Computationally efficient image encryption technique based on selective pixel diffusion

Malik Obaid Ul Islam
Dept. of Electronics and IT.
University of Kashmir
Srinagar, India
malikobaid044@gmail.com

Shabir A. Parah
Dept. of Electronics and IT
University of Kashmir
Srinagar, India
shabireltr@gmail.com

Bilal A. Malik
Institute of Technology Zakura
Srinagar, India
bilalmalik@kashmiruniversity.ac.in

Abstract— Medical images play a vital role in disease diagnosis. When the medical images are communicated through an insecure transmission channel, their chances of being accessed by an unauthorized user increase resulting in the loss of patients' sensitive personal data. Thus, providing security to such image data while transmitting it over an insecure communication network becomes crucial. This work presents a computationally efficient cryptosystem for encrypting medical images. The encryption process consists of multiple phases. In the first phase the control parameters and initial values for the various chaotic maps used, are evaluated. This phase is followed by encryption in which these evaluated values are used to obtain the chaotic sequences for encryption. In the subsequent phases, we make use of a new approach of selective, pixel-dependent diffusion to obtain the cipher image. The effectiveness of our cryptosystem is evaluated using security analysis and execution time analysis. The obtained outcome shows a high-security level compared to already existing state-of-the-art techniques. In addition, the computational complexity of our scheme is very small (0.1sec for encrypting a 256×256 image) making it suitable for real-time smart health applications.

Keywords— Lightweight Image Encryption, Chaotic Maps, IoMT, Real-Time Application

I. INTRODUCTION

Today's internet-coupled devices are intended to improve effectiveness, lower care costs, and provide better results in healthcare. With their ability to collect, analyze and transmit health data such as medical images, IoMT tools are rapidly altering the healthcare system. For patients and clinicians, these applications are playing a central part in tracking and preventing chronic illnesses [1]. Once this data is sent over the insecure transmission channel, its chances of being accessed by an illegitimate user increase, resulting in various security challenges. So secure communication over an insecure transmission channel is very important [2, 3]. A lot of data medical data breaches have been reported recently [4]. This makes secure communication of electronic health records like medical images with integrity, legitimacy, availability, and privacy very much essential. Encryption is an effective process to guarantee medical image security by altering the original medical image into a cipher image using various secret keys. Without having secret keys, the adversary cannot reinstate the original image. Compare with textual information, images have more redundancy, non-uniform distribution of pixels, a huge amount of data, and high correlation among neighboring pixels which makes traditional cryptosystems like Advanced Encryption Standard (AES), Data Encryption Standard (DES) [5,6] not convenient in the field of real-time image cryptography. Furthermore, these systems are very secure, but have high computational complexity, and are not applicable for real-time applications due to a huge number of encryption rounds. To resolve this issue, researchers have suggested various image cryptosystems as in [7]. The authors present a medical image cryptosystem based on image splitting followed by a zigzag pattern, rotation, and random permutation. This scheme is computationally complex and is susceptible to a brute-force attack. A medical image encryption algorithm based on cubic-logistic map, discrete wavelet transforms (DWT) and bit-plane extraction is presented in [8]. The use of DWT makes the process computationally inefficient and cannot be applied to securing patient data in real-time application. In [9] the authors present an image encryption scheme based on a 2D logistic-modulated -sine-coupling-logistic chaotic map in which the original images undergo two round row and column scrambling followed by two round row and column diffusion. The suggested technique offers a high level of security, but it has high computational complexity and can't be used for battery-driven IoMT devices. In [10], an image cryptosystem based on multiple chaotic S-boxes created using Chebyshev chaotic map has been put forward. The security of the techniques lies in the number of substitution boxes applied, more the substitution boxes, the more randomness is added. However, increases the computational cost and therefore may not remain sufficient for limited resource devices in real-time applications. In [11], a new image encryption scheme is offered based on discrete wavelet transform and hyperchaotic maps. The suggested scheme displays high security and large key space. However, the utilization of high dimensional (HD) chaotic maps along with discrete wavelet transform increases the computational cost and execution time which makes it incompetent for real-time processing. Among these approaches, the spatial domain-based approach is the most effective and reliable one for lightweight cryptosystems compared to the existing approaches that have high computational cost and therefore not applicable in real-time applications. Among various spatial domain techniques chaos-based (1D and HD) spatial domain image encryption approach is the best one fetching excellent results [12]. Because of their uncomplicated structure, small implementation time, and ease of application [13]one-dimensional chaotic maps are extensively applied in cryptosystems. Subsequently, many researchers have suggested an enhanced version of prevailing 1D chaotic maps to overcome the shortcomings of simple 1D chaotic maps [14].

978-1-6654-9291-1/22/&31.00©2022IEEE

In this work, we propose an efficient lightweight image encryption algorithm based on the combination of improved 1D chaotic maps like the logistic-sine system, improved sine-tangent system, Tent-logistic system, and hash functions. The encryption is performed in five phases, in the first phase the key control parameters and initial values for the improved 1D chaotic maps are evaluated, in the second phase the chaotic sequences are generated using different chaotic maps, in the third phase confusion operation is performed using 1D improved chaotic map. The last two phases involve selective pixel diffusion for the generation of the cipher image. The experimental outcomes confirmed that the proposed image encryption system is fast such as the encryption time of the image with size $256 \times 256$is only 0.10 seconds. Furthermore, it provides better security compared to the previously existing state-of-the-art techniques.

The key contributions of our proposed scheme are summarized as follows:

- Our scheme makes use of lower dimensional improved chaotic systems having lower computational complexity than hyperchaotic systems. Besides, the maps used have a large chaotic range and are fast which makes them applicable for protecting patients' data in real-time processing.
- The proposed cryptosystem is lightweight and provides adequate security to medical images making it a good candidate for IoMT applications.

The remaining portion of the paper is organized as follows. Section 2 describes the preliminaries. In section 3 the proposed image encryption technique is presented. Section 4 presents the experimental results and security analysis. Finally, the conclusion of the proposed scheme is drawn in section 5.

II. PRELIMINARIES

The fundamental associated with the proposed scheme has been explicated in this section. Various chaotic maps along with the hash function have been explained in detail.

A. Chaotic map

Chaotic maps are mathematical evolution functions that exhibit chaotic behavior. These maps are applied for creating chaotic sequences for information security applications [15]. The three chaotic maps applied in the proposed cryptosystem are Tent-LogisticSystem (TL), Improved Sine-Logistic System (ISL), and Improved Sine-Tangent System (IST). For the solution of problems faced by the Tent chaotic map and logistic map in terms of their chaotic performance and chaotic range, [16] suggested a new compound chaotic system by joining together the logistic and Tent map resulting in a new system known as the Tent-logistic system. Furthermore, its chaotic region is sufficiently larger than the logistic and tent map. More details on ISL and IST can be had from [17] and [18] respectively. These maps are computationally very fast and efficient making them applicable for real-time applications.

B. Cryptographic Hashing

A hash function is a process that takes variable length input data and converts it into a fixed length of output sequence. As it has several data safety applications, besides that it is capable to resist all well-known cryptanalytic attacks, additionally, these functions are computationally fast. The hash function utilized in the proposed work is Secure Hash Algorithm-384 (SHA-384) [19].

III. PROPOSED SCHEME

In the proposed encryption scheme, the original plain image undergoes three processes as illustrated in Fig.1. Initially, the permutation operation is performed using the 1D improved chaotic map in such a way that the chaotic behavior obtained depends on the input image making the cryptosystem image sensitive. This operation is followed by two rounds of selective inter-pixel dependent diffusion operation resulting in the final crypto image.

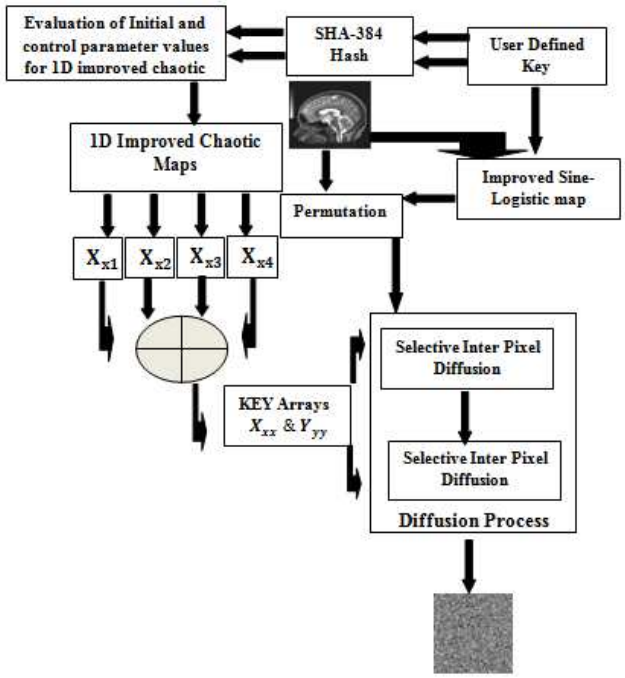


Fig.1 Block diagram of the proposed cryptosystem

A. Generation of Control and Initial Values

Step 1: As we know hash functions can take variable length input to produce fixed-length output using that property we have selected two strings S_1 and $S_2$of 37 characters each, apply these two strings as input to hash function SHA-384 separately to obtain two hash values of length 384 bits each i.e. 48 decimal elements respectively as S_{hash1} and S_{hash2} .

Step 2: From S_{hash1} and S_{hash2} generate another two sequences S_{R1} and S_{R2} of length 1×40 as follows

$$S_{R1}(i) = \mathrm{mod}\left(\left(S_{hash1}(i) \oplus S_{hash2}(48-i)\right), 256\right) \oplus \mathrm{mod}\left(\left(S_{hash1}(i) \oplus S_{hash2}(1+i)\right), 256\right) \quad (1)$$

$$S_{R2}(i) = \begin{cases} S_{hash2}(i+3) & : i = \text{even} \\ S_{hash1}(i) & : i = \text{odd} \end{cases} \quad (2)$$

Step 3: Concatenate the four generated sequences to obtain a single sequence R_R of length 1×176.

Step 4:Generate another sequence $Z_1$of 6000 elements by iterating an improved Sine-Logistic system 6000 times under its

chaotic behavior with an initial value Z_0 and control parameter b.

Step 5: The generated sequence is processed as

$$Z_1 = \text{floor}\left(\text{mod}\left((Z_1 \times 10^8), 256\right)\right) \quad (3)$$

Step 6: Another sequence Z_2 of length 1×6000 is generated using sequence Z_1 as

$$Z_2(i) = \begin{cases} \text{mod}\left((Z_1(i) \oplus Z_1(6000 - i + 2)), 256\right) \\ : i = \text{even} \\ \text{mod}\left((Z_1(i) \oplus Z_1(1 + i)), 256\right) \\ : i = \text{odd} \end{cases} \quad (4)$$

Step 7: Another sequence F_s is obtained by concatenating generated sequencesZ_1, R_R and Z_2 resulting in a sequence oflength1×12176. From F_s randomly select 2222 decimal elements to obtain sequence g of length1×1112.

$$g = F_{S_X} \ : \ F_{S_{X+2221}} \quad (5)$$

Step 8: Again, from sequence g we obtain another two sequences of length 1×556 respectively as

$$SL_1 = g(i) \ : i = \text{odd} \quad (6)$$

$$SL_2 = g(i) \ : i = \text{even} \quad (7)$$

Step 9: For another two sequences S_1 and S_2 of length 1×128 select randomly two arrays from SL_1 and SL_2 of length1×256 respectively and are generated as

$$S_1 = SL_1(i) \oplus SL_2(i) \ : \ i = \text{odd} \quad (8)$$

$$S_2 = SL_1(i) \oplus SL_2(i) \ : \ i = \text{even} \quad (9)$$

Step 10: Another sequence S_3 of length 1×128 is generated as

$$S_3(i) = \begin{cases} \text{mod}\left(\left(\begin{matrix} \text{mod}\left(\begin{pmatrix} S_1(i) \\ +S_2(i) \\ +SL_1(i) \\ +SL_2(i) \end{pmatrix}, 256\right) \\ \times \text{mod}\left(\begin{pmatrix} SL_1(i+2) \\ +SL_2(i+2) \end{pmatrix}, 256\right) \end{matrix}\right), 256\right) \\ : i = \text{odd} \\ \text{mod}\left(\left(\begin{matrix} \text{mod}\left(\begin{pmatrix} S_1(i) \\ +S_2(i) \\ +SL_1(i) \\ +SL_2(i) \end{pmatrix}, 256\right) \\ \times \text{mod}\left(\begin{pmatrix} SL_1(i+1) \\ +SL_2(i+1) \end{pmatrix}, 256\right) \end{matrix}\right), 256\right) \\ : i = \text{even} \end{cases} \quad (10)$$

Step 11: Yet another two sequences Sq_1 and Sq_2 of length are 1×128 are obtained as

$$Sq_h = S_h \oplus S_{h+1} \quad (11)$$

Where $h = 1{:}2$

Step 12: Two key values are obtained as

$$j_c = \text{sum}(SL_c) \quad (12)$$

Where $c = 1{:}2$

Step 13: The initial values $x_{ii1-4}$and control parametersAl_{1-4} for the applied chaotic maps are determined using equations 13, 14 and 15

$$x_{iip} = mod\left(\frac{mod(j_1, R_{Kp})}{256}, 1\right) \quad (13)$$
$$p : 1 \,\&\, 3$$

$$x_{iip} = mod\left(\frac{mod(j_2, R_{Kp})}{256}, 1\right) \quad (14)$$
$$p : 2 \,\&\, 4$$

Where R_{Kp} are four key values generated from SL_1 and SL_2 by performing bit xor operation between arbitrarily selected elements.

$$Al_x = \text{mod}\left(\left(\left(T_x + \left(\text{double}\left(\left(\left(\left(\begin{matrix} Sq_1(1, x+a) \\ \oplus Sq_2(1, x+a+1) \\ \oplus Sq_1(1, x+a+2) \\ \oplus Sq_2(1, x+a+3) \\ \oplus Sq_1(1, x+a+4) \end{matrix}\right)\right)\right)\right)\right) / 256\right)\right), 8\right) \quad (15)$$

Where $x \in [1{:}4]$ and a is a random positive integer belonging to the sequence Sq indexes.

B. Chaotic Sequence generation using the evaluated control parameters and initial values:

Step 1: Generate four sequences P_1, P_2, P_3 and P_4 of length $1 \times$ mn where m and n are the height and width of the input original image, by iterating two different improved 1D chaotic maps i.e.sine-tangent system and tent-logistic system, mn times under their chaotic behavior.

Step 2: The generated sequences are processed as

$$X_{xu} = \text{floor}\left(\text{mod}\left((P_u \times 10^8), 256\right)\right) \quad (16)$$

Where $u = 1{:}4$

$$X_{xx} = \text{mod}\left(\left(\text{mod}\left(\left(\left(\begin{pmatrix} X_{x1}(i) \\ +X_{x3}(i) \end{pmatrix} \times 10^8\right), 256\right) + \begin{pmatrix} X_{x1}(i) \\ +X_{x3}(i) \end{pmatrix}\right), 256\right) + X_{x3}(i)\right), 256\right) \quad (17)$$
$$i = 1{:}mn$$

$$Y_{yy} = \text{mod}\left(\left(\text{mod}\left(\left(\left(\begin{pmatrix} X_{x2}(i) \\ +X_{x4}(i) \end{pmatrix} \times 10^8\right), 256\right) + \begin{pmatrix} X_{x2}(i) \\ +X_{x4}(i) \end{pmatrix}\right), 256\right) + X_{xx}(i)\right), 256\right) \quad (18)$$
$$i = 1{:}mn$$

C. Permutation Operation

The plain image I is subjected to a permutation operation by which the pixel location is changed to increase security by repositioning the pixels arbitrarily which results in making the image visually unreadable. Besides, this process breaks the correlation among the neighboring pixels by reducing its value closer to the ideal value of zero. The steps involved in this operation are as

Step 1: Generation of the chaotic sequence H_1using a sine-logistic system whose control parameter Al_5 is taken from the key K and the initial value x_{ii5} is made reliant on the original plain image to make the cryptosystem tremendously sensitive. The initial value is computed as

$$x_{ii5} = \mathrm{mod}\left(\left(\frac{\left(\mathrm{mod}\left(\left(\sum_1^{R\times C} I\right) + \left(\sum_1^{R/2\times C/2} I\right), 255\right)\right)}{10000}\right), 1\right) \quad (19)$$

Step 2: These control parameters and initial value i.e.Al_5 and x_{ii5} are then substituted into the sine-logistic system and then iterating this sine-logistic system $m \times n$ times to obtain a pseudo-random sequence H_1.

Step 3: Next the pixel loci of the substituted image are permuted to confirm that the pixels don't remain in their actual loci. This operation helps in breaking the correlation between the neighboring pixels by reducing its value closer to zero. The various steps required are as under

- Acquire pixel permutation of the selective pixel-diffused image utilizing the random sequence H_1generated using a sine-logistic system under its chaotic behavior.
- Express the whole substituted image as a 1-D sequence I^{1D}.Organize the chaotic sequence H_1.in
- increasing order to achieve the index string $H_{1_{index-seq}}$.
- Finally jumble I^{1D} as per the index order $H_{1_{index-seq}}$ as

$$I^{1D}{}_j = I^{1D}{}_{H_{1_{index-seq}}} : \quad j \in [1, m \times n] \quad (20)$$

- Reshape the jumbled sequence to obtain the required permuted image I_p.

D. First round of diffusion

Step 1: Initialize two values as

$$S^1 = \sum_i^{mn} I_p(i) \quad (21)$$

$$S^2 = 0 \quad (22)$$

Step 2: The selective pixel diffusion of the permuted image I_p is performed on every pixel, the operations performed on individual pixels differ as per the even and odd pixel index and can be displayed as a pseudo-code

$$C(1) \leftarrow \begin{pmatrix} \left(\left(I_p(1) \oplus X_{xx}(1)\right) \oplus Y_{yy}\right) \\ \oplus \left(mod\left((S^1 + X_{xx}(1)), 256\right)\right) \end{pmatrix}$$

For $i = 1{:}2{:}mn$

$S^1 = S^1 - I_p(i)$

$S^2 = S^2 + C(i-1)$

If $mod(i,2) = 1$

$$C(i) \leftarrow \left(I_p(i) \oplus \left(mod\left((S^1 + X_{xx}(i)), 256\right)\right)\right) \oplus \mathrm{mod}\left(\left(S^2 + Y_{yy}(i)\right), 256\right) \oplus \mathrm{mod}\left(\left(S^2 + S^1 + C(i-1)\right), 256\right)$$

Else if $mod(i,2) \neq 1$

$$C(i) \leftarrow I_p(i) \oplus \mathrm{mod}\left(\left(S^1 + X_{xx} + C(i-1)\right), 256\right)$$

end

end

end

E. Second Round of Substitution Process

The obtained pixel-defused image C undergoes the second round of diffusion operation in which the selective pixel diffusion is performed on each induvial pixel based on pixel index and can be explained using the corresponding pseudo-code as

$$I_{cipher}(1) \leftarrow \begin{pmatrix} \left(\left(C(1) \oplus X_{xx}(1)\right) \oplus Y_{yy}\right) \\ \oplus \left(mod\left((S^1 + X_{xx}(1)), 256\right)\right) \end{pmatrix}$$

For $i = 1{:}2{:}mn$

$S^1 = S^1 - C(i)$

$S^2 = S^2 + I_{cipher}(i-1)$

If $mod(i,2) = 1$

$$I_{cipher}(i) \leftarrow C(i) \oplus \left(I_{cipher}(i-1)\right)$$

Else if $mod(i,2) \neq 1$

$$I_{cipher}(i) \leftarrow \left(C(i) \oplus \left(mod\left((S^1 + X_{xx}(i)), 256\right)\right)\right) \oplus \mathrm{mod}\left(\left(S^2 + Y_{yy}(i)\right), 256\right) \oplus \mathrm{mod}\left(\left(S^2 + S^1 + I_{cipher}(i-1)\right), 256\right)$$

end

end

end

At the end of this phase, we get the cipher image I_{cipher}.

F. Decryption Phase

At the receiver end the cipher image I_{cipher} needs to be decrypted to retrieve the original image I using the original key and by inverting the encryption stages. The decryption process is described as follows:

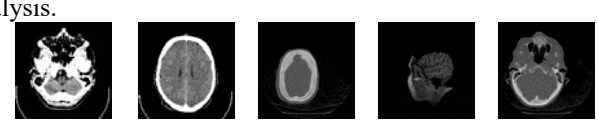
Step1: The obtained cipher image I_{cipher} initially undergoes reverse selective pixel diffusion operation i.e. the inverse process of the second round of substitution process to obtain C.

Step 2: The diffused image C is subjected to another phase of diffusion i.e. the inverse of the process performed in the first round of diffusion to retrieve I_p.

Step 3: Return each pixel of the I_p at its original position by performing a reverse permutation operation to obtain the required original image I.

IV. EXPERIMENTAL OUTCOMES

Grayscale test medical images of different sizes have been used for experimentation. All the images used in this section are shown in Fig.2, in which all the images are taken from [20-21]. The proposed algorithm has been executed using MATLAB2016a on a computer system with Intel core i7-7700 CPU @ 3.60GHz processor and 8 GB RAM. The proposed scheme has displayed a higher level of efficiency and resistance to withstand all types of statistical attacks against other techniques. The parameters used for the evaluation consist of Information, Correlation Coefficient, Histogram Differential Attacks Analysis (NPCR and UACI), and key sensitivity analysis.



M.Ig1 M.Ig2 M.Ig3 M.Ig4 M.Ig5

Fig.2. Test Medical Images

A. Keyspace Analysis

The secret key utilized in the proposed cryptosystem consists of the 74-character string resulting in $122^{74} \approx 2^{518}$combinations and the initial value Z_0 and control parameters b and Al_5. These parameters are applied to the improved logistic-sine system to generate sequences for image encryption. Besides that, T_1, T_2, T_3, T_4 and T_5 are the constant key values utilized in several equations which makes the key space large enough to survive the brute force attack.

B. Key Sensitivity Analysis

In any cryptosystem, the cipher image should go through a complete change even if a minute alteration is done in the secret keys. To evaluate the key sensitivity of the suggested encryption technique, we encrypt the plain image with the original key and at the same time, we encrypt it applying the same key but having a one-bit change. The NPCR and UACI of the encrypted crypto images are evaluated and are shown in below Table 1. The values obtained above from the proposed encryption algorithm are closer to their ideal value which indicates that the proposed cryptosystem can effectively withstand differential attacks.

Table1: NPCR and UACI Test Outcomes After 1Bit Alteration

Test Images	M.Ig1	M.Ig2	M.Ig3	M.Ig4	M.Ig5
NPCR	99.60	99.62	99.63	99.64	99.60
UACI	33.43	33.51	33.56	33.33	33.48

C. InformationEntropy

The obtained randomness of the cipher image is determined by Shannon entropy [22]. The entropy results of the encrypted image as displayed in Table 2. From the outcomes, we can examine that all the attained entropy outcomes are very close to the ideal value 8, which demonstrates that it is impossible to obtain visual information.

Table2: Information entropy of medical crypto images and their comparison.

Test Images	Plain Image	Ref. [7]	Proposed
M.Ig1 (512×512)	2.1036	7.9993	7.9993
M.Ig2(512×512)	2.8321	7.9994	7.9994
M.Ig3(256×256)	4.6899	7.9974	7.9976
M.Ig4(256×256)	4.2243	7.9972	7.9973
M.Ig5(256×256)	5.1510	7.9977	7.9974

D. Analysis of correlation coefficient

The efficiency of the encryption algorithm is based on producing a cipher image with almost no correlation among the neighboring pixels. We evaluate the correlation coefficient among the randomly selected m pair of adjacent pixels from the image to be examined using the procedure [23]the results are listed in Table 3. While comparing we can find that the correlation among the adjacent pixels is almost zero indicating that the proposed cryptosystem can resist statistical attacks.

Table 3: Comparison with various methods in terms of correlation coefficient with pairs of pixels=5000

Test Images		M.Ig1	M.Ig2	M.Ig3	M.Ig4	M.Ig5
Plain image	H	0.9680	0.9724	0.9934	0.9574	0.9839
	V	0.9757	0.9851	0.9925	0.9676	0.9839
	D	0.9549	0.9654	0.9862	0.9398	0.9696
Ref.[7]	H	-	0.0182	0.0059	-0.0044	0.0298
	V	-	-0.0108	-0.0237	0.0046	0.0063
	D	-	0.0165	0.0080	0.0081	0.0012
Proposed	H	-0.0003	0.0007	0.0031	0.0024	-0.0037
	V	0.0024	-0.0010	0.0014	-0.0040	-0.0009
	D	0.0002	-0.0016	-0.0026	-0.0025	-0.0004

E. Analysis of the capability to resist Differential Attacks

The differential attack is one of the most effective attacks in cryptography. It is a selective plaintext attack that evaluates the probability of differential propagation of specific plaintext differential values in the encryption algorithm. It is substantiated by the unified average change intensity (UACI) and the number change rate (NPCR) [24]. The evaluated values after 1-bit alteration between the two input plain images and their comparison are shown in Table 4.

Table 4: Comparison in terms of NPCR and UACI results after 1-bit alteration in the plain image

Test Images		M.Ig1	M.Ig2	M.Ig3	M.Ig4	M.Ig5
Ref. [7]	NPCR	-	99.62	99.62	99.60	99.62
	UACI	-	33.44	33.48	33.45	33.49
Proposed	NPCR	99.61	99.62	99.60	99.61	99.60
	UACI	33.45	33.46	33.45	33.54	33.46

The values obtained above from the proposed algorithm are closer to their absolute value. The comparison drawn shows that the proposed encryption scheme can effectively resist differential attacks.

F. Analysis of Histogram

A histogram is a graphic means that is used to reveal the distribution of pixel intensity values of an image. The cipher image must have a uniform distribution such that the illegitimate user is unable to get any information from it. The histogram with spikes shows less randomness whereas uniform distributed pixel intensities are a sign of a reliable and secure cryptosystem and helps in resisting various statistical attacks. Fig. 3 shows that the proposed system is secure.

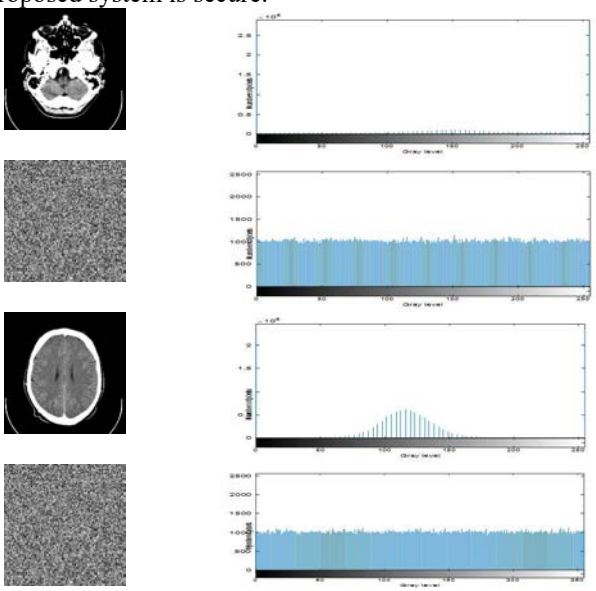


Fig.3: Histogram of Original image and their Cipher image

G. Evaluation of Computational Complexity Analysis

Encryption speed is an important parameter for evaluating the computational efficiency of the lightweight cryptosystem. The experiments were performed on MATLAB2016a with Intel core i7-7700 CPU @ 3.60GHz processor and 8 GB RAM as well as on MATLAB2016a with Intel core i3-6006U CPU @ 2GHz processor and 8GB RAM with windows 10 operating system. The average encryption time interval (Enc Time in seconds) is

evaluated for encrypting the 256×256 images n number of times. The results presented in Table5 prove that the proposed technique displays extremely high speed in contrast to other techniques thereby fulfilling the necessity of real-time processing. The analysis shows that our scheme has the potential to be implemented on hardware[27,28] so that it can be used for real-time applications

Table 5: Comparison with various other methods in terms of encryption speed

Scheme	Enc Time	Processor speed	RAM	MATLAB Version
Proposed	0.10	3.60 GHz	8 GB	MATLAB 2016a
Proposed	0.21	2.00 GHz	8 GB	MATLAB 2016a
Ref. [25]	0.38	3.30 GHz	8 GB	MATLAB 2016a
Ref. [26]	0.27	2.80 GHz	8 GB	MATLAB 2016b

V. CONCLUSION

This paper presents a computationally efficient image cryptosystem based on lower dimensional chaotic maps and hash function. The proposed cryptosystem makes use of selective pixel diffusion to yield an efficient and lightweight cryptosystem. The proposed system performance has been evaluated in terms of various objective parameters like entropy, correlation coefficient, histogram analysis, keyspace analysis, and key sensitivity. The results obtained show that our cryptosystem is highly effective in encrypting medical images at a fast rate while providing better security. A comparison with the state of the art shows that our scheme is a potent candidate for real-time image encryption in smart health applications.

Acknowledgments: The authors acknowledge the role of JK Science Technology & Innovation Council, Department of Science and Technology, Government of Jammu and Kashmir, for funding this work under grant number JKST&IC/SRE/874-77

REFERENCES

[1] P. Sarosh, S. A. Parah, B. A. Malik, M. Hijji and K. Muhammad, "Real-Time Medical Data Security Solution for Smart Healthcare," in IEEE Transactions on Industrial Informatics, 2022, doi: 10.1109/TII.2022.3217039.

[2] A. Ro., P. A Misra, & S. Banerjee "Chaos-based image encryption using vertical-cavity surface-emitting lasers,". Optik, Vol. Pp. 176, 119-131(2019).

[3] S. J Khan, and J. Ahmad "Chaos based efficient selective image encryption. "Multidimensional Systems and Signal Processing, Vol. 30(2), pp. 943-961 (2019).

[4] S.A.Parah, J.A. Sheikh, F. Ahad, G.M. Bhat(2018). High Capacity and Secure Electronic Patient Record (EPR) Embedding in Color Images for IoT Driven Healthcare Systems. In Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. Studies in Big Data, vol 30. Springer, Cham. https://doi.org/10.1007/978-3-319-60435-0_17

[5] D. Selent, ''Advanced encryption standard,'' Rivier Acad. J., vol. 6, no. 2, pp. 1–14, 2010.

[6] D. Coppersmith, ''The data encryption standard (DES) and its strength against attacks,'' IBM J. Res. Develop., vol. 38, no. 3, pp. 243–250, May 1994.

[7] T. S Kamal, M. K Hosny, M. T Elgindy, M. M Darwish, and M.M Fouda "A new image encryption algorithm for grey and color medical images," IEEE Access, Vol. 9, pp. 37855-37865 (2021).

[8] A. Shafique, J. Ahmed, M. U Rehman, and M. M Hazzazi "Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain," IEEE Access, Vol. 9, pp. 59108-59130 (2021).

[9] H. Zhu, Y. Zhao, and Y. Song "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption," IEEE Access, Vol. 7, pp. 14081-14098 (2019).

[10] I. Hussain, A. Anees, A. H Alkhaldi, M. Aslam, N. Siddiqui, and R. Ahmed, "Image encryption based on Chebyshev chaotic map and S8 S-boxes," Optica Applicata, Vol. 49 no. 2(2019).

[11] L. Ding, &Q. Ding, "A novel image encryption scheme based on 2D fractional chaotic map, DWT and 4D hyper-chaos," Electronics, Vol. 9 no. 8, pp. 1280(2020).

[12] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," Pattern Recognition Letters, Vol. 31 no.5, pp. 347-354(2010).

[13] W. Zhang, Z. Zhu, &H. Yu, "A symmetric image encryption algorithm based on a coupled logistic–bernoulli map and cellular automata diffusion strategy," Entropy, Vol. 21 no. 5, pp. 504(2019).

[14] M. K Khairullah, A. A Alkahtani, M. Z BinBaharuddin, & A. M Al-Jubari, "Designing 1D Chaotic Maps for Fast Chaotic ImagEncryption," Electronics, Vol. 10 no. 17, pp. 2116(2021).

[15] S.Patel, V.Thanikaiselvan, D. Pelusi, B. Nagaraj, R. Arunkumar, and R. Amirtharajan, "Colour image encryption based on customized neural network and DNA encoding," Neural Computing and Applications, Vol. 33 no.21, pp. 14533-14550(2021).

[16] Q. Lu, C. Zhu, and G. Wang, "A novel S-box design algorithm based on a new compound chaotic system," Entropy, Vol. 21 no. 10, pp. 1004(2019).

[17] Q. Lu, C. Zhu, and X. Deng, " An efficient image encryption scheme based on the LSS chaotic map and single S-box," IEEE Access, Vol 8, pp. 25664-25678(2020).

[18] A.Belazi, S.Kharbech, M. N. Aslam, M. Talha, W. Xiang, A. M Iliyasu, and A. A.Abd El-Latif, "Improved Sine-Tangent chaotic map with application in medical images encryption," Journal of Information Security and Applications, Vol. 66, pp. 103131(2022).

[19] T. Velmurugan, and S. Karthiga, "Security based Approach of SHA 384 and SHA 512 Algorithms in Cloud Environment".

[20] Category: Computed Tomography Images of Mikael Häggström's Brain. Accessed: Jul. 16, 2021. [Online]. Available: https://commons.wikimedia.org/wiki/

[21] The Stanford Volume Data Archive. Accessed: Jul. 19, 2021. [Online]. Available: https://graphics.stanford.edu/data/voldata/

[22] Y. Wu, J. P Noonan, and S. Agaian, "Shannon entropy based randomness measurement and test for image encryption ". arXivpreprintarXiv: pp. 1103.5520.

[23] Ahmad, J., & Ahmed, F. (2010). Efficiency analysis and security evaluation of image encryption schemes. computing, 23, 25.

[24] Wu, N. P. C. R. UACI randomness tests for image encryption, Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun, (1), 31.

[25] Q. Lu, C. Zhu, &X. Deng, " An efficient image encryption scheme based on the LSS chaotic map and single S-box," IEEE Access, Vol. 8, pp. 25664-25678(2020).

[26] X. Wang, &R. Si, "A new chaotic image encryption scheme based on dynamic L-shaped scrambling and combined map diffusion," Optik, Vol. 245, pp. 167658(2021).

[27] G. M. Bhat, M. Mustafa, S. A. Parah, & J. Ahmad, J. (2010). Field programmable gate array (FPGA) implementation of novel complex PN-code-generator-based data scrambler and descrambler. Maejo international journal of science and technology, 4(1), 125-135.

[28] G. M. Bhat, M. Mustafa, S. A. Parah, & J. Ahmad, J.(2009). VHDL modeling and simulation of data scrambler and descrambler for secure data communication. Indian Journal of Science and Technology, 2(10).