PROVIDE A NEW ENCRYPTION ALGORITHM FOR MEDICAL IMAGES AND EVALUATE THE PROPOSED ALGORITHM

Mehdi Lotfi¹, Hossein Kheiri^{2*} , Azizeh Jabbari³

¹ MSc in Applied Mathematics, Faculty of Mathematical Sciences, University of Tabriz, Tabriz, Iran.

² Professor, Faculty of Mathematical Sciences, University of Tabriz, Tabriz, Iran.

³ Assistant Professor, Faculty of Engineering of Marand, University of Tabriz, Tabriz, Iran.

Article Info	ABSTRACT
<p>Article type: Research</p> <hr/> <p>Article History: Received: 2018-09-11 Revised: 2018-11-25 Accepted: 2018-12-03</p> <hr/> <p>* Corresponding author: Hossein Kheiri Faculty of Mathematical Sciences, University of Tabriz, Tabriz, Iran. Email: h-kheiri@tabrizu.ac.ir</p>	<p>Introduction: In this paper, an encryption algorithm for the security of medical images is presented, which has extraordinary security. Given that the confidentiality of patient data is one of the priorities of medical informatics, the algorithm can be used to store and send medical image.</p> <p>Material and Methods: In this paper, the solutions of chaotic differential equations are used to generate encryption keys. This method is more than other methods used in encoding medical images, resistant to statistics attacks, low encryption and decryption time and very high key space. In the proposed algorithm, unlike other methods that use random key generation, this method uses the production of solutions of the chaotic differential equations in a given time period for generating a key. All simulations and coding are done in MATLAB software.</p> <p>Results: Chaotic Differential Equations have two very important features that make it possible to encode medical images. One is the unpredictability of the system's behavior and the other is a severe sensitivity to the initial condition.</p> <p>Conclusion: These two features make the method resistant to possible attacks to decode the concept of synchronization chaotic systems. Using the results of the method, medical information can be made safer than existing ones.</p> <p>Keywords: Encoding, Medical Images, Medical Data Security, Chaos, Synchronization</p>

How to cite this paper

Lotfi M, Kheiri H, Jabbari A. Provide a New Encryption Algorithm for Medical Images and Evaluate the Proposed Algorithm. Front Health Inform. 2019; 8(1): e2. DOI: [10.30699/fhi.v8i1.155](https://doi.org/10.30699/fhi.v8i1.155)

INTRODUCTION

For ensuring the safety of medical data in a computer environment, one of the proposed ways is encrypting data. When the user sends his message, after clicking on the submit button, the message text is encrypted using a predefined encryption key and encrypted by the particular algorithm and placed in the communication channel. After being received by the user, it is decrypted by the key. To protect data, unauthorized access to encryption, concealment, and intrusion is used [1].

Among these three methods, encryption has become one of the important tools for providing a high level

of security. The main idea and key of the theory of chaos is that in any disorder, the order lies. In that sense, order should not be searched on a single scale. A phenomenon that appears on a local scale is completely random and unpredictable. That is likely to be quite robust and predictable on a larger scale. Circular rotation of encryption keys is a common mechanism for increasing the security of encryption methods. In this method, the turbulent rotation, in which the rotation of the pairs and repetitive mappings causes periodic circulation in chaos sets, is introduced as a new encryption method combining chaotic behavior with periodic key changes [2].

In previous years, the ideas and methods of the

theory of dynamical systems and chaos have been considered in various fields such as communication and encryption [3-8].

For example, this method is used to coordinate messaging systems in messaging systems. The main idea is that the sender generates a chaotic signal to cover the message sent as the raw text. At the receiving point, the secondary chaos system coincides with the received signaling signal, which is called cipher text. Then a simple subtraction operation displays the message. There are other ideas for sending encrypted messages based on chaos control basic theory and research. The unpredictable irregular behavior of many nonlinear systems is described as chaos. One of the main characteristics of chaotic systems is that it does not repeat its past behavior (even approximately). Another characteristic of dynamic systems that exhibits chaotic behavior is that such systems must necessarily include at least one nonlinear expression [9-11].

MATERIALS AND METHODS

In order to protect the medical and patient data about the confidentiality of information, we need methods in place to prevent unauthorized access. The methods that enable us to achieve this are encryption methods. Any medical data, including text data and image data obtained through medical devices and medical devices, can be converted to an image using a scanner. The image is converted into a matrix using the software, so that each bar of this matrix shows the color intensity of each pixel.

In the following, we can make the necessary changes, such as compression (using Fourier transforms and wavelets), and encryption on medical data using the created matrix. The medical data encoding topic can also be used to store information in the medical records and health records, as well as in the telemedicine section for sending medical pictures. The process is shown in Fig 1.

Fig 1: The Diagram of Changes on Medical Data

This article focuses on encoding medical images. Each encryption system that we use for encryption consists of two parts of the encryption (for the sender part) and decryption (for the receiver part). The algorithm used to encrypt chaotic differential equations solutions is used. To detect encrypted data, decryption should be done, using the concept of synchronization.

The system provided for synchronization

In this section, based on the Laplace transform theory, we construct a synchronization system with the PC method. Consider the fractional model similar to the Chen system described below [12]

$$\begin{cases} D^{\alpha_1} x = a(y - x), \\ D^{\alpha_2} y = dx - xz + cy, \\ D^{\alpha_3} z = xy - bz, \end{cases} \quad (1)$$

where α_i are fractional order derivatives of the state variables (x, y, z) and (a, b, c, d) are system parameters.

$D^\alpha f(t)$: Represents the Caputo fractional derivative of the order $(\alpha \in \mathbb{R})$ defined as follows:

$$D^\alpha f(t) = \frac{1}{\Gamma(n-\alpha)} \int_0^t \frac{f^{(n)}(\tau)}{(t-\tau)^{\alpha-n+1}} d\tau, \quad n-1 < \alpha < n,$$

which $\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt$ is the Gama Euler's function. Equation (1) offers chaotic behavior with

$$(\alpha_1 = 0.9, \alpha_2 = 0.95, \alpha_3 = 0.95, a = 35, b = 3, c = 28, d = -7).$$

Now master-slave PC system is build [3]. First consider the base system as the model (1) by assuming that the index of state variables are shown with m that is the first letter is the word (master).

$$\begin{cases} D^{\alpha_1} x_m = a(y_m - x_m), \\ D^{\alpha_2} y_m = dx_m - x_m z_m + cy_m, \\ D^{\alpha_3} z_m = x_m y_m - bz_m \end{cases} \quad (2)$$

and we consider the follower system with index s that is the first letter is the word (slave).

$$\begin{cases} D^{\alpha_1} x_s = a(y_s - x_s), \\ D^{\alpha_2} y_s = x_s y_s - bz_s. \end{cases} \quad (3)$$

By assuming $e_1 = x_s - x_m, e_3 = z_s - z_m$, the error system for equations (2) and (3) is obtained as follow:

$$\begin{cases} D^{\alpha_1} e_1 = -ae_1, \\ D^{\alpha_3} e_3 = -be_3 + y_m e_1. \end{cases} \quad (4)$$

Now, by applying Laplace transform to two sides of the equation (4) and assuming $E_i(s) = L(e_i)$, $i = 1, 3$ and using $L(D^{\alpha_i} e_i) = s^{\alpha_i} E_i(s) - s^{\alpha_i-1} e_i(0)$ we have:

$$\begin{cases} s^{\alpha_1} E_1(s) - s^{\alpha_1-1} e_1(0) = -aE_1(s), \\ s^{\alpha_3} E_3(s) - s^{\alpha_3-1} e_3(0) = -bE_3(s) + L[y_m e_1]. \end{cases} \quad (5)$$

From equation (5) we can conclude that

$$\begin{aligned} E_1(s) &= \frac{s^{\alpha_1-1} e_1(0)}{s^{\alpha_1} + a} \\ E_3(s) &= \frac{s^{\alpha_3-1} e_3(0)}{s^{\alpha_3} + b} + \frac{L[y_m e_1]}{s^{\alpha_3} + b}. \end{aligned} \quad (6)$$

By using the Laplace transform properties, we have:

$$\begin{aligned} \lim_{t \rightarrow \infty} e_1(t) &= \lim_{s \rightarrow 0} s E_1(s) = \lim_{s \rightarrow 0} s \frac{s^{\alpha_1-1} e_1(0)}{s^{\alpha_1} + a} = 0 \\ \lim_{t \rightarrow \infty} e_3(t) &= \lim_{s \rightarrow 0} s E_3(s) = \frac{1}{b} \lim_{s \rightarrow 0} s L[y_m e_1]. \end{aligned} \quad (7)$$

Since E is bounded, it follows that $\lim_{t \rightarrow \infty} e_3(t) = 0$.

So, synchronization is established between the base system and the follower system. We simulate the synchronization between the base system and the follower. The parameters used are the same parameters used in equation (1), and the initial conditions for the base and the follower systems are respectively (2.2, 2.4, 28) and (18, 8). The synchronization error's diagrams are shown in Fig 2 and 3, which show that the error in the limited time period tends to zero and synchronization works correctly.

Fig 2: Error's Diagram for $e_1 = (x_s - x_m)$

Fig 3: Error's Diagram for $e_3 = (z_s - z_m)$

Presentation of image encryption algorithm based on chaotic fractional system

Using the chaotic system introduced in the previous section, we introduce chaotic encryption for images. In the transmitter, the system generates a chaos signal. To perform the synchronization operation,

one of the variables must be selected as the agent variable; we use y_m for this purpose. Next, mix the generated chaotic sequence with the original image matrix data to get the encrypted image. The general schema of encryption and decryption process is shown in Fig 4. In the following, we describe the algorithm in a stepwise manner.

Encryption algorithm

Assume that the matrix form of the original image be the matrix $P_{M \times N}$ (which is M, N respectively the size of the row and column of the matrix). The pixels are arranged, respectively, from left to right and from top to bottom as numbers in the basis of ten.

$$S = \{S_{1,1}, \dots, S_{1,N}, \dots, S_{M,1}, \dots, S_{M,N}\}$$

- Simulate the base-follower system in the software and make sure the synchronization operation is done correctly.
- After achieving the synchronization, generate a vector with the size $M \times N$ from the solutions of the chaotic fractional order system; Then form the chaotic decimal sequence form such as:

$$\{z_m(i) \quad i=1,2,\dots\}$$

- In this step, decimal digits need to be preprocessed as follows:

$$z_m(i) = \text{round}(\text{mod}((\text{abs}(z_m(i)) - \text{floor}(\text{abs}(z_m(i)))) \times 10^5, 255)), \quad i=1,2,\dots$$

Encryption $D = \text{de2bi}(B) \oplus \text{de2bi}(C)$, where $\oplus$ indicates XOR and

$$B = \{B_1, \dots, B_N, \dots, B_M, \dots, B_N\}$$

And de2bi Converts the decimal value to its binary value, so the code set is in the form $D = \{D_1, D_2, \dots, D_N\}$

- Convert the encryption set from binary to decimal value to get encrypted two-dimensional image.

Decrypt

The decryption process is similar to encryption, with the difference that we are using a follower system at this stage.

Fig 4: Schematic encoding / decoding of the image with the proposed algorithm

RESULTS

Here we simulate the simulation results for the method presented in the MRI image. Fig 5a shows the original image whose equivalent histogram is shown in Fig 5b. In simulating chaos signals after synchronization, we generate 65536 samples. In Fig 5c and 5d, respectively, we encoded the image using the proposed algorithm and its equivalent histogram. The decoded image and the corresponding histogram are also depicted in Fig 5e and 5f. The results of Fig 5 show that the proposed algorithm works correctly. The encoded image is completely different from the original image, and the encrypted image is successfully retrieved, which is very close to the original image.

Fig 5a: Original Image

Fig 5b: Histogram of the Original Image

Fig 5c: Encrypted Image

Fig 5d: Encoded Image Histogram

Fig 5e: Decoded Image

Fig 5f: Histogram of Decoded Image

Evaluation of provided encryption algorithm

By applying an image encryption algorithm, the amount of pixels in the image varies from that of the

original image. A strong encryption algorithm should perform these changes at the maximum and most significant variation levels for the pixel values in the original image and image encoded. Also, to get an encrypted image, you must create random patterns that do not reveal any of the original image forms. The encoded image should have a very little dependency on the original image. One of the most important criteria for evaluating an encrypted image is visual inspection:

The more specific the image cached, the better the encryption algorithm gets. Criteria are used to measure the degree of encryption. Scattering is an important parameter that must be measured to judge the randomness of the encryption algorithm. If the algorithm has a good dispersion characteristic, the relationship between the encoded image and the original is very complicated and cannot be easily predicted. To measure the dispersion of any algorithm, one bit changes in the original image and obtains the difference between the encoded image obtained from the original image and the image obtained by changing a bit. In the following, we describe the criteria for evaluating the encryption algorithm [13].

Algorithm assessment criteria

In this section, two sets of encryption evaluations are discussed; the first one measures the ability of the encryption algorithm to replace the original image with an uncoordinated encoded image. In this category, five criteria were studied: histogram difference (D_H), correlation coefficients (r_{xy}), irregular difference (D_I) of histogram unevenness and difference from idealism. The second category measures the scattering property of the encryption algorithm. In this category, three criteria are studied: the effect of a sudden fall, the rate of change in the number of pixels (NPCR) and the capacity to change the mean of uniformity (UACI).

Histogram difference

Differences in histogram evaluate the encoding quality in terms of how to maximize the difference between the original images and encrypted it. The steps to calculate this benchmark are as follows:

- 1) Draw a histogram of the original image and it's encrypted
- 2) Estimate the net difference between two histograms
- 3) Estimates of the area under the difference curve divided by the whole image as follows

$$D_H = \frac{\frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} d_i}{M \times N},$$

which d_i is the net difference domain in the i category and M, N are the dimensions of the image we want to encrypt. The large amount of D_H will improve the quality of the encoded image. Although this criterion gives good results in returning the encoded image from the original image, but it cannot be used alone to measure encryption quality due to some limitations.

Entropy analysis of information

The entropy of information is calculated in the form of the following formula:

$$H(S) = \sum_{i=0}^{2^N-1} P(S_i) \log_2 \frac{1}{P(S_i)},$$

where $P(S_i)$ indicates the appearance possibility of the corresponding information S_i . The entropy of information for an image means the dispersion of gray values (0–255). The ideal value is equal $H(S)=8$ to entropy. The difference between the amounts of entropy for an encrypted image near this value is, of course, to indicate that the encryption algorithm is better. The calculations for the proposed algorithm show that the entropy for an encrypted image using the proposed algorithm is equal to $H(S)=7.9983$ that which is very close to the ideal value.

Correlation coefficients

One of the important criteria for evaluating the encryption quality of each image password system is the correlation coefficients between the pixels in the same profile in the encrypted image and the original image. This criterion can be calculated as follows:

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

which x, y is the original and encrypted images respectively. In numerical calculations, the following formulas can be used to calculate correlation coefficients

$$E(x) = \frac{1}{L} \sum_{i=1}^L x_i,$$

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

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

where L is number of pixels involved in the calculation. The closer value of r_{xy} to zero, indicate the better qualify of encryption algorithm.

In our article, 3,000 pairs of pixels were randomly selected close to each other horizontally from the original and encrypted images, in which case we conclude that $r_{xy} = 0.0076$.

Histogram uniformity

For a histogram, a graph of the bar indicates a grayish image for the event. The vertical axis represents the gray level. This axis starts from zero and goes up to higher gray levels. Each horizontal bar shows the number of events corresponding to the intensity of the gray color in the image. For each encoding algorithm, the histogram of the encrypted image must have the following two properties:

- 1) The whole histogram of the original image should be different from the encoded image.
- 2) The encoded image should have a uniform distribution, which means that the probability of occurrence of each color intensity is equal.

Space key

A secure encryption algorithm should have a key space greater than 2100 to be under the threat checking of all states [14]. In the proposed algorithm, the space of the key is obtained as follows: the initial conditions $(x_m, y_m, z_m, x_s, z_s)$ and the derivative order of the fraction $(\alpha_1, \alpha_2, \alpha_3)$, for initial conditions, range from 0 to 65535 with a length of step of 0.001 to 65535, and for derivatives of the range of 0.934464 to 0.999999 with a step length of 0.000001 to 65535, which for 8 private keys is a total of 2128, which is above 2100; therefore, encryption algorithm using chaotic differential equations, can provide a high level of security for key space to create.

DISCUSSION

In this section, the Comparison of the encryption algorithm provided with the AES encryption algorithm. In this paper, the comparison is done on two images; the average results for these states are presented in Tables 1 and 2. Selected images include MRI and chest (chest photo), as shown in Fig 6a and 6b, respectively.

Fig 6a: Chest Image

Fig 6b: MRI Image

Table 1: Comparison of the Encryption Algorithm Provided with the AES Algorithm for Mary Image

Algorithm	Entropy	Correlation coefficients	time for encryption and decryption	The number of key space
AES	7.9740	0.0227	175 Millisecond [15]	2128
Encryption using chaotic differential equations	7.9983	0.0076	61 Millisecond	2128

Table 2: Compare Encryption Algorithm Provided with AES Algorithm for Chest Image

Algorithm	Entropy	Correlation coefficients	time for encryption and decryption	The number of key space
AES	7.9800	0.0173	175 Millisecond [15]	2128
Encryption using chaotic differential equations	7.9959	0.0036	61 Millisecond	2128

CONCLUSION

In this paper, an algorithm was proposed for encoding medical images that is essential for the safety of patient data. The proposed method is known as chaotic encryption method. Given that each encryption algorithm consists of two parts of encryption and decryption, the proposed algorithm is not excluded from this rule. In the encryption section for generating keys, we generated responses to chaotic differential equations, and then we mixed the keys with the image pixel values, which resulted in the encrypted image. The decoding concept of synchronization was used later. There are various ways to synchronize chaotic systems, such as full synchronization, sliding mode, linear feedback, and other synchronization methods, for example, in which full synchronization was used. To measure

the efficiency and degree of assurance of the proposed method, it was necessary to compare with the encryption algorithm used in the images.

In this paper, the chaotic algorithm was compared with the AES encryption method. The ranking of two algorithms showed that the chaotic algorithm works better and has high security. Given that the method is not only theoretical but also practical, it can be used to maintain the privacy rights of patient information, this method can be used in hospital archiving systems.

AUTHOR'S CONTRIBUTION

All the authors approved the final version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest regarding the publication of this study.

FINANCIAL DISCLOSURE

No financial interests related to the material of this manuscript have been declared.

REFERENCES

1. Wang B, Wen G. On the synchronization of a class of chaotic systems based on backstepping method. *Physics Letters A*. 2007; 370(1): 35-9.
2. Lynch S. *Dynamical systems with applications using Maple*. Springer Science & Business Media; Switzerland. 2009.
3. Pecora LM, Carroll TL. Synchronization in chaotic circuits. *Phys Rev Lett*. 1990; 64(8): 821-4.
4. Grzybowski JMV, Rafikov M, Balthazar JM. Synchronization of the unified chaotic system and application in secure communication. *Communications in Nonlinear Science and Numerical Simulation*. 2009; (14)6: 2793-806.
5. Mata-Machuca JL, Martínez-Guerra R, Aguilar-López R, Aguilar-Ibañez C. A chaotic system in synchronization and secure communications. *Communications in Nonlinear Science and Numerical Simulation*. 2012; (17)4: 1706-13.
6. Yu F, Wang C. Secure communication based on a four-wing chaotic system subject to disturbance inputs. *Optik*. 2014; (125)20: 5920-25.
7. Wang B, Zhong SM, Dong XC. On the novel chaotic secure communication scheme design. *Communications in Nonlinear Science and Numerical Simulation*. 2016; 39: 108-17.
8. Fradkov AL, Evans RJ. Control of chaos: Methods and applications in engineering. *Annual Reviews in Control*. 2005; (29)1: 33-56.
9. Chen HH, Sheu GJ, Lin YL, Chen CS. Chaos synchronization between two different chaotic systems via nonlinear feedback control. *Nonlinear Analysis: Theory, Methods & Applications*. 2009; (70)12: 4393-401.
10. Dong-Feng W, Jin-Ying Z, Xiao-Yan W. Synchronization of uncertain fractional-order chaotic systems with disturbance based on a fractional terminal sliding mode controller. *Chinese Physics B*. 2013; (22)4: 1-7.
11. Haeri M, Emadzadeh AA. Synchronizing different chaotic systems using active sliding mode control. *Chaos, Solitons & Fractals*. 2007; (31)1: 119-29.
12. Chen DY, Liu YX, Ma XY, Zhang RF. Control of a class of fractional-order chaotic systems via sliding mode. *Nonlinear Dynamics*. 2012; 67(1): 893-901.
13. Abd El-Samie FE, Ahmed HEH, Elashry IF, Shahieen MH, Faragallah OS, El-Rabaie ESM et al. *Image encryption: A Communication perspective*. CRC Press, Boca Raton; 2013.
14. Wu J, Liao X, Yang B. Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation. *Signal Processing*. 2018; 142: 292-300.
15. Kumar L, Reddy AR, Jilani SAK. Implementation of 128-bit AES algorithm in MATLAB. *International Journal of Engineering Trends and Technology (IJETT)*. 2016; 33(3): 126-9.