ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 11 (2021) No. 1, pp. 176-192
DOI:10.33168/JSMS.2021.0111

Building Enhanced Chaotic Map Encryption Method for Medical Information System

Rashmi Parameshachari, Supriya Maganahalli Chandramouli

Research Scholar, Sri Siddhartha Academy of Higher Education, Tumakuru, India
Associate Professor, Dept. of MCA, SSIT, Sri Siddhartha Academy of Higher Education, Tumakuru, India
rashmibdp@gmail.com, supriya.mc9@gmail.com

Abstract. The medical photographs, patient history, doctor's note, and clinical review contained in an electronic health record are highly sensitive data. Since it is vulnerable to many security problems, this data isn't normally sent to the network in its own way. Inside the medical picture, the proposed method used aggressive encryption and biplanes encryption to provide additional protection. Histogram process used for Region of Interest (ROI) output in medical imaging. To reduce the constant tension of the algorithm, the four high-level biplanes of the ROI component continue to push and distribute. The explosion of a plane carried out with the help of many turbulent systems is followed by diffusion operation. Furthermore, the medical images' accuracy is assured, restricting the amount of encryption time available (there must be limits for real-time applications). Experiments using a variety of medical imaging affirm the goals of our research. The evaluation and theoretical review results support the proposed addition's effectiveness in terms of encryption, confidentiality, and authenticity.

Keywords: Chaotic system. histogram, image encryption, information entropy, region of interest.

1. Introduction

With the advancement in the development of image processing equipment, photographic data, such as human images, is being collected and used in a variety of fields. Image processing equipment is also increasingly linked to network locations. Images are accurate and sensitive, which means that without the protection of privacy, data leaks, such as privacy breaches, and leaks of confidential information are possible. As such threats increase in complexity and number, privacy concerns grow, raising the need for image data to be stored and protected by encryption based on a security algorithm. The image encryption method can protect the security of photographs and protect the privacy of communications (Bang et al., 2016; Kumari, 2017; Jang and Lee, 2020). Many encryption techniques have been developed over the last few decades, including the Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and Advanced Encryption Standard (AES). However, because of the unique characteristics of image formats, such as large volumes of data, high throughput, and strong pixel interaction, those methods are better suited to text encryption than image encryption. The Chaotic system has properties like sensitivity to initial conditions and control parameters, periodic density points, and replication versatility that make it perfect for image encryption.

The volume of image data transmitted through the Internet has been increased due to the evolution in digital data communication and network technologies. Applying the conventional encryption algorithms directly on image data has limitations due to the intrinsic features of images. In recent years, many research papers have been published focusing on image encryption based on the proven techniques utilized in text message encryption. Among the several methods of image encryption, the methods based on permutation and substitution is simple and easy to implement. There are two ways to protect the image, one is the full encryption and the other one is selective encryption. Full encryption is defined as the complete image encryption used when required to perform encryption properly. Symmetric-based or clutter-based, maps encryption methods, and hyper chaos encryption and support, are currently being studied. Selective image encryption is used to protect sensitive information within the image. Selective encryption method is used to encrypt part of the image depending on different attributes such as image frequency (Xian and Wang, 2021).

Chaotic image encryption is mainly divided into two steps: scrambling and diffusion. Diffusion involves changing the pixel value of each pixel in a specific way to achieve the purpose of protecting image information. In its essence, diffusion is the process of changing the values of pixels. Scrambling involves exchanging the positions of pixels in the spatial domain with a selected fixed order or an ordering with random properties, which means that scrambling is the process of exchanging the pixel positions. This category of methods usually exchanges pixel positions to destroy the spatial correlation between pixels in the original plaintext,

thereby encrypting image information. Except for the commonly used chaos method, most methods of scrambling can be classified as scan methods. This method can start at a certain pixel point of the image and follow a set order with left, right, up, down, or oblique directions to rearrange all pixels of the image without repeating.

2. Literature Survey

Darwish (2019) described the unimaginable reduction in encryption techniques. This process selects the most important part of the image after the contourlet conversion. However the less important parts have lost the pressure by using a simple rule of thumb and arithmetic coding to make the image completely invisible.

Shakir (2019) introduces a new approach based on a map with a nonlinear view that combines Haar wavelet transform with Advanced Encryption Standard (AES) and pixel variables. The Haar wavelet transform is calculated from the first image in the proposed method to discover the image's various frequencies, i.e., the equilibrium (LL) and the details (LH, HL and HH).

Han (2019) et.al presents a novel design based on the concept of selective agnostic encryption to better protect social data based on block coding encryption with a prepared truncation system. By encrypting specifically a small portion of streams in the central part of this coding system, a high level of security and efficiency can be achieved for both.

Zhou et al. (2020) claimed a hidden ROI status. In the encryption process, ROI is a pixel rate that is adjusted to achieve the non-loss of medical imagery and to protect medical image data from loss.

Heidari et al. (2019) et.al introduced the preferred method of writing in detail for medical imaging. ROI (Reproductive Region) is often the most important part of medical photographs, which should be protected during delivery. The proposed approach encrypts the region successfully by exploiting small image planes with keys.

Khashan and Muath (2020) presented a preferred encryption system for encrypting maps on the edge of medical images. An edge access is used to extract the edge first. Then, to generate a large key space, a chaotic map is used. To encrypt the sequence of image blocks discovered, we propose a one-time algorithm. The proposed encryption system offers an appropriate percentage of encryption, according to test results. The proposed encryption system offers an appropriate proportion of encrypted image data, according to test results.

Afzal et al. (2020) proposed method has used two encryption methods namely, confusing encryption and bitplane encryption in the medical image which provides additional security to the image. While using cloud encryption (confusing) the proposed method ensures that cloud managers do not receive anything about the information contained in the information sent to them.

Khan and Jawad (2019) proposed strategies that start by dividing the descriptive

image into multiple blocks and calculating the integration coefficients for each block. The smart pixel XOR with random numbers generated on the skew tent map based on the predefined limit value has the highest proportional values. Finally, the entire image is rendered in a random sequence based on the chaotic map created by the TD-ERCS. Finally, the entire image is rendered in a random sequence based on the chaotic map created by the TD-ERCS.

Madhusudhan and Sakthivel (2020) described a medical image transfer algorithm based on Arnold's binary bits and maps. The proposed approach involves the approval and distribution process. Arnold's map used to encrypt selected part of medical images.

Khan and Fawad (2019) have used many confusing maps to propose the process of writing with novel illustrations. Suggested encryption adds confusion and spread to a given system which is one of the most important aspects of the encryption process.

Sankaradass et al. (2018) have proposed a ROI-encrypted grey image encryption. The ROI areas were first identified using the Sobel edge-finding operator, then subdivided into important and insignificant regions based on the number of edges present during each block. The Lorenz system (both confusing and scattering process) is then used to encrypt key regions, while the Fourth map is used to encrypt non-critical regions. Lorenz's system eventually released the entire image with new conditions to compel the final image to be encrypted.

Talhaoui et al. (2020) proposes a picture encryption program supported the troubled Bülban map. Unlike many existing programs, we wisely use this easy, chaotic map to get only a couple of numbers of rows and random columns. additionally, to further increase speed, we propose the processing unit from pixel level to row / column level. the safety of the new system is achieved through the replacement network, where we use circular rotation of rows and columns to interrupt the solid pixels of adjacent pixels. then, we combine XOR functionality with Module function to cover pixel values and stop any information leakage.

3. Proposed Method

In this paper, various chaotic maps are used to produce the chaotic sequence and to regulate the method of encryption. The chaos streams are generated by using various chaotic maps among the varied maps are investigated and their characteristics are analysed.

3.1. Zaslavsky Chaotic Map

This two-dimensional (2-D) map of the conflict was presented by George M. Zaslavsky (1978). It is an independent time-varying flexibility system that is very sensitive to its initial values. This high sensitivity makes this program very useful for many cryptographic programs as well as for other applications that require

hypocrisy - random. Zaslavsky's 2-D map can show real random numbers and show a noisy character. We set up this map as a random number generator that generates the keys to our proposed encryption algorithm. Random false numbers can be generated by the multiplication process (Rafik and Faiza, 2016).

The 2-D map is defined as coupled Eqs (1) and (2):

$$x_{n+1}=[x_n+v(1+\mu y_n)+\varepsilon v\mu cos(2\pi x_n)](mod1) \quad (1)$$

$$y_{n+1}=e^{-r}(y_n+\varepsilon cos(2\pi x_n)) \quad (2)$$

$$\mu=\frac{1-e^{-r}}{r} \quad (3)$$

where x_n, y_n are the chaotic samples of this map. x_0, and y_0 are the initial values. ε, τ, and ν are the controlling parameters to oversight the chaotic behavior proposed, and e is the exponentiation.

3.2. Bifurcation of Gauss/Mouse Map

The Gauss map (also known as the Gaussian map or mouse map) is a nonlinear iterated map of the reals into a true interval given by the Gaussian function in mathematics (Zhang et al., 2015).

$$x_{n+1}=\exp(-\alpha x_n^2)+\beta \quad (4)$$

where α and β are real-world variables.

The function, named after Johann Carl Friedrich Gauss, maps the bell-shaped Gaussian function in a manner similar to the logistic map.

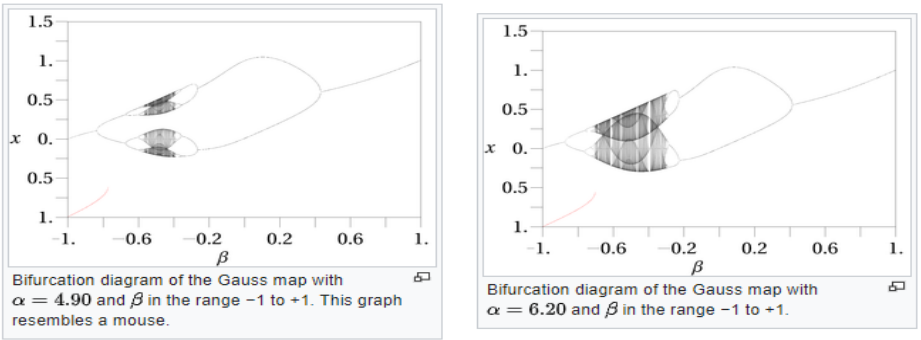


Fig.1: Bifurcation diagram.

3.3. The Skew Tent Map

The skew tent map (Ramasamy et al., 2019; Khade and Narnaware, 2012), a simple dynamic nonlinear equation with complex chaotic behaviour, is one of the most well-known chaotic maps, as expressed by the equation below.

$$T_{n+1}=\begin{cases} T_n/c\,, & 0< T_n \leq c \\ (1-T_n)/(1-c), & c < T_n < 1 \end{cases} \quad (5)$$

where Tn [0, 1] is the state, c [0, 0.5] [0.5, 1] is the action parameter, and n is the number of permutations that are used to iteratively construct state values.

3.4. Piecewise Linear Chaotic Maps (PWLCMs)

For Lyapunov exponents, sequential sequencing maps (PWLCMs) are simple non-specific programmes with a lot of potential. Jun et al. (2008) shows that they involve a range of systematic complex elements that will be used in cryptotic algorithms. PWLCM has a wide range of dynamic and character properties, including a consistent distribution, an automatic adjustment mechanism, periodicity, a broad Lyapunov exposition, and material. The orbit is a sequence of real numbers between 0 and 1 generated by converting PWLCM with the primary value and control parameters (Rhouma et al., 2009). The big positive display of Lyapunov indicates that the mechanism behaves strangely in the majority of cases (Li et al., 2005; Mahmoud, 2015). Lyapunov function is provided in Equation (6).

$$V(x)=\frac{d}{dt}V(x(t)=\frac{\partial V}{dx}.\frac{dx}{dt}=\nabla V.\ x=\nabla V.f(x) \quad (6)$$

where V is the Lyapunov-candidate-function.

PWLCMs are a quite simple chaotic system that only requires one split and a few additions. Skew tent map may be a PWLCM for a common type of tent map that resembles a tent map with slight differences (see Equation (7)). Equation describes a complex example of PWLCM (8). Equation (8) clearly shows that f (0, p) = 0, f2 (0.5, p) = 0, and f3 (1, p) = 0 for any P (0, 0.5). As a result, we can never use those numbers since they are the first xn parameters.

$$x_{n+1}=f(x_n,p)=\begin{cases} x_n/p\,, & x_n \in [0,p] \\ (1-x_n)/(1-p), & x_n \in [p,1] \end{cases} \quad (7)$$

$$x_{n+1}=f(x_n,p)=\begin{cases} x_n/p\,, & x_n \in [0,p] \\ (x_n-p)/(0.5-p), & x_n \in [p,0.5] \\ f(1-x_n,p), & x_n \in [0.5,1] \end{cases} \quad (8)$$

where x0 is the initial condition value, P is the control parameter, xn [0, 1], and P is the control parameter (0, 0.5).

3.5. Sine Chaotic Map

One of the most well-known 1D chaotic maps is the Sine map (Pareek et al., 2006; Zhang et al., 2020; Zhu et al., 2019). It's a simple phase space with complicated chaotic behaviour, similar to the Logistic map. The Sine map's mathematical model is frequently expressed as

$$x(n+1) = \mu / 4 \times \sin(\pi \times x(n)) \quad (9)$$

where μ is the system parameter in the range (0, 4], x(0) is the system's initial state value, and x(n), n = 1, 2,... is the system's output sequence of state values. Figure 1 display the Lyapunov Exponent and bifurcation diagram of the Sine map to observe its chaotic behaviours.

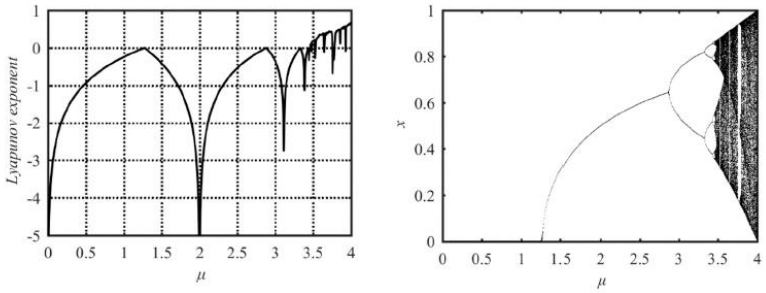


Fig. 2: Lyapunov Exponent and bifurcation diagram of the Sine map. (a) Lyapunov Exponent diagram; (b) bifurcation diagram.

Figure 2 shows block diagram of ROI based medical image encryption. Proposed method mainly consists of three process namely ROI part detection, Bitplane shuffling and diffusion operation.

3.6. ROI Detection

Original medical image of size MxN is segmented into non-overlapping 16x16 blocks. Histogram for every 16x16 blocks is calculated. As we that most of the medical images having a background which represent black pixel which is not important. By fixing the histogram threshold such way that if the 60% of every 16x16 block is black pixel then that block represented as Region of not interest (RONI) block and remaining blocks are ROI block.

3.7. Bitplane Shuffling

Light encryption with Bit-plane encryption is an unused encryption method based on aircraft crash. It can be easily applied to hardware. In this process the image to be nailed is divided into several planes using any binary decay method. Then the top four planes were replaced using four different chaotic systems with different initial conditions. The small controlled planes are then assembled together to get an

embedded image of Bitplane. The Bitplane shuffling method is based on Zaslavsky chaotic map, Bifurcation of Gauss/mouse map, and the skew tent map.

3.8. Diffusion Operation

To get more secure encrypted image diffusion operation is employed. In diffusion process based on chaotic system a random image is generated. Then Bitwise XOR operation applied between bitplane encrypted image and random image to get ROI part encrypted image. The Diffusion operation is carried out based on Piecewise linear chaotic maps (PWLCMs) and Sine Chaotic Map.

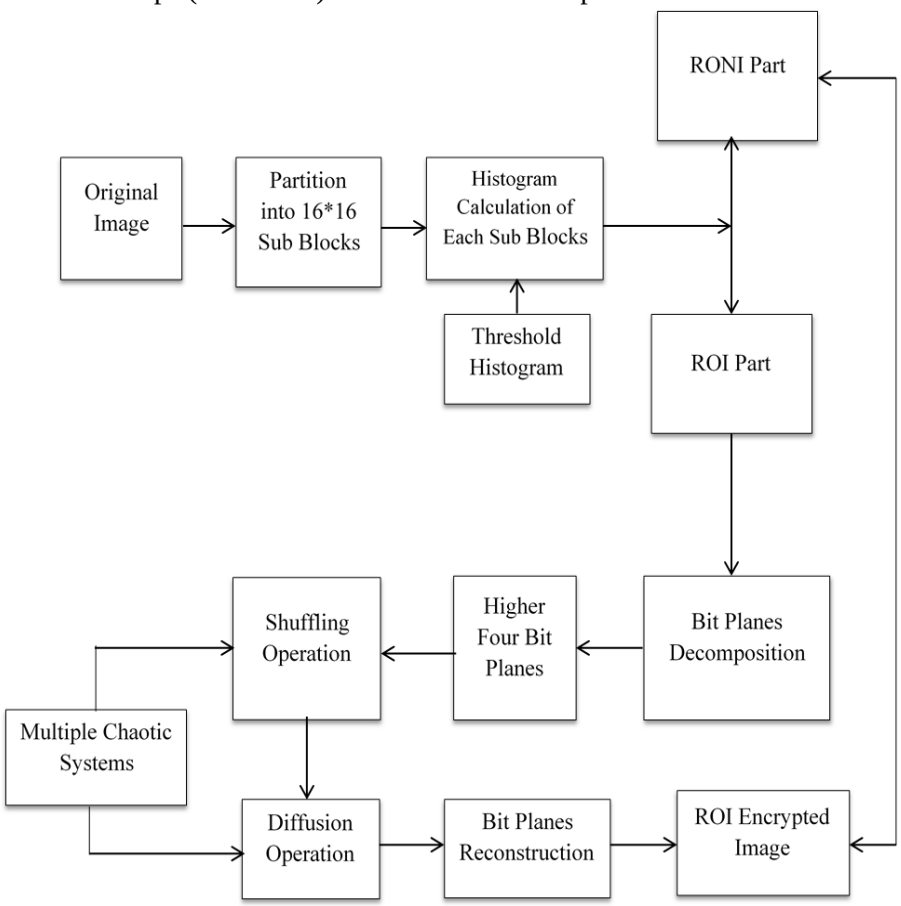


Fig. 3: Block Diagram for ROI based image encryption.

4. Results and Discussion

During this part, the proposed approach is introduced. In our database, we used grey images (Hand picture, Leg image, MRI image, Foot image, and Fetus image). They were n m in dimension, with n=m. Table 1 displays all of these images. Simulations

were run on a MATLAB 2016b platform with a 2.5 GHz core processor (TM) i7-353U and 4.0 GB memory. Different parameters should be evaluated to analysis the performance of proposed scheme. The subsequent parameters are involved as follows.

Entropy Analysis: The knowledge entropy, as defined by information theory, quantifies the degree of randomness in a collection of knowledge. If the entropy value of a cypher grey image is extremely close to 8, the 8-bit pixels are uniformly distributed. If si is the frequency of the pixel with the value I I =0.....255, and P(si) is the likelihood of si, then The formula for calculating entropy is from them (Arwa et al., 2020; Zhang et al., 2019):

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) log_2 \frac{1}{P(s_i)} = -\sum_{i=0}^{2^N-1} P(s_i) log_2 (P(s_i) \quad (10)$$

Where P(si) is the probability of the i^{th} grey level appearing in an image. For a random image, the ideal entropy value is 8. If it's lower, there's a greater chance of predictability.

Mean Square Error (MSE): In general, MSE is calculated by taking the mean of the squared difference between the plain image and the cypher image. Higher MSE values result in more encryption and noise in the plain image. MSE has the following mathematical equation (Jawad and Fawad, 2012).

$$MSE= \frac{1}{M*N} \sum_{i=1}^{N} \quad \sum_{j=1}^{M} [org(i,j) - enc\ (i,j)]^2 \quad (11)$$

Peak Signal to Noise Ratio (PSNR): The PSNR may also be used to assess the difference between the plain image and the resulting encrypted image. This metric shows how much the plain image has deteriorated as a result of the encryption process. Picture that is always stable, with more MSE and lower PSNR. PSNR is represented mathematically as (Wu et al., 2011).

$$PSNR= 20\ log_{10} \left[\frac{255}{MSE}\right] \quad (12)$$

UACI and NPCR: Sensitivity analysis can be described as a measurement of the amount of change in the cypher image caused by a small change in the encryption key or plain image. Number of pixels change rate (NPCR) and Unified average changing intensity (UACI) are two standard measures for evaluating the sensitivity of a main or plain image (Wang et al., 2004). Equation 13 is the formula for calculating UACI.

$$UACI = \frac{1}{M*N} \sum_{i,j} \frac{|org(i,j) - enc(i,j)|}{255} \text{ x } 100\ \% \quad (13)$$

Where m stands for the number of rows, n for the number of columns, and org(i, j) and end(i, j) stand for the first and cypher image, respectively. Equation 14 is commonly used to measure NPCR.

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{M * N} \text{ x } 100\ \% \tag{14}$$

where the cypher image is known as, D(i,j) is a bipolar array of equal size.

$$D(i,j) = \begin{cases} 1 \ if \ I(i,j) \neq E(i,j); \\ 0 \ if \ I(i,j) = E(i,j); \end{cases} \tag{15}$$

where the first and cypher images, respectively, are I(i,j) and E(i,j).

Universal Image Quality Index (UIQ): Universal index quality is employed for measuring similarity between original image and cypher image. Range of UIQ is [-1,1] where value 1 indicates more similarity and value -1 indicates less similarity. The UIQ is described in (Wang and Alan, 2006).

$$UQI(x,y) = \frac{\sigma_{xy}}{\sigma_x \, \sigma_y} * \frac{2\mu_x\mu_y}{\mu_x^2+\mu_y^2} * \frac{2\sigma_x \, \sigma_y}{\sigma_x^2+\sigma_y^2} \tag{16}$$

where μ_x, μ_y, σ_x, σ_y and σ_{xy} are the mean of x and y, the variance of x and y, and hence the covariance of x and y.

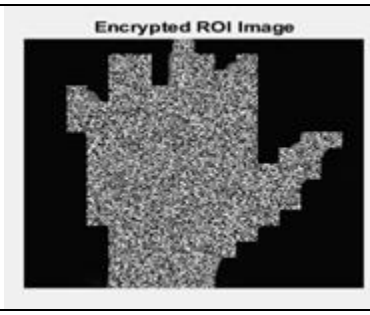
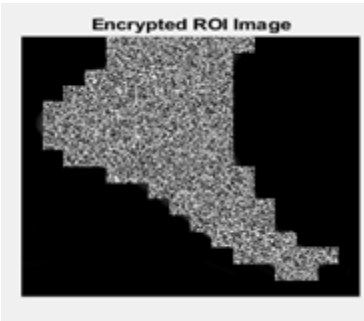
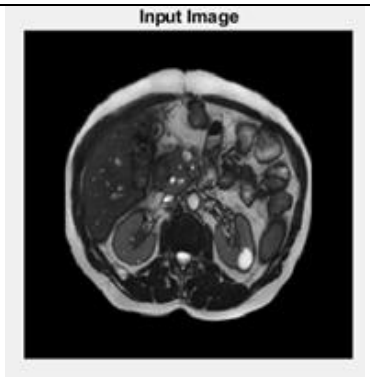
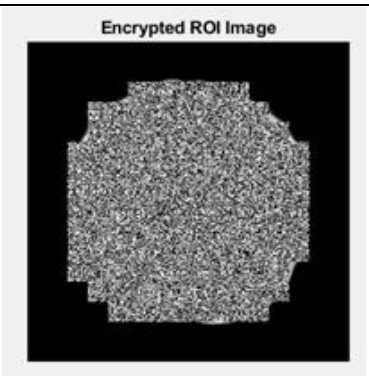
Structural Similarity Index Measure (SSIM): The SSIM is a more comprehensive version of the UIQ. The SSIM range is [-1,1], with 1 indicating greater similarity and -1 indicating less similarity. Sajjad et al. (2017) gives the concept of SSIM.

$$SSIM\ (x,y) = \frac{(2\mu_x\mu_y+C1)(2\sigma_{xy}+C2)}{(\mu_x^2+\mu_y^2+C1)(\sigma_x^2+\sigma_y^2+C2)} \tag{17}$$

$$SSIM = (1/M) \sum_{j=1}^{M} SSIM(x_j, y_j) \tag{18}$$

where C1, C2 are two constants that help to keep the division with a weak denominator stable.

Table 1: Input Image and output image for the Proposed Method

Name of the Input Image	Input Image	Encrypted Image
Input Hand Image		
Leg Image		
MRI Image		

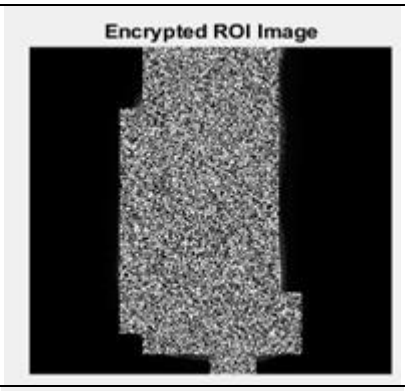
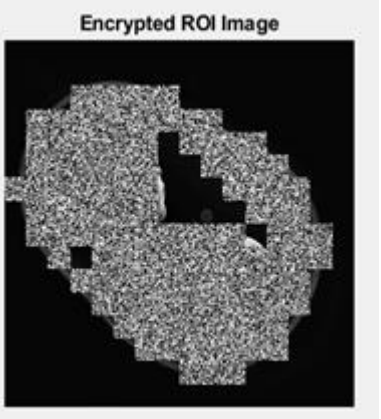
Input Foot Image		
Input Fetus Image		

Table 2: Performance parameters for proposed ROI encrypted system

Image Name	Entropy_In (Bit)	Entropy_Enc (Bit)	MSE	PSNR(db)	NPCR(%)	UACI(%)	UQI	SSIM
Leg	4.7639	4.9012	41.8391	31.9150	41.2445	12.4808	0.8668	0.5629
Fetus	4.9216	5.4233	26.1371	33.9582	45.8984	16.6886	0.7060	0.4454
MRI	4.5597	4.9973	33.7087	32.8534	49.0204	16.6988	0.7826	0.4418
Hand	4.4401	5.0011	66.6292	29.8942	47.0779	16.1082	0.8421	0.4508
Foot	3.7644	4.0888	39.1270	32.2060	36.9583	11.6299	0.9139	0.5437

Table 3: Efficiency of proposed ROI encrypted system

Image Name	Encryption Time (sec)	Time (%) Saving Compared to Full Image Encryption
Baby	0.271694	41.7969
Baby Womb	0.296692	46.4844
MRI	0.317435	49.6094
Hand	0.315953	47.6563
Foot	0.298069	37.5000

We can deduce from Table 2 that the entropy values of cypher images are higher than those of the explicit image. MSE values are elevated in conjunction with a special picture that specifies the encryption value. Because of the proposed NPCR

encryption method's chosen encryption, it's not quite different, indicating that calculation costs and time are reduced, and similarity indicator steps are reduced to 0, implying that lowering the worth increases the gap between the input image and thus the encrypted ROI image.

Table 3 presents the effectiveness of the proposed method in terms of performance speed and price. Comparing full image encryption this method saves about 50% of the calculation costs and achieves a faster time to use image encryption.

By analyzing the entropy values of the numerous images of the structure of table 1 formats, it's clear that entropy is high with the new encryption algorithm. Since the theoretical value is 8 and thus the analysis above shows that the entropy value of the cipher image is closer to the theoretical value and shows the upper inconsistency within the ultimate image.

The SSIM value between the original image and the encrypted image should be as small as possible, indicating the encryption algorithm's efficiency. The SSIM value between the ultimate medical encrypted image and the real medical image is determined in Table 2. It's clear that our method is producing small amounts of SSIM.

Table 3 shows that we were able to obtain a fast encryption time for different medical models. This is often done since, rather than using complete image encryption, we use a simplified method to encrypt weight. As a result, the time needed to form the plane encryption is reduced.

Table 4: MRI image parameters compared with current method

Parameters	**Proposed Method**	**Existing Method**
MSE	33.7087	86.2657
PSNR	32.8534	10.0881
NPCR	49.0204	0.5147
UACI	16.6988	12.4579
SSIM	0.4418	0.4620
Encryption Time	0.317435	72.50

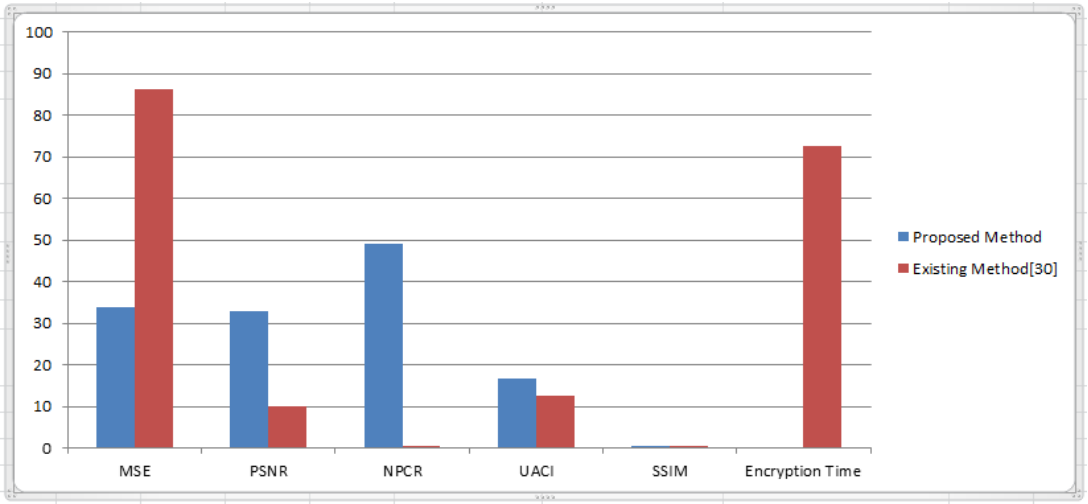


Fig. 4: Graphical analysis of parameters comparison with existing method.

The proposed approach decreases encryption time, guarantees the validity of the image submitted to the cloud, and provides protection through a two-level encryption scheme. We measure NPCR, MSE, PSNR, SSIM, encryption time, and other parameters to ensure the effectiveness of our chosen encryption scheme. The proposed encryption scheme was discovered to be an effective tool since it achieves better results than current systems.

5. Conclusion

In this paper, we've introduced how to access patient data from insecure networks to make sure data privacy and integrity on a resource-based platform. we've used aggressive encryption and biplanes encryption within the medical image that gives additional security to the image. to scale back further complexity of algorithm, higher four biplanes of ROI part is undergo shuffling and diffusion operation. Bit plane shuffling through with the assistance of multiple chaotic system followed by diffusion operation. The Simulation results, security analysis, and comparisons for the proposed image encryption are introduced and compared with existing algorithms. The results show that proposed method has a superb security performance. the longer term work are going to be in-depth study of the various chaotic orders as control flows in traditional encryption algorithm. it's hoped that this new idea can enhanced the normal cryptography capacity.

References

Afzal, I., Parah S.A. and Hurrah N.N. (2020). Secure patient data transmission on resource constrained platform. *Multimed Tools Appl*, https://doi.org/10.1007/s11042-020-09139-3.

Arwa, B., Maryam A., Rawan A. and Kaouther L. (2020). A novel approach of image encryption using pixel shuffling and 3D chaotic map. *Journal of Physics: Conference Series*, DOI: 10.1088/1742-6596/1447/1/012009.

Bang, J., Kang S. and Kim M. S. (2016). The study of factors to affect on users' self-disclosure in social networking services. *Journal of Korea Academic Industrial Cooperation Society*, 17(8): 69-76.

Darwish, S. M. (2019). A modified image selective encryption-compression technique based on 3D chaotic maps and arithmetic coding. *Multimedia Tools and Applications*, 78(14): 19229-19252.

Han, Q. (2019). Lightweight selective encryption for social data protection based on ebcot coding. *IEEE Transactions on Computational Social Systems*, 7(1): 205-214.

Heidari, S., Mosayeb N. and Koji N. (2019). Quantum selective encryption for medical images. *International Journal of Theoretical Physics*, 58(11): 3908-3926.

Jang, W. and Lee S. Y. (2016). Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment. *International Journal of Distributed Sensor Networks*, 16(3), DOI: 10.1177/1550147720914779.

Jawad, A. and Fawad A. (2012). Efficiency analysis and security evaluation of image encryption schemes. *Computing*, 23(25): 2012.

Jun, P., Jin S. Z., Liu Y. G., Yang Z. M., You M. Y. and Pei Y. J. (2008). A novel scheme for image encryption based on piecewise linear chaotic map. *2008 IEEE Conference on Cybernetics and Intelligent Systems*, Chengdu, 21-24 September 2008, 1012-1016.

Khan, J. S. and Jawad A. (2019). Chaos based efficient selective image encryption. *Multidimensional Systems and Signal Processing*, 30(2): 943-961.

Khade, P.N. and Narnaware M. (2012). 3D chaotic functions for image encryption. International Journal of Computing Science, 9, 323-328.

Khan, M. and Fawad M. (2019). A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimedia Tools and Applications*, 78(18): 26203-26222.

Khashan, O. A. and Muath A. (2020). Edge-based lightweight selective encryption scheme for digital medical images. *Multimedia Tools and Applications*, 79(35): 26369-26388.

Kumari, S. (2017). A research paper on cryptography encryption and compression techniques. *International Journal of Engineering in Computer Science*, 6(4): 20915-20919.

Li, S., Chen G. and Mou X. (2005). On the dynamical degradation of digital piecewise linear chaotic maps. *International Journal of Bifurcation and Chaos*, 15, 3119-3151.

Madhusudhan, K. N. and Sakthivel P. (2020). A secure medical image transmission algorithm based on binary bits and Arnold map. *Journal of Ambient Intelligence and Humanized Computing*, DOI: 10.1007/s12652-020-02028-5.

Mahmoud M. (2015). A Novel triangular chaotic map (TCM) with full intensive chaotic population based on logistic map. *Journal of Software Engineering and Applications*, 8, 635-659.

Pareek, N. K., Patidar V. and Sud, K. K. (2006). Image encryption using chaotic logistic map. *Image and Vision Computing*, 24, 926-934

Rafik, H. and Faiza T. (2016). A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. *Information Security Journal: A Global Perspective*, 25(4-6): 162-179.

Ramasamy, P., Ranganathan V., Kadry S., Damaševičius R. and Blažauskas T. (2019). An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—tent map. *Entropy*, 21(7): 656.

Rhouma, R., Arroyo D. and Belghith S. (2009). A new color image cryptosystem based on a piecewise linear chaotic map. *6th International Multi-Conference on Systems, Signals and Devices*, 23-26 March 2009, 1-6.

Sajjad, M., Muhammad K., Baik S. W., Rho S., Jan Z., Yeo S. S. and Mehmood I. (2017). Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. *Multimed Tools Appl*, 76(3): 3519-3536.

Sankaradass, V., Murali P. and Tholkapiyan M. (2018). Region of Interest (ROI) based image encryption with sine map and lorenz system. *International Conference on ISMAC in Computational Vision and Bio-Engineering*, Springer, Cham, 2018.

Shakir, H. R. (2019). An image encryption method based on selective AES coding of wavelet transform and chaotic pixel shuffling. *Multimedia Tools and Applications*, 78(18): 26073-26087.

Talhaoui, M. Z., Wang X. and Mohamed A. M. (2020). Fast image encryption algorithm with high security level using the Bülban chaotic map. *Journal of Real-Time Image Processing*, 1-14.

Wang, Z., Alan C. B., Hamid R. S. and Eero P. S. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, 13(4): 600-612.

Wang, Z. and Alan C. B. (2006). Modern image quality assessment. *Synthesis Lectures on Image, Video, and Multimedia Processing*, 2(1): 1-156.

Wu, Y., Joseph P. N. and Sos A. (2011). Cyber Journals: Multidisciplinary Journals in Science and Technology. *Journal of Selected Areas in Telecommunications*, 31-38.

Xian, Y. and Wang X. (2021). Fractal sorting matrix and its application on chaotic image encryption. *Information Sciences*, 547, 1154-1169.

Zhou, J., Li J. and Di X. (2020). A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position. *IEEE Access*, 8: 122210-122228.

Zhang, G. Ding W. and Li L. (2020). Image encryption algorithm based on tent delay-sine cascade with logistic map. *Symmetry*, 12, 355.

Zhang, X., Wang L., Cui G. and Niu Y. (2019). Entropy-based block scrambling image encryption using des structure and chaotic systems. *Hindawi International Journal of Optics*, Article ID: 3594534, 13.

Zhang, Y., Ji G., Dong Z., Wang S. and Preetha P. (2015). Comment on 'An Investigation into the Performance of Particle Swarm Optimization with Various Chaotic Maps'. *Hindawi Publishing Corporation Mathematical Problems in Engineering*, Article ID: 815370.

Zhu, S. Wang G. and Zhu C. (2019). A secure and fast image encryption scheme based on double chaotic s-boxes. *Entropy*, 21, 790.