016	0.0031	99.71	33.54	7.9991

From Table V, it can be seen that the Horizontal Corr., Vertical Corr. and Diagonal Corr. generated are better than the existing schemes. The NPCR value obtained is 99.68 which is higher than that of the other techniques. The UACI value obtained is 33.6995 which is higher than 33.44, 33.52 and 33.49.

E. Performance Analysis

The performance of the proposed technique in terms of time has been calculated for different size of the image. The experiment was carried out using the hardware and software specifications listed below. The Wolfram Mathematica 11 kernel is chosen with the Windows 10 (64-bit) operating system. Intel(R) Pentium(R) processor running at 3.80 GHz with 8 GB of RAM. The time

complexity is computed and captured in the Table VI and a comparison is detailed in Table VI and Fig. 7 with the existing technique Bhattacharjee *et al*. [1]. It has been observed from Table VI that due to the addition of fuzzy steps, the time complexity of the existing algorithm has been increased by some milliseconds.

TABLE VI. PERFORMANCE COMPARISON ANALYSIS BETWEEN THE PROPOSED TECHNIQUE WITH [1]

Image Name	Proposed Method	Bhattacharjee *et al*. [1]
5.1.09	3.345	3.241
5.1.10	3.641	3.022
5.1.11	3.216	3.015
5.1.12	3.502	3.102
5.1.13	3.258	3.023
5.1.14	3.658	3.068
5.2.08	10.346	10.908
5.2.09	12.014	11.646
5.2.10	11.256	11.760
7.1.01	11.985	11.62
7.1.02	11.021	10.887
7.1.03	12.015	11.57
7.1.04	12.326	12.261
7.1.05	11.978	11.086
7.1.06	11.897	11.152
7.1.07	11.569	11.191
7.1.08	11.012	10.948
7.1.09	10.968	10.901
7.1.10	11.659	11.058

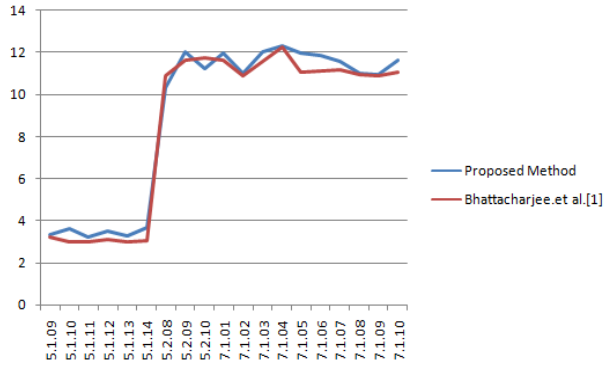


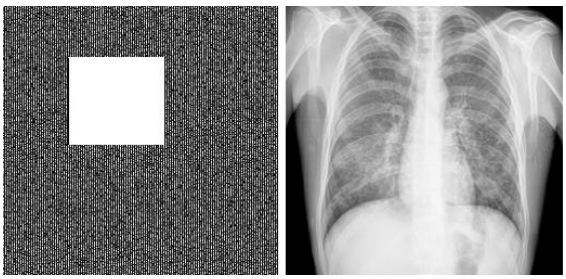
Figure 7. Performance complexity (Graphical analysis) captured between the proposed method with Bhattacharjee *et al.* (2022) [1].

F. Robustness Analysis

In order to check the robustness of the encryption technique, we have experimented to see the quality of the decrypted image when the encrypted image is subjected for a data loss attack.

The encrypted image that loses 1/9 of the image information is shown in Fig. 8(b). Fig. 8(c) shows that even after losing 1/9 of the information, the decryption quality is still good. The decrypted image is both easy to recognise and quite close to the original image Fig. 8(a). This indicates that the proposed fuzzy based encryption scheme is resistant to attacks involving data loss.

(a)



(a) (b)

Figure 8. (a) Original Image (b) Encrypted Medical Image with data lost. (c) Decrypted data lost image.

IV. CONCLUSION

In this study, we proposed a way for dynamically altering the logistic map's reproduction rate, making it very difficult for an unauthorised user to access the data. The proposed method was used in this paper to improve one of the existing techniques, and it is clear from the findings that security parameters have changed without compromising data integrity. The correlation coefficient value appears from −0.0002167 to −0.0001121 in horizontal direction pixels when fuzzy is applied. In the vertical direction, there is a gain of −0.0001121 from 0.0053385; in the diagonal direction, the value appears to be 0.0004122 from 0.0006699 when fuzzification stages are added to the existing method. The NPCR value is raised from 99.6632 to 99.6834. The change in UACI value from 33.6992 to 33.6652. This research work recommends that fuzzification of the reproduction rate parameter increases the security of the encryption techniques and can resist statistical and other types of attacks.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

S.B. wrote the manuscript. M.G., S.B., and B.C. were involved in study design and performed the experiment. All authors have gone through the manuscript and approved the final version

REFERENCES

[1] M. Gad, E. A. A Hagras, H. Soliman, and N. A. Hikal, "A new parallel fuzzy multi modular chaotic logistic map for image encryption," *Int. Arab J. Inf. Technol*., vol. 18, no. 2, pp. 227–236, Mar. 2021.

[2] A. G. Mohamed, N. O. Korany, and S. E. El-Khamy, "New DNA coded fuzzy based (DNAFZ) S-boxes: application to robust image encryption using hyper chaotic maps," *IEEE Access*, vol. 9, pp. 14284–14305, Jan. 2021.

[3] L. Moysis, C. Volos, S. Jafari, J. M. Munoz-Pacheco, J. Kengne, K. Rajagopal, and I. Stouboulos, "Modification of the logistic map using fuzzy numbers with application to pseudorandom number generation and image encryption," *Entropy*, vol. 22, no. 4, April 2020.

[4] P. Mani, R. Rajan, L. Shanmugam, and Y. H. Joo, "Adaptive control for fractional order induced chaotic fuzzy cellular neural networks and its application to image encryption," *Information Sciences*, vol. 491, pp. 74–89, July 2019.

[5] R. Hosseinzadeh, M. Zarebnia, and R. Parvaz, "Hybrid image encryption algorithm based on 3D chaotic system and choquet fuzzy integral," *Optics Laser Technology*, vol. 120, Dec. 2019.

[6] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering*, vol. 27, pp. 15–43, 2020.

[7] J. P. Cohen, P. Morrison, and L. Dao, "COVID-19 image data collection," arXiv reprint, arXiv:2003.11597, 2020.

[8] S. E. El-Khamy, N. O. Korany, and A. G. Mohamed, "A new fuzzy-DNA image encryption and steganography technique," *IEEE Access*, vol. 8, pp. 148935–148951, August 2020.

[9] S. Abdullah, S. Ayub, I. Hussain, B. Bedregal, and M. Y Khan, "Analyses of S-boxes based on interval valued intuitionistic fuzzy sets and image encryption," *International Journal of Computational Intelligence Systems*, vol. 10, no. 1, pp. 851–865, 2017.

[10] K. Ratnavelu, M. Kalpana, P. Balasubramaniam, K. Wong, and P. Raveendran, "Image encryption method based on chaotic fuzzy cellular neural networks," *Signal Processing*, vol. 140, pp. 87–96, 2017.

[11] H. M. M. Miss and P. V. C Miss, "Fuzzy logic based image encryption for confidential data transfer using (2, 2) secret sharing scheme," *Procedia Computer Science*, vol. 78, pp. 632–639, 2016.

[12] X. Chen and C. J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping," *Saudi journal of Biological Sciences*, vol. 24, no. 8, pp. 1821–1827, 2017.

[13] A. Souyah and K. M. Faraoun, "An image encryption scheme combining chaos-memory cellular automata and weighted histogram," *Nonlinear Dynamics*, vol. 86, no. 1, pp. 639–653, 2016.

[14] G. M. Kumar and V. Chandrasekaran, "A novel image encryption scheme using Lorenz attractor," in *Proc. 4th IEEE Conference on Industrial Electronics and Applications*, 2009, pp. 3662–3666.

[15] S. Karpate and A. Barve, "A novel encryption algorithm using chaotic Lorenz attractor and Knights tour," in *Proc. the Sixth International Conference on Computer and Communication Technology 2015*, 2015, pp. 323–327.

[16] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017.

[17] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Optics & Laser Technology*, vol. 115, pp. 257–267, July 2019.

[18] A. P. Kari, A. H. Navin, A. M. Bidgoli, and M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," *Multimedia Tools and Applications*, vol. 80, no. 2, pp. 2753–2772, Sep. 2021.

[19] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letters*, vol. 31, no. 5, pp. 347–354, Apr. 2010.

[20] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin, and S. Liu, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," *Optics Communications*, vol. 284, no. 1, pp. 123–128, Jan. 2011.

[21] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *The European Physical Journal Plus*, vol. 133, no. 8, pp. 1–16, Aug. 2018.

[22] Y. Hui, H. Liu, and P. Fang, "A DNA image encryption based on a new hyperchaotic system," *Multimedia Tools and Applications*, pp. 1–25, Feb. 2021.

[23] P. Mishra, C. Bhaya, A. K. Pal, and A. K. Singh, "A medical image cryptosystem using bit-level diffusion with DNA coding," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–22, Aug. 2021.

[24] A. Majumdar, A. Biswas, A. Majumder, S. K. Sood, and K. L. Baishnab, "A novel DNA-inspired encryption strategy for concealing cloud storage," *Frontiers of Computer Science*, vol. 15, no. 3, pp. 1–18, Dec. 2021.

[25] P. K. Naskar, S. Bhattacharyya, K. C. Mahatab, K. G. Dhal, and A. Chaudhuri, "An efficient block-level image encryption scheme based on multi-chaotic maps with DNA encoding," *Nonlinear Dynamics*, vol. 105, no. 4, pp. 3673–3698, Aug. 2021.

[26] M. Roy, S. Chakraborty, K. Mali, D. Roy, and S. Chatterjee, "A robust image encryption framework based on DNA computing and chaotic environment," *Microsystem Technologies*, vol. 27, no. 10, pp. 3617–3627, Jan. 2021.

[27] S. Pankaj and M. Dua, "A novel ToCC map and two-level scrambling-based medical image encryption technique," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 10, no. 1, pp. 1–19, July 2021.

[28] J. Wang, X. Zhi, X. Chai, and Y. Lu, "Chaos-based image encryption strategy based on random number embedding and DNA-level self-adaptive permutation and diffusion," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 16087–16122, Feb. 2021.

[29] J. P. Cohen, P. Morrison, L. Dao, K. Roth, T. Q. Duong, and M. Ghassemi, "COVID-19 image data collection: Prospective predictions are the future," arXiv preprint arXiv:2006.11988, 2020.

[30] N. Iqbal, R. A. Naqvi, M. Atif, M. A. Khan, M. Hanif, S. Abbas, and D. Hussain, "On the image encryption algorithm based on the chaotic system, DNA encoding, and castle," *IEEE Access*, vol. 9, pp. 118253–18270, Aug. 2021.

[31] X. Yan, X. Wang, and Y. Xian, "Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10949–10983, Jan. 2021.

[32] A. Kamrani, K. Zenkouar, and S. Najah, "A new set of image encryption algorithms based on discrete orthogonal moments and Chaos theory," *Multimedia Tools and Applications*, vol. 79, pp. 20263–20279, Apr. 2020.

[33] H. Karmouni, M. Sayyouri, and H. Qjidaa, "A novel image encryption method based on fractional discrete Meixner moments," *Optics and Lasers in Engineering*, vol. 137, Feb. 2021.

[34] B. Xiao, J. Luo, X. Bi, W. Li, and B. Chen, "Fractional discrete Tchebyshev moments and their applications in image encryption and watermarking," *Information Sciences*, vol. 516, pp. 545–559, Apr. 2020.

[35] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map," *The Visual Computer*, vol. 39, no. 3, pp. 1027–1044, Jan. 2023.

[36] M. A. Tahiri, H. Karmouni, A. Bencherqui, A. Daoui, M. Sayyouri, H. Qjidaa, and K. M. Hosny, "New color image encryption using hybrid optimization algorithm and Krawtchouk fractional transformations," *The Visual Computer*, pp. 1–26, Dec. 2022.

[37] C. Zhao, T. Wang, H. Wang, Q. Du, and C. Yin, "A novel image encryption algorithm by delay induced hyper-chaotic chen system," *The Journal of Imaging Science and Technology*, Jan. 2023.

[38] X. Y. Wang, X. L. Wang, L. Teng, D. H. Jiang, and Y. Xian, "Lossless embedding: A visually meaningful image encryption algorithm based on hyperchaos and compressive sensing," *Chinese Physics B.*, vol. 32, no. 2, 2023.

[39] D. Zhang, L. Chen, and T. Li, "Hyper-chaotic color image encryption based on 3D orthogonal Latin cubes and RNA diffusion," *Multimedia Tools and Applications*, pp. 1–24, May 2023.

[40] Y. Huang and L. Zhou, "A hyper-chaos-based image encryption scheme with double parity alternate scrambling," *Multimedia Tools and Applications*, pp. 1–15, Apr. 2023.

[41] Z. Liang, Q. Qin, C. Zhou, and S. Xu, "Color image encryption algorithm based on four-dimensional multi-stable hyper chaotic

system and DNA strand displacement," *Journal of Electrical Engineering & Technology*, vol. 18, no. 1, pp. 539–559, July 2023.
[42] K. U. Shahna, "Novel chaos based cryptosystem using four-dimensional hyper chaotic map with efficient permutation and substitution techniques," *Chaos, Solitons & Fractals*, vol. 170, no. 113383, May 2023.
[43] S. Bhattacharjee, M. Gupta, and B. Chatterjee, "Time efficient image encryption-decryption for visible and COVID-19 X-ray images using modified chaos-based logistic map," *Applied Biochemistry and Biotechnology*, pp. 2395–2413, Sep. 2022.