A chaos-based medical image encryption method

Xuehong Wang, Chunling Tu
Departement of Computer Systems Engineering, Tshwane University of Technology, South Africa

Article Info

Article history:

Received Jan 7, 2020
Revised Mar 12, 2020
Accepted Apr 9, 2020

Keywords:

Chaos
Diffusion
Encryption
Unpredictable

ABSTRACT

The information in the e-health system involves the patient's extremely sensitive privacy. For instance, this information record social security numbers and detailed medical history. When the breach happens, there are illegal, or disclosure behaviors are taken to privacy that should be compromised security. In this paper, medical digital images are protected by the proposed chaos-based encryption method in the process of transmission and utilization. Then the authentication is granted to patients and telemedicine staffs by the decryption method proposed. The Qi 3-D four-wing chaotic system is employed in this method. The proposed method promises the keys with higher complexity and unpredictability than traditional cryptography methods by introducing the chaotic dynamics in the new cryptography. Digital medical images are used to validate the proposed method under the brute and differential attacks. The pixels of the image are scrambled completely based on the cat map and the sub-blocks of the image are diffused in the way that the original image is changed into a chaotic image robust to all kinds of attacks. The experiments show that the proposed method has higher performance and higher computation for decryption.

Corresponding Author:

Chunling Tu,
Department of Computer Systems Engineering,
Tshwane University of Technology, South Africa
Email: duc@tut.ac.za

1. INTRODUCTION

In recent years, with the rapid development of the internet, digital images security is attracting attention by more and more researchers[1-3]. One side, the Internet brings lots of benefits to humans. However, on the other side, the benefits are damaged by hacks committed via the same Internet, such as [4-6], virus[7-9], spy [10] and so on. Therefore, various digital image encryption technologies have been developed and applied in many fields, such as telemedicine, military, E-health, private communication, commercial system and so on. E-health is the use of information and communication technologies for health services. In the E-health, protecting patient privacy information contained in digital images is essential due to rapidly increasing data transmission based on the network [11, 12]. It is very important to protect the digital images of E-health with proper cryptography. Some traditional methods have been used to encrypt digital images. However, the medical images contain a lot of confidential information related to patients' privacy, when the digital medical image encryption properties are concerned, a large amount of data is in lack of enough security. The most traditional encryption methods for digital images just concern the correlation between adjacent pixels and high redundancy of neighbor pixels [13, 14]. The cryptography with chaotic dynamics has exceptional properties[15-22], because of the complexity and unpredictability of chaotic system. In this paper, a combination scheme of Arnold's cat map, Qi 3D four-wing chaos-system, and the Logistic system is employed which is sensitive to the keys from the analysis and evaluation. The proposed system is compared with ACM common technology, and the proposed method outperforms in the aspects of decryption complexity and sensitivity to the keys.

The rest of the paper is organized as follows. Section 2 is the relative work for the chaos-based image encryption scheme. Section 3 presents a description of the proposed method and encryption processes. Section 4 shows the experiment results and encryption key analysis. Section 5 concludes the paper.

2. THE PROPOSED METHOD AND RELATIVE WORK

2.1. Arnold's cat map

Arnold's cat map [23] (ACM) is a chaotic map from the torus into itself proposed in the 1960s. With Arnold's cat map, the pixels have been scrambled and reassembled. The original image cannot be recognized easily, because all the pixels have been repositioned. Arnold's cat map is defined [23-25] as below:

$$\Gamma \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} \tag{1}$$

It can be decomposed in the following steps.
Step 1: Shear in the x-direction

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ y \end{bmatrix} \tag{2}$$

Step 2: Shear in the y-direction:

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ x+y \end{bmatrix} \tag{3}$$

Step 3: Evaluate the modulo:

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} mod\ n \tag{4}$$

Where n is the size of an image ($n \times n$).

2.2. Qi 3D four-wing chaotic system

When the pixels have been scrambled by the cat map, to introduce the complexity and unpredictability of chaotic dynamics to the encryption, the Qi 3D four-wings chaotic system is used to encrypt the pixels. The state-space variable equations of the Qi 3-D [26] system is described in (5).

$$\begin{aligned} \dot{x} &= a(y-x)+eyz \\ \dot{y} &= cx+dy-xz \\ \dot{z} &= -bz+xy \end{aligned} \tag{5}$$

where $a, b, d, e \in R^+$ and $c \in R$ (R^+ denote the set of all positive real numbers, R denote the set of all real numbers) are constant parameters of the system, and $\mathrm{a}=14, \mathrm{b}=43, \mathrm{c}=-1, \mathrm{d}=16, \mathrm{e}=4$. It exhibits a chaotic phenomenon. This algorithm encrypted an image with a chaotic system. To make the encrypted image more complicated and safer, another chaotic system is introduced to select keys. The improved algorithm can be used for an RGB image. The R, G, B layers of an image is encrypted with $\mathrm{x, y, z}$ respectively: $C_R = A_R \oplus B_x$, $C_G = A_G \oplus B_y$, $C_B = B \oplus B_z$. Where C is the encrypted image, A is the plain image, $\oplus$ is the bitwise XOR operator, $B_x \subset \{x, y, z\}$, $B_y \subset \{x, y, z\}$, $B_z \subset \{x, y, z\}$ are the keystream from set $\{x, y, z\}$ according the function(Eq.5). The output of the Logistic system will be an important parameter for the function.

2.3. Logistic system

The logistic system is a second-order polynomial mapping that explains the complex chaotic behaviors of a very simple non-linear dynamical equation. It is proposed in 1976 [27], with the state space variable equations shown in(6).

$$p_{n+1} = \mu p_n(1-p_n) \tag{6}$$

Where p_n is a number which is greater than 0 and less than 1, μ in the interval [0,4], it also exhibits chaotic phenomenon.

2.4. The Proposed Method

This system will use to make the key stream as follow:
The output p of the logistic system determines the keystream of B_x, B_y, B_z shown in (7)

$$\begin{aligned} B_x &= \{\cdots,\ B_{i-1}^x, B_i^x,\ B_{i+1}^x,\ \cdots\} \\ B_y &= \{\cdots,\ B_{i-1}^y, B_i^y,\ B_{i+1}^y,\ \cdots\} \\ B_z &= \{\cdots,\ B_{i-1}^z, B_i^z,\ B_{i+1}^z,\ \cdots\} \end{aligned} \tag{7}$$

Where

$$B_i^x = \begin{cases} round[mod(x_i \times 1000, 255)], p > 0.7 \\ round[mod(y_i \times 1000, 255)], 0.3 \le p \le 0.7 \\ round[mod(z_i \times 1000, 255)], p < 0.3 \end{cases}$$

$$B_i^y = \begin{cases} round[mod(y_i \times 1000, 255)], p > 0.7 \\ round[mod(z_i \times 1000, 255)], 0.3 \le p \le 0.7 \\ round[mod(x_i \times 1000, 255)], p < 0.3 \end{cases}$$

$$B_i^z = \begin{cases} round[mod(z_i \times 1000, 255)], p > 0.7 \\ round[mod(x_i \times 1000, 255)], 0.3 \le p \le 0.7 \\ round[mod(y_i \times 1000, 255)], p < 0.3 \end{cases}$$

Here round(x) rounds the elements of x to the nearest integers. *mod* (x) means the remainder after division. p is the output of (6), x, y, z are the output of (5).

3. METHODOLOGY

In this paper, we propose a combination scheme of Arnold's cat map, Qi 3D four-wing chaos-system and the Logistic system as shown in Figure 1. The key is expected to be more complex and robust by introducing a higher level of confusion and diffusion.

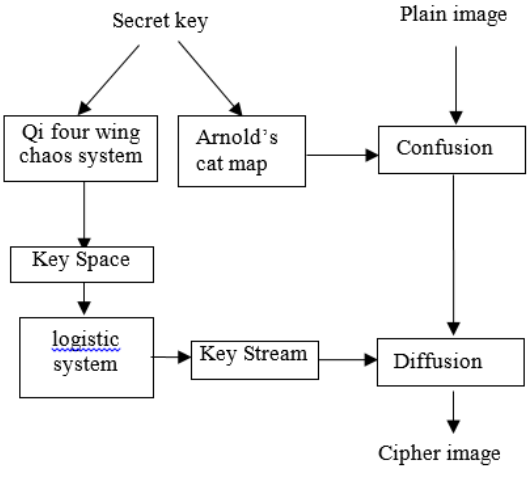


Figure1. The flow of chaos image encryption

3.1. Arnold's cat mapping process

According to Arnold cat map (ACM), let $X = \begin{bmatrix} x \\ y \end{bmatrix}$ be a $n \times n$ matrix of the image to be encrypted, then the mapping transformations in eq. (1) and (5) can be presented in a matrix form shown in(8).

$$\Gamma\begin{bmatrix}x\\y\end{bmatrix} \rightarrow \begin{bmatrix}1 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} mod\ n \tag{8}$$

where the *mod* is the modulo operation.

Consider a 3 × 3 image $\begin{bmatrix}G & H & I\\D & E & F\\A & B & C\end{bmatrix}$ the corresponding $(x,\ y)$-coordinates of the pixels are

$$\begin{bmatrix}(0,0) & (1,0) & (2,0)\\(0,1) & (1,1) & (2,1)\\(0,2) & (1,2) & (2,2)\end{bmatrix} mod\ 3 \tag{9}$$

Take the orbit of a pixel under the Arnold cat map (ACM) as the sequence in (9)

$$(1,1) \rightarrow (2,0) \rightarrow (2,2) \rightarrow (1,0) \rightarrow (1,1) \tag{10}$$

one gets the orbit of the entire image as eq. (11).

$$\begin{bmatrix}G & H & I\\D & E & F\\A & B & C\end{bmatrix} \rightarrow \begin{bmatrix}G & C & E\\F & H & A\\B & D & I\end{bmatrix} \rightarrow \begin{bmatrix}G & I & H\\A & C & B\\D & F & E\end{bmatrix} \rightarrow \begin{bmatrix}G & E & C\\B & I & D\\F & A & H\end{bmatrix} \rightarrow \begin{bmatrix}G & H & I\\D & E & F\\A & B & C\end{bmatrix} \tag{11}$$

Therefore, the 3×3 image has a period of $T = 4$ to be presented once again by Arnold's Cat Mapping. Dyson and Falk [28] analyzed the relationships and bounds on the period and the size of an image N:

$$T\begin{cases}= 3N & for\ N = 2(5^s); s \in N\\ = 2N & for\ N = 5^s\ or\ 6(5^s); s \in N\\ \le \frac{12N}{7} & for\ other\ N\end{cases} \tag{12}$$

Figure 2 is the original 256×256 image of an x-ray image. Figure 3 (a)-(d) show the outcome with different iterations under the ACM transformations.

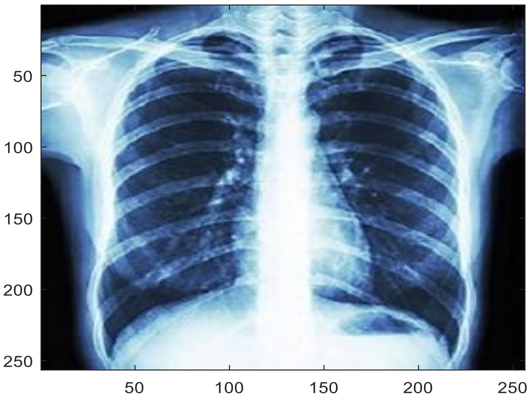
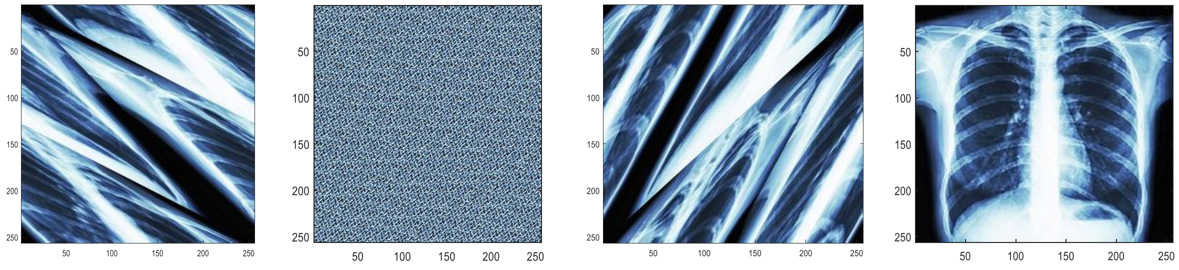


Figure 2. The original image

After different times of ACM mapping transformation, the original image transformation will be shown in Figures 3(a)-(d). It can be seen that the period of 192 for this transformation under ACM mapping. Therefore, if the iteration of encryption is p, the output of the ACM mapping will be the original image after the $192 - p$ iterations. So the decryption can be just encrypting the image several times. So based on the outcome in this step, a stronger encryption key is needed to protect the image.

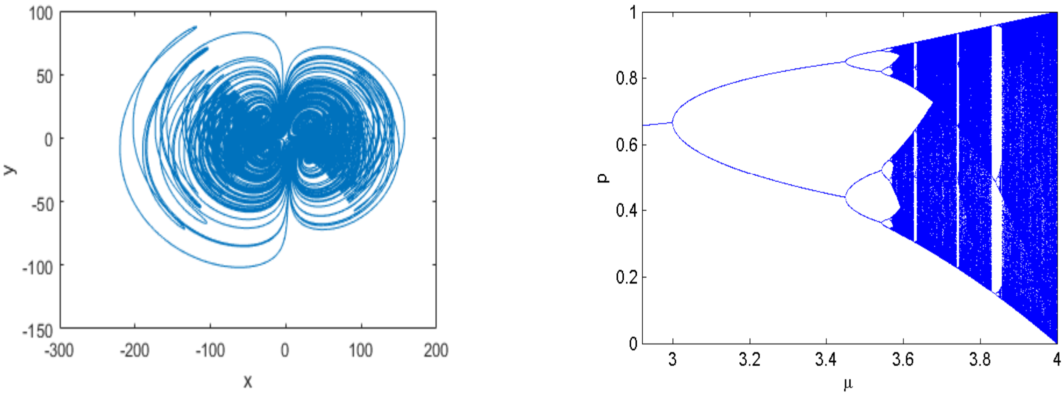


(a) (b) (c) (d)

Figure 3. (a)After the first iteration under ACM mapping. (b) The 10th iteration under ACM mapping. (c) 192th iteration under ACM mapping (d) 193th iteration under ACM mapping

3.2. Encryption by coupling 3D chaotic system and logistic system

First, the Qi 3D four-wing chaotic system and the Logistic system are recalled. When $\mathrm{a} = 14, \mathrm{b} = 43, \mathrm{c} = -1, \mathrm{d} = 16, \mathrm{e} = 4$, the Qi 3D, As shown in (5) will show a complicated chaotic performance, as shown in Figure 4 (a). The Logistic system will be a chaotic system when $\mu \in [3.4, 6]$, as shown in Figure 4 (b). For an $N \times N$ RGB image, there are three layers- red, blue, and green. Any layer can be a set $\mathrm{A}_{R,G,B} = \{\mathrm{A}_1^{\mathrm{R,G,B}}, \mathrm{A}_2^{\mathrm{R,G,B}}, \cdots, \mathrm{A}_{\mathrm{N\times N}}^{\mathrm{R,G,B}}\}$. The iterate Qi 3-D four-wing chaotic system times. $x_i\, y_i\, z_i$ can be got from each iteration. They can be reprocessed three key streams B_x, B_y, B_z for every layer of an RGB image.



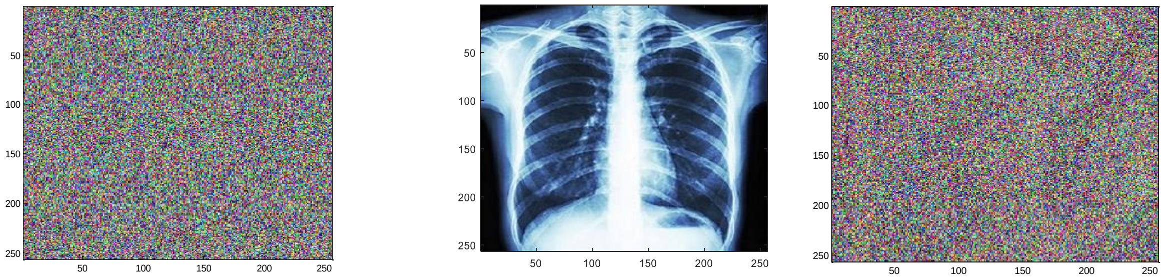
(a) 3D Qi System (b) Logistic system

Figure 4. Chaotic performance of Qi system and logistic system

According to eq. (7) the key streams areB_x, B_y, B_z, and their elementary are B_i^x, B_i^y, B_i^z, Then encrypt the keystream for every layer:

$$C_i^R = A_i^R \oplus B_i^x,\ \ C_i^G = A_i^G \oplus B_i^y,\ C_i^B = A_i^B \oplus B_i^z \tag{13}$$

The symbol $\oplus$ means exclusive or operation. Encrypt the red set $A_R = \{\mathrm{A}_1^{\mathrm{R}}, \mathrm{A}_2^{\mathrm{R}}, \cdots, \mathrm{A}_{\mathrm{N\times N}}^{\mathrm{R}}\}$, to cipher red set of $C_R = \{\mathrm{C}_1^{\mathrm{R}}, \mathrm{C}_2^{\mathrm{R}}, \cdots, \mathrm{C}_{\mathrm{N\times N}}^{\mathrm{R}}\}$. The one layer of cipher image can be obtained from this process. As the same process, the other two layers of cipher image can be obtained: $C_G = \{\mathrm{C}_1^{\mathrm{G}}, \mathrm{C}_2^{\mathrm{G}}, \cdots, \mathrm{C}_{\mathrm{N\times N}}^{\mathrm{G}}\}$, $C_B = \{\mathrm{C}_1^{\mathrm{B}}, \mathrm{C}_2^{\mathrm{B}}, \cdots, \mathrm{C}_{\mathrm{N\times N}}^{\mathrm{B}}\}$. Figure 2 is the input image, Figure 5 (a), (b), (c) shows the data before and after the encrypting and decrypting processes. The parameters are $a = 14, b = 43, c = -1, d = 16, e = 4$, $\mu = 3.8$. The initial condition of a 3D chaotic system, Logistic and the iteration T of Logistic are $x(0) = 0.002$; $y(0) = -1$; $z(0) = 0.3$; $p(0) = 0.1$; $T = 10000$. These parameters and initial values are important elements of the keyspace.

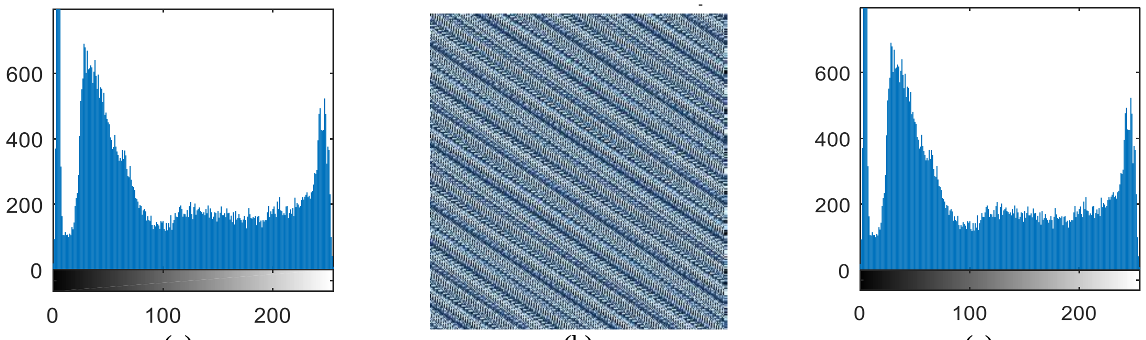


(a) (b) (c)

Figure 5. (a)The encrypted image (b) Decrypt image with correct keys (c) Decrypt image with wrong keys

3.3. Encryption process combine Arnold cat map, 3D Qi chaotic and logistic system

In this section, the plain image is firstly shuffled by ACM mapping. Then, the shuffled image is encrypted by Qi 3D four-wing chaotic system. Figure 6 (a) shows the input image’s histogram. After the first transformation under ACM mapping, the plain image change to Figure 6 (b), (c). The shuffled image is then encrypted by Qi 3D four-wing chaos system as shown in Figure 7. From Figure 6, one finds that the ACM mapping changes the position of the pixies, however, the values of the pixels are the same as the original image, as demonstrated in the histogram. The 3D chaotic system makes the pixel values (shown in the histogram in Figure 7 different from the original image, which makes it safer. For the decryption process, first, decrypt the cipher image with 3D Qi chaotic system, then sort the pixies with Arnold cat map, as shown in Figure 8. The decryption procedure uses the same parameter and the same process with encryption. Then conversely execute the encryption process, anti-shuffled scrambled image. The original image can be obtained. From the proposed method, the level of security is boosted. For instance, even a little bit of change of initial condition $x(0) = 0.002001$; $y(0) = -1$; $z(0) = 0.3$; $p(0) = 0.1$; $T = 10000$. for the 3D Qi chaotic system, the keys $x(0) = 0.002001$; $y(0) = -1$; $z(0) = 0.3$, are a little bit different to the correct keys $x(0) = 0.002$; $y(0) = -1$; $z(0) = 0.3$.



(a) (b) (c)

Figure 6. (a) input image’s histogram, (b) Shuffled image under Arnold cat map and (c) its histogram

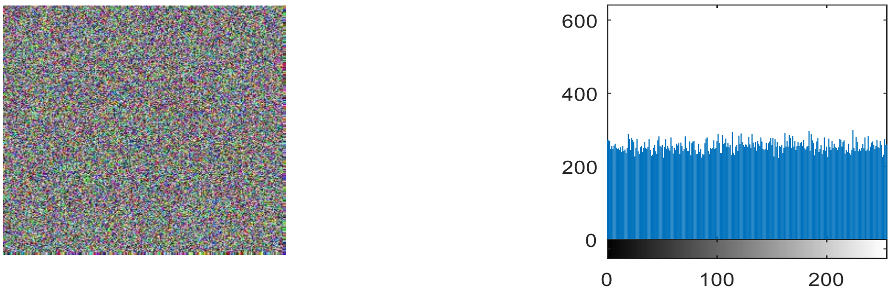


Figure 7. The final cipher image and its histogram

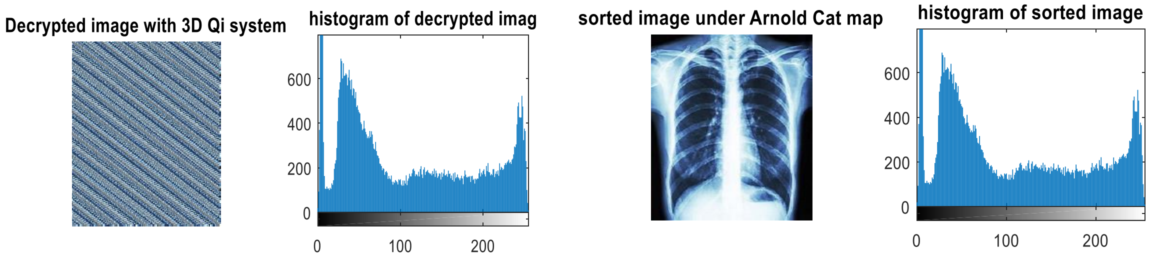
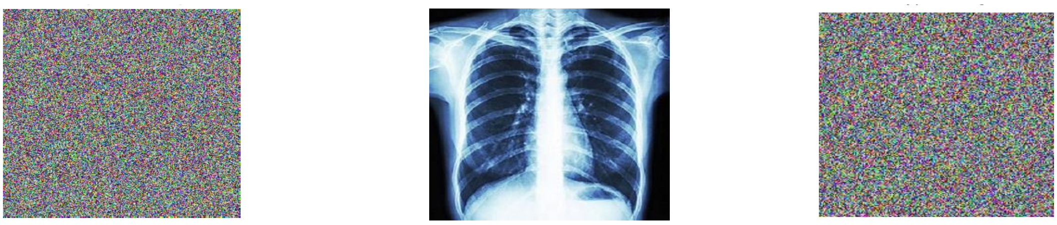


Figure 8. The decryption process image and its histogram

4. RESULTS AND ANALYSIS

4.1. The sensitivity of the keys

A good algorithm of image encryption should be sensitive to the keys. For the proposed method, assume the keys= $[0.001; -1; 0.3; 0.1; 100]$, as the correct keys, the encrypted image and decrypted images are shown in Figure 9 (a), (b). Given a little change to the keys, for example, new keys= [0.001001; -1; 0.3;0.1;100], the encrypted image and decrypted images are shown in Figure 9(a), (c).



(a) (b) (c)

Figure 9. (a) the encrypted image (b) decrypted image with keys = [0.001; -1; 0.3;0.1;100] (c) decrypted image with keys = [0.001001; -1; 0.3;0.1;100].

4.2. Evaluation of result

Attackers always try to find the difference between the plain image and the cipher image. The number of pixels changes rate (NPCR) is the rate of the mount of the pixels has been changed. Unified average changing intensity (UACI) is used to measure the different average intensities of the plain image and the ciphered image [29]. To demonstrate the influence of the proposed method on encryption, this common attack method is used. NPCR is considered to test the percentage of different pixels between the two images. $p_1(i.j)$and $p_2(i,j)$ are pixels of the two images with the same positions. NPCR can be defined as:

$$\text{NPCR} = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)}{W\times H} \times 100\% \tag{14}$$

where W and H are the image width and height respectively. $\text{D}(i,j)$ is defined as:

$$D(i,j) = \begin{cases} 0 & if\ p_1(i,j) = p_2(i,j) \\ 1 & if\ p_1(i,j) \neq p_2(i,j) \end{cases} \tag{15}$$

When $p_1(i,j) = p_2(i,j)$, $D(i,j) = 0$, which means the pixels of the same position are the same in the two images, otherwise, $D(i,j) = 1$. The UACI is used to measure the average intensity of the differences between the two images. It is defined as (16). When the NPCR and UACI values are more close to their expected values, the scheme has a higher security level. For the proposed scheme, for one-pixel change in the original image NPCR=0.996 and UACI=0.303, which means that the proposed scheme can survive in differential attack comparing with average NPCR=0.9962 and UACI=0.334 in reference [30].

$$\text{UACI} = \frac{1}{W\times H}\left[\sum_{i}^{W}\sum_{j}^{H}\frac{p_1(i,j)-p_2(i,j)}{L-1}\right] \times 100\% \tag{16}$$

5. CONCLUSION

This paper proposed a chaos-based encryption algorithm, which is sensitive to the keys from the analysis and evaluation. Besides, compared with ACM mapping, a very common technique to encrypt the image, the proposed method outperformance in the aspects of decryption complexity and sensitivity to the keys. The experimental evaluation validated that the novel encryption scheme boosted the security level of encrypted images, by greatly reducing the redundancy of neighbor pixels and correlation between adjacent pixels compared with the ACM method. Also, the telemedicine digital image encryption is considered to solve the increasing security problems in the E-health system.

REFERENCES

[1] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation,* vol. 18, no. 11, pp. 3075-3085, 2013.

[2] F. Adhanadi, L. Novamizanti, and G. Budiman, "DWT-SMM-based audio steganography with RSA encryption and compressive sampling," *TELKOMNIKA (Telecommunication Computing Electronics and Control),* vol. 18, no. 2, pp. 1095-1104, 2020.

[3] R. F. Abdel-Kader, S. H. El-Sherif, and R. Y. Rizk, "Efficient two-stage cryptography scheme for secure distributed data storage in cloud computing," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 3, pp. 3295-3306, 2020.

[4] C. C. Zou, L. Gao, W. Gong, and D. Towsley, "Monitoring and early warning for internet worms," in *Proceedings of the 10th ACM conference on Computer and communications security*, ACM, pp. 190-199, 2003.

[5] C. C. Zou, W. Gong, D. Towsley, and L. Gao, "The monitoring and early detection of internet worms," *IEEE/ACM Transactions on Networking (TON),* vol. 13, no. 5, pp. 961-974, 2005.

[6] J. Nazario, *Defense and detection strategies against Internet worms*. Artech House, 2004.

[7] M. W. Eichin and J. A. Rochlis, "With microscope and tweezers: An analysis of the internet virus of november 1988," in *Proceedings. 1989 IEEE Symposium on Security and Privacy*, IEEE, pp. 326-343, 1989.

[8] B. Samman, "Virus protection in an internet environment," ed: Google Patents, 2012.

[9] C. Gan, X. Yang, W. Liu, Q. Zhu, J. Jin, and L. He, "Propagation of computer virus both across the Internet and external computers: A complex-network approach," *Communications in Nonlinear Science and Numerical Simulation,* vol. 19, no. 8, pp. 2785-2792, 2014.

[10] J. Ball, J. Borger, and G. Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security," *The Guardian,* vol. 6, pp. 2-8, 2013.

[11] N. Calabretta, "Consumer-driven, patient-centered health care in the age of electronic information," *Journal of the Medical Library Association,* vol. 90, no. 1, pp. 32-37, 2002.

[12] M. E. Hameed, M. M. Ibrahim, N. A. Manap, and A. A. Mohammed, "An enhanced lossless compression with cryptography hybrid mechanism for ECG biomedical signal monitoring," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 3, pp. 3235-3243, 2020.

[13] Y. Mao and G. Chen, "Chaos-based image encryption," *Handbook of Geometric Computing,* pp. 231-265, 2005.

[14] P. Chen, X. Liu, J. Zhang, C. Yu, H. Pu, and Y. Yao, "Improvement of PRIME Protocol Based on Chaotic Cryptography," in *2019 22nd International Conference on Electrical Machines and Systems (ICEMS)*, IEEE, pp. 1-5, 2019.

[15] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits and Systems Magazine,* vol. 1, no. 3, pp. 6-21, 2001.

[16] M. Sharafi, F. Fotouhi-Ghazvini, M. Shirali, and M. Ghassemian, "A low power cryptography solution based on chaos theory in wireless sensor nodes," *IEEE Access,* vol. 7, pp. 8737-8753, 2019.

[17] A. Roy, "Chaos synchronization and cryptography for network security," 2018.

[18] P. Tobin, L. Tobin, M. Mc Keever, and J. Blackledge, "Chaos-based cryptography for cloud computing," in *2016 27th Irish Signals and Systems Conference (ISSC)*, IEEE, pp. 1-6., 2016.

[19] G. Jakimoski and L. Kocarev, "Chaos and cryptography: block encryption ciphers based on chaotic maps," *IEEE transactions on circuits and systems i: fundamental theory and applications,* vol. 48, no. 2, pp. 163-169, 2001.

[20] A. Di Falco, V. Mazzone, A. Cruz, and A. Fratalocchi, "Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varying silicon chips," *Nature Communications,* vol. 10, no. 1, pp. 1-10, 2019.

[21] E. de Almeida Ramos, J. C. Britto Filho, and R. Reis, "Cryptography by Synchronization of Hopfield Neural Networks that Simulate Chaotic Signals Generated by the Human Body," in *2019 17th IEEE International New Circuits and Systems Conference (NEWCAS)*, IEEE, pp. 1-4, 2019.

[22] R. I. Abdelfatah, "Secure image transmission using chaotic-enhanced elliptic curve cryptography," *IEEE Access,* vol. 8, pp. 3875-3890, 2019.

[23] P. N. Khade and M. Narnaware, "Practical Approaches for image encryption/scrambling using 3D Arnolds Cat Map," in *Advances in Communication, Network, and Computing*: Springer, pp. 398-404, 2012.

[24] E. Hariyanto and R. Rahim, "Arnold's cat map algorithm in digital image encryption," *Int. J. Sci. Res,* vol. 5, no. 10, pp. 1363-1365, 2016.

[25] N. A. Abbas, "Image encryption based on independent component analysis and arnold's cat map," *Egyptian informatics journal,* vol. 17, no. 1, pp. 139-146, 2016.

[26] G. Qi, G. Chen, M. A. van Wyk, B. J. van Wyk, and Y. Zhang, "A four-wing chaotic attractor generated from a new 3-D quadratic autonomous system," *Chaos, Solitons & Fractals,* vol. 38, no. 3, pp. 705-721, 2008.

[27] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature,* vol. 261, pp. 459-467, 1976.

[28] F. J. Dyson and H. Falk, "Period of a discrete cat mapping," *The American Mathematical Monthly,* vol. 99, no. 7, pp. 603-614, 1992.

[29] S. Ahadpour and Y. Sadra, "A chaos-based image encryption scheme using chaotic coupled map lattices," *arXiv preprint arXiv:1211.0090,* p. 3, 2012.

[30] Z. C.-X. S. Ke-Hui, "Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms [J]," *Acta Physica Sinica,* vol. 61, no. 12, pp. 120503-1- 120503-12, 2012.

BIOGRAPHIES OF AUTHORS

Xuehong Wang obtained Diploma of Communication Network from Luoyang normal university in 2010 and Bachelor of communication network from Tshwane university of technology in 2016. Now she is currently pursuing her master’s in computer system engineering in the faculty of Information and Communication Technology, Tshwane university of technology, Pretoria, South Africa. Her research interest is in computer vision, Information system and Image Encryption.

Dr Chunling Tu received the Bachelor degree of computer science from Tianjin University of Technology and Education, China in 2002; MTech and MSc degrees in Electrical Engineering from Tshwane University of Technology(South Africa) and ESIEE Paris University(France) in 2010; DTech and PhD degrees of Electrical Engineering from Tshwane university of Technology and University Paris East, France in 2015. She is currently a senior lecturer at Tshwane University of Technology. Her research interests include image processing, AI, industrial control, machine learning, deep learning and pattern recognition.