RESEARCH ARTICLE OPEN ACCESS

An Novel Image Encryption Algorithm Based on ROI

Weiming Meng
Henan University of Science and Technology, Luoyang, 471023, China

ABSTRACT

Aiming at the problem of insufficient efficiency and robustness of the current medical image encryption algorithm based on hyperchaos. To improve the security of image data in medical information sharing, an image encryption scheme based on ROI, SHA-3 algorithm and high-dimensional chaotic system is proposed. The algorithm first uses ROI to select the encrypted region, and at the same time uses the SHA-3 algorithm to calculate the hash value of the input image. The calculation result is used as the initial value of the hyperchaotic system. Use the improved hyperchaotic sequence to generate a chaotic key sequence of length L. Then the intensity value of the input image is converted into a serial binary digital stream and XORed with the chaotic key sequence to generate the final key sequence. Finally, the final key sequence is used to perform parallel encryption and ciphertext interleaving diffusion operations on the two sub-blocks divided by the input image. Simulation results show that the encryption system has a good performance in terms of robustness against statistical attacks. Fast encryption speed and high security.

***Keywords* -** Image Encryption, SHA-3, ROI, Hyperchaotic System, Ciphertext Staggered Diffusion

Date of Submission: 08-05-2020 Date of Acceptance: 22-05-2020

I. INTRODUCTION

With the continuous increase of image information, the content of image information is rich, which is one of the important means of information expression at present. Digital image information on the network is often communicated confidentially through receivers and senders as areas. For example, architectural drawings of financial institutions, drawings of military installations, pictures taken by military satellites, and new weapon design drawings[1]. In addition, there are some medical image information, such as the patient's visit pathology information (including the medical image of the patient's visit) in the remote medical information system. According to relevant laws and regulations, such private information must be encrypted before it can be transmitted over the network[2]. Image data transmission through the Internet is not only convenient and fast, but is less restricted by regions. It can also save costs and improve efficiency, saving time and effort. But because medical image data is special and private. That is, neither the sender nor the receiver allows the medical image information of the patient to be transmitted on the network to be viewed without authorization without permission[3]. Medical image information involves not only the patient's personal privacy but also the national security level, so the protection of data is particularly important.

Generally speaking, after the image is encrypted, the image information will be transformed into information similar to some channel random noise[4-6]. Internet eavesdroppers who do not know the correct key will not be able to identify it effectively (unless it is effectively deciphered). Therefore, the image data in transmission can be effectively protected.

In an image, the most significant amount of information is a meaningful visual image composed of a specific distribution or pixel gray value, color, etc. The area where people are most interested （ROI） [7]. By concealing some of the most important visual images, the content and meaning originally intended to be expressed in the entire image are completely changed. Process medical images containing patient sensitive information by using this method, make it processed into an ordinary image without useful information. This operation will reduce people's attention and paralyze the attacker, then achieve the purpose of protecting private information.

Chaos is an approximately random phenomenon[8]. It seems that there are no specific rules, but it is generated in a deterministic system. It meets the characteristics of image encryption by repeatedly and rapidly generating chaotic sequences. Chaos has this This excellent characteristic has led many scholars to shift their research focus from traditional encryption algorithms to chaos-based encryption algorithms[9-11]. Excellent chaotic encryption algorithms have been continuously proposed.

The architecture of chaotic encryption usually consists of three parts: one is to generate chaotic sequences, the other is to scramble pixel positions, and the third is to diffuse and replace pixel values [12]. The methods of evaluating the pros and cons of the chaotic encryption algorithm are mainly: the size of the key space, the sensitivity of the plaintext and the key, the correlation of neighboring pixels, statistical characteristics, the robustness of the algorithm, and the information entropy[13] . Literature [14] proposed a new hyperchaotic encryption algorithm. This algorithm improved the high correlation of images during the encryption process. After the image encryption, it has a good effect. Since all images are encrypted, the The amount of encryption calculation in non-essential areas decreases the encryption speed. Literature [15] proposed a typical image encryption algorithm based on hyper-chaotic system using image pixel position scrambling and pixel value encryption. However, the algorithm's plaintext has nothing to do with the key, making it unable to defend against known plaintext attacks. At the same time, the replacement of the algorithm and the scrambling operation are independent, making the image scrambling operation ineffective. Ref. \cite{16} proposed an image encryption algorithm, the correlation between the plaintext and the key was considered during the encryption process. However, the scrambling and encryption encryption structure of Ref. \cite{15} is basically used. Literature [17] proposed an algorithm to improve the encryption speed and efficiency by transforming chaotic sequences, but the correlation between the plaintext image and the key is low, and the entire image is encrypted, and the encryption efficiency is low.

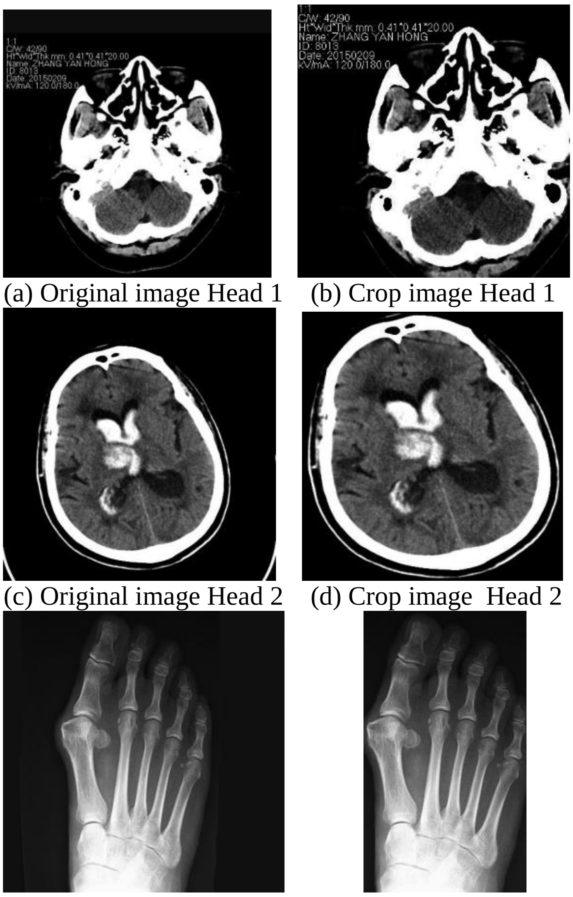
This paper proposes to segment the ROI from the medical image, combine the plaintext with the key, then perform chaotic encryption on it, and finally embed it in the original image to form an encrypted ordinary image. For transmission over the Internet. After analysis and verification, the algorithm has obvious advantages in encryption effect and speed, and has a good practical application effect in the field of medical image encryption.

The rest of the chapter is structured as follows: Chapter 2 explains the basic principles of the hyperchaos algorithm. The third chapter describes the specific principles and steps of the algorithm. The third chapter describes the specific principles and steps of the algorithm.

II. ALGORITHM PRINCIPLE

A. Region Of Interest(ROI)

In practical applications, the doctor can select the region of interest ROI in the medical image P according to actual needs. In order to improve confidentiality, the area of size $m\times n$ can be selected as the image to be encrypted according to the confidentiality needs of the patient. The process of acquiring the image D to be encrypted is shown in the Fig. 1.



(a) Original image Head 1 (b) Crop image Head 1

(c) Original image Head 2 (d) Crop image Head 2

(e) Original image Palm (f) Crop image Head Palm

Fig. 1. Original and cropped images of Head 1、Head 2 and Palm.

B. Hyperchaotic Initial Value Generation

The sponge structure-based SHA-3 algorithm [18] is the third-generation secure hash algorithm in the family. Hash algorithms are widely used in information interaction. However, due to the obvious shortcomings of the first-generation hash algorithm and the second-generation hash algorithm, they can no longer meet the requirements of secure and efficient encryption. In this context, algorithms emerged at the historic moment. Hash algorithms are also called hash algorithms. It has the advantages of low overhead, fast encryption speed, and no limit on message length. Hash algorithms are very sensitive to small changes in the image. A change in a pixel value will completely change the calculated hash value.

The input image will generate a set of 256-bit hash values for generating the initial values of the hyperchaotic system. The sequences are identified as, r_1, r_2, r_3,..., r_{32}. The number of horizontal pixels in the image is ψ, $(\psi=0,1,2,3,4,5,6)$, and the calculation formula for the initial value of hyperchaos is as follows:

$$x_1=(r_1\oplus r_2\oplus\cdots\oplus r_8)/10/2^{\psi}+x_0 \quad (1)$$

$$x_2=(r_9\oplus r_{10}\oplus\cdots\oplus r_{16})/10/2^{\psi} \quad (2)$$

$$x_3=(r_{17}\oplus r_{18}\oplus\cdots\oplus r_{24})/10/2^{\psi} \quad (3)$$

$$x_4=(r_{25}\oplus r_{26}\oplus\cdots\oplus r_{32})/10/2^{\psi} \quad (4)$$

Among them, x_1, x_2, x_3, x_4 is the initial value of the hyperchaotic system, expressed as an addition operation; set as 0.12.

C. Hyperchaotic Systems

In 2010, Wang et al. Constructed a new four-dimensional hyperchaotic system based on the chaotic system constructed by Cai. This system can produce complicated dynamic behavior with the change of parameters, and in its phase space, the range of motion traversal is large [19]. The mathematical model of a hyperchaotic system is as follows:

$$\begin{cases}\dot{x}_1=\alpha(x_2-x_1)\\ \dot{x}_2=bx_1+cx_2-x_1x_3+x_4\\ \dot{x}_3=x_2^2-dx_3\\ \dot{x}_4=-ex_1\end{cases} \quad (5)$$

The coefficient in the formula is a normal number. Among them, a, b, c and e are system control parameters x_1, x_2, x_4 and are the rate of change of system state variables over time. When the parameters $\alpha=27.5$, $b=3$, $c=35$, $d=5$, $e=3$ have two positive exponents [20], the system is in a hyperchaotic state.

D. Hyperchaotic Sequence

Due to the mismatch between the pixel value types of digital images and the numerical types of real numbers in the hyperchaotic sequences directly generated by the hyperchaotic system, and the pseudo-random characteristics and distribution characteristics of the hyperchaotic sequences are not ideal. Therefore, the generated hyperchaotic sequence is improved to make it more suitable for image data encryption [17]. The improved chaotic key sequence generation steps are as follows:

Step 1: The chaotic sequence expression directly generated by the hyperchaotic system is

$$\{x_j(i):i=1,2,\cdots,N_0+L/4;\ j=1,2,3,4\} \quad (6)$$

Where, Contains 4 sequences $\{j=1,2,3,4\}$ of lengths of $(N_0+L/4)$ real numbers. N_0 is the number of pre-iterations of the hyperchaotic system, and is the total number of pixels of the input image.

Step 2: In order to enhance the sensitivity of the generated sequence to the initial conditions of the system and to eliminate the harmful effects caused by transient processes in the sequence, remove the first N_0 values in the generated chaotic sequence. The newly generated chaotic sequence is 4 sequences $L/4$ with a length of $\{x_j(i):i=1,2,\cdots,L/4;\ j=1,2,3,4\}$; the sequence $\{x_j(i)\}$ is improved by using equation (7), and the new improved sequence $\{y_j(i)\}$ is:

$$y_j(i)=[2\times x_j(i)-(\max\_x_j+\min\_x_j)]/(\max\_x_j-\min\_x_j) \quad (7)$$

In the formula, $\min\_x_j$ and $\max\_x_j$ respectively represent the minimum and maximum values in the j-th sequence, $j=1,2,3,4$. Use the sequence $\{y_j(i)\}$ for a second improvement to generate four chaotic key subsequences $\{z_j(i)\}$:

$$z_j(i)=\mathrm{mod}((|y_j(i)|-\mathrm{floor}(|y_j(i)|))\times 10^m,256) \quad (8)$$

Where, $i=1,2,\cdots,L/4;\ j=1,2,3,4$.

In the formula, $|x|$ represents the absolute value of x; the value of is set to 14, and $\mathrm{floor}(x)$ represents the largest integer not greater than x;

Step 3: Combine the generated 4 subsequences to obtain a hyperchaotic sequence L of length K. The combined expression is as follows:

$$K=[z_1(1),z_2(1),z_3(1),z_4(1),\cdots,z_1(L/4),z_2(L/4),z_3(L/4),z_4(L/4)] \quad (9)$$

III. ALGORITHM PRINCIPLE

A. Encryption Steps

Suppose the image to be encrypted is D, the image size is $m\times n$, the total number of pixels is $L=m\times n$, and the matrix representation is:

$$P=\begin{bmatrix}P_1 & P_2 & \cdots & P_n\\ \vdots & \vdots & \vdots & \vdots\\ P_{(m-1)n+1} & \cdots & \cdots & P_L\end{bmatrix} \quad (10)$$

In the image encryption process, the expression form of the matrix is shown in Equation (10). Generates a ciphertext pixel sequence $\{C(i),i=1,2,\cdots,L\}$ in progressive scanning order. Let the pixel sequence $\{P(1),P(2),\cdots,P(L/2)\}$ be the first half of the image to be encrypted. Let the pixel sequence $\{P(L/2+1),P(L/2+2),\cdots,P(L)\}$ be the second half of the image to be encrypted.

The encryption algorithm process is as follows:

Step 1: Enter the image D to be encrypted.

Step 2: Perform a hash value calculation on the input image to obtain the initial values of the hyperchaotic system, x_1, x_2, x_3, x_4.

Step 3: Substituting the initial values x_1, x_2, x_3, x_4 into the hyperchaotic system formula to generate a chaotic real number sequence $\{x_j(i): i = 1, 2, \cdots, N_0 + L/4; j = 1, 2, 3, 4\}$.

Step 4: The generated chaotic real number sequence is transformed and optimized to obtain the intermediate chaotic key sequence K. Perform the first round of encryption operations, from step 5 to step 7.

Step 5: $i \leftarrow 1$; At the same time, the first pixel in the previous sub-block is calculated using equations (11) and (12) to generate the final encryption key, and the final encryption key is used for the encryption operation; The first pixel in the latter sub-block is calculated using equations (13) and (14) to generate the final encryption key, and the final encryption key is used for the encryption operation.

$$\mathrm{Key}(i) = \mathrm{mod}(C_0 + K(i), 256) \quad (11)$$

$$C(i) = \mathrm{bitxor}(P(i), \mathrm{Key}(i)) \quad (12)$$

$$\mathrm{Key}(L/2+i) = \mathrm{mod}(C(i) + K(L/2+i), 256) \quad (13)$$

$$C(L/2+i) = \mathrm{bitxor}(P(L/2+i), \mathrm{Key}(L/2+i)) \quad (14)$$

Where $\mathrm{mod}(x, y)$ is the remainder after dividing x by x to get the integer quotient; $\mathrm{bitxor}(x, y)$ represents the exclusive XOR operation of x and y. C_0 is a preset positive integer, $C_0 \in [1, 255]$. $P(i)$ and $C(i)$ represent the values of the i -th pixel of the plaintext image and the encrypted image, respectively.

Step 6: $i \leftarrow i+1$; At the same time, the -th pixel in the previous sub-block is calculated using equations (15) and (16) to generate the final encryption key, and the final encryption key is used for the encryption operation; The first pixel in the latter sub-block is calculated using equations (13) and (14) to generate the final encryption key, and the final encryption key is used for the encryption operation.

$$\mathrm{Key}(i) = \mathrm{mod}(C(L/2+i-1) + K(i), 256) \quad (15)$$

$$C(i) = \mathrm{bitxor}(P(i), \mathrm{Key}(i)) \quad (16)$$

Step 7: Repeat Step 6 until $i = L/2$ the first round of encryption operation is completed. The encryption operation of the second round is from step 8 to step 10.

Step 8: $i \leftarrow 1$; at the same time, the first pixel in the previous sub-block is calculated using equations (17) and (18) to generate the final encryption key, and the final encryption key is used for the encryption operation. The first pixel in the latter sub-block is calculated using equations (19) and (20) to generate the final encryption key, and the final encryption key is used to perform the encryption operation.

$$\mathrm{Key}(i) = \mathrm{mod}(C_0 + K(i), 256) \quad (17)$$

$$C(i) = \mathrm{bitxor}(C(i), \mathrm{Key}(i)) \quad (18)$$

$$\mathrm{Key}(L/2+i) = \mathrm{mod}(C(i) + K(L/2+i), 256) \quad (19)$$

$$C(L/2+i) = \mathrm{bitxor}(C(L/2+i), \mathrm{Key}(L/2+i)) \quad (20)$$

Step 9: $i \leftarrow i+1$; At the same time, the i _th pixel in the previous sub-block is calculated using equations (21) and (22) to generate the final encryption key, and the final encryption key is used for the encryption operation; The first pixel in the latter sub-block is calculated using equations (19) and (20) to generate the final encryption key, and the final encryption key is used for the encryption operation.

$$\mathrm{Key}(i) = \mathrm{mod}(C(L/2+i-1) + K(i), 256) \quad (21)$$

$$C(i) = \mathrm{bitxor}(C(i), \mathrm{Key}(i)) \quad (22)$$

Step 10: Repeat step 9 until $i = L/2$, the encryption operation of the second round is completed. Generate a ciphertext image C.

It can be known from the above encryption process that the initial value of the hyperchaotic system generated by SHA-3 is used to closely associate the plaintext image with the system. The final key $\mathrm{Key}(i)$ is used to encrypt the image pixels, so that the current chaotic key $\mathrm{K}(i)$ and the final key $\mathrm{Key}(i)$ are related to each other, and also the previous encrypted ciphertext pixel value in the other sub-block is related to the final key $\mathrm{Key}(i)$.

Decryption operation process is the reverse operation process of encryption operation.

IV. EXPERIMENTAL RESULTS

A. Experimental setup

This paper uses Matlab2016b as an experimental platform to simulate the algorithm. The initial value of the hyperchaotic system is calculated based on the hash value of the input image. The system parameters of the hyperchaotic system are: $a = 27.5$, $b = 3$, $c = 35$, $d = 5$, $e = 3$. The iteration time step is set to 0.001. The test images for simulation experiments are shown in Table 1. The image before and after encryption is shown in Fig. 2.

An excellent image encryption algorithm is extremely sensitive to small changes. When the key value changes slightly, the encrypted image changes dramatically. Corresponding to this, a slight change in the decryption key will cause a huge change in the decrypted image and the original image.

Table 1 Test images

Image	Resolution
Head1	410×410
Head2	378×430
Palm	544×1024

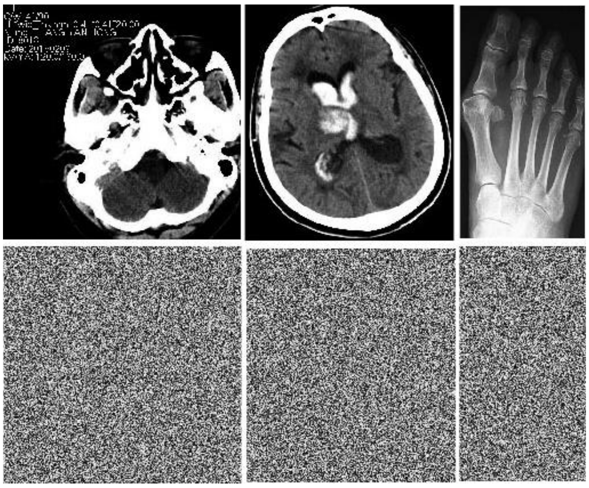


Fig. 2. Encrypted images of Head1, Head 2 and Palm.

B. Key Space Analysis

In this paper's encryption scheme, the SHA-3 algorithm is used to generate the initial values of the four state variables of the hyperchaotic system, which are represented by 15-digit decimal double-precision real numbers. The key space in the encryption scheme is: $10^{15}\times10^{15}\times10^{15}\times10^{15}=\times10^{60}\approx2^{199}$, which is roughly equivalent to a key length of $199\,\mathrm{bit}$. If the positive integer c and the number of pre-iterations are also used as the original key, the key space will be larger. Therefore, the algorithm has sufficient ability to attack the exhaustion. The experimental hardware conditions are a 2.7 GHz Intel (R) Core (TM) i7-7500U CPU, a notebook computer with 8GB of memory and a 500GB hard disk; the software environment is Windows 10 OS + Matlab2016b compiler.

C. Statistical Analysis

The original image and the encrypted image are statistically analyzed, and their statistical characteristics are analyzed. Use histograms to compare the histograms of the original and encrypted images. As shown in Fig. 3. It can be seen that the histogram of the original image shows irregular changes, while the histogram of the encrypted image shows very regular and smooth. The statistical information of the original image cannot be read from the encrypted image, which indicates that the hyperchaos algorithm has sufficient resistance to statistical attacks.

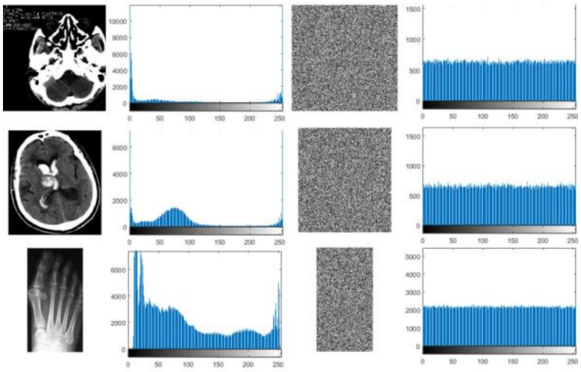


Fig. 3. The first column is the plaintext image of Head 1, Head 2 and Palm.

The second column is the histogram of the plaintext image. The third column is ciphertext image. The fourth column is the histogram of ciphertext image.

D. Anti-differential Analysis

The excellent image encryption algorithm can diffuse the information of the input image to the full image. When a pixel value in the plaintext image is changed, the entire password image will be completely changed. This can effectively resist differential attacks.

Use NPCR (pixel number change rate) and UACI (pixel average change intensity) to measure the password image is affected by small changes in the input image.

Set the plaintext image C_1 size to $m\times n$. A plaintext image C_2 is generated by changing any one pixel in the plaintext image C_1, and the pixel position of the change is set to (i, j), so the pixel values of the C_1 and C_2 images at (i, j) are $C_1(i, j)$ and $C_2(i, j)$ respectively.

$$NPCR=\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}D(i,j)\times100\% \qquad (23)$$

$$UACI=\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{|c_1(i,j)-c_2(i,j)|}{255}\times100\% \quad (24)$$

The calculated results are shown in Table 2 and Table 3. The maximum theoretical values of NPCR and UACI are:

$$NPCR_E=(1-2^{-r})\times100\%=99.6094\% \quad (25)$$

$$UACI_E=\frac{1}{2^{2n}}\frac{\sum_{i=1}^{2^n-1}i\left(i+1\right)}{2^{2r}-1}\times100\%=33.4635\%, \ (26)$$

The input image is an 8-bit grayscale image, and the n value in the formula is set to 8.

Enter three images, randomly change one bit for each image ten times, and calculate the NPCR and UACI after each change respectively to calculate the average performance.

Table 2 Average performance of NPCR (%)

Image	Ciphertext	C-DNA[21]	CHC[22]
Head1	99.2623	59.4884e-07	99.6371
Head2	99.2094	61.5233 e-07	99.6050
Palm	100	17.9515 e-07	99.6140

Table 3Average performance of UACI (%)

Image	Ciphertext	C-DNA[21]	CHC[22]
Head1	33.5236	23.3288e-09	33.5077
Head2	33.4953	24.1268e-09	33.3996
Palm	33.4666	7.03981e-09	33.4379

E. Key Sensitivity Analysis

Key sensitivity, an excellent image encryption algorithm is extremely sensitive to small changes. When the key value changes slightly, the encrypted image changes dramatically. Corresponding to this, a slight change in the decryption key will cause a huge change in the decrypted image and the original image.

When the initial value of the system changes 10^{-10}, as shown in Fig. 4, the decrypted image changes greatly, and the original image cannot be identified. This shows that the hyperchaos algorithm has sufficient ability to resist exhaustive attacks.

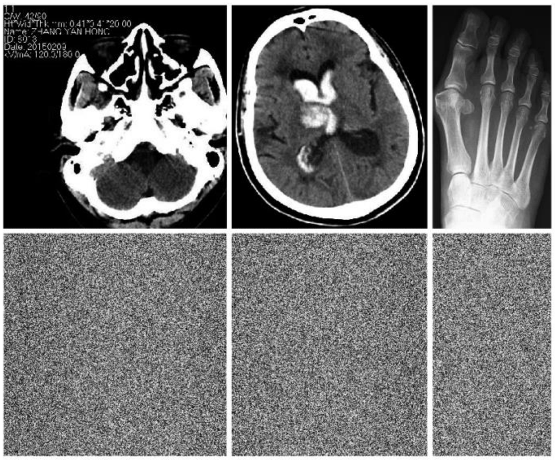


Fig. 4. Head1, Head2 and Palm decrypted images.

The first line is decrypted with the correct key, and the second line is decrypted with the wrong key.

F. Information Entropy Analysis

The definition of information entropy is the uncertainty of displaying image information. The larger the information entropy, the more uniform the gray value distribution of the image. Otherwise, it means that the distribution is uneven. An eight-bit grayscale image has 2^8 possibilities for its intensity value, so the closer the entropy value is to 8, the more ideal it is for a randomly distributed state. The formula for calculating information entropy is shown in (27):

$$H(s) = -\sum_{i=0}^{2^n-1} P(s_i)\log_2 |P(s_i)| \qquad (27)$$

Where s is the source of information and $P(s_i)$ is the probability of occurrence of information . The total number of information sources is . The encrypted image is calculated. The results are shown in Table 4. It can be seen that the entropy value of the encrypted image is close to 8, which shows that it can effectively resist the entropy attack.

Table 4 Ciphertext image performance

Image	Ciphertext	C-DNA[21]	CHC[22]
Head1	7.9988	7.9989	7.9986
Head2	7.9987	7.9988	7.9985
Palm	7.9997	7.9997	7.9995

G. Correlation Analysis

Attackers obtain image information by analyzing image information with high correlation between adjacent pixels. Therefore, correlation is an important indicator for testing the effect of image encryption. The closer the correlation coefficient is to 0 in the encrypted image, the better.

The formula for calculating the correlation coefficient is:

$$\gamma = \frac{\sum_{i=1}^{N}(x_i^a - \overline{x}^a)(y_i^b - \overline{y}^b)}{\sqrt{[\sum_{i=1}^{N}(x_i^a - \overline{x}^a)^2][\sum_{i=1}^{N}(y_i^b - \overline{y}^b)^2]}} \qquad (28)$$

The intensity values of the i pair of adjacent pixels a and b are represented by x_i^a and x_i^b. The average intensity value of adjacent pixel pairs is represented by $\overline{x}^a = \frac{1}{N}\sum_{i=1}^{N} x_i^a$. The average value of the next pixel of adjacent pixels is expressed by $\overline{y}^b = \frac{1}{N}\sum_{i=1}^{N} y_i^b$. Calculate the correlation coefficient γ_h in the horizontal direction, the correlation coefficient γ_v in the vertical direction, and the correlation coefficient γ_d in the diagonal direction. Image D is in size. The number of adjacent pixel pairs in the horizontal direction or the vertical direction is $N = m \times n - 1$ images.

By calculating the correlation coefficient between the original image and the encrypted image, the calculation results are shown in Table 5. The correlation coefficient of the original image is close to 1, and the calculated correlation coefficient of the encrypted image is close to 0, which indicates that the image encrypted using the hyperchaotic algorithm is irrelevant. As shown in Fig. 5.

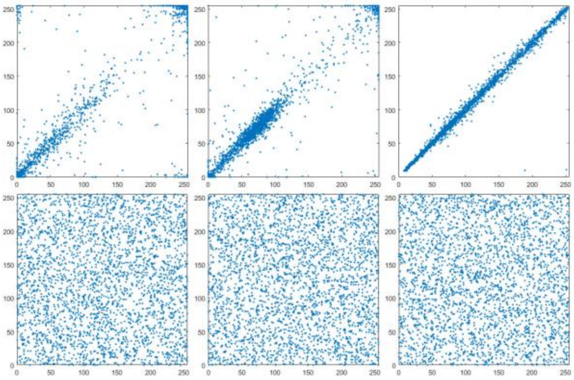


Fig. 5. The horizontal distribution of adjacent pixels between plaintext and ciphertext images.

Table 5 Correlation coefficient

Image	γ	Input	Ciphertext	C-DNA[21]	CHC[22]
Head1	γ_h	0.9251	-0.0025	-0.0026	0.00081
	γ_v	0.9478	-0.00095	-0.0023	-0.0017
	γ_d	0.9107	0.0028	0.00082	0.0031
Head2	γ_h	0.9657	-0.0014	0.0029	-0.00093
	γ_v	0.9728	-0.00004	0.00011	-0.00274
	γ_d	0.9477	-0.00045	0.00065	0.00220
Palm	γ_h	0.9966	-0.00086	0.00062	0.00202
	γ_v	0.9955	-0.00014	-0.0021	-0.00104
	γ_d	0.9953	0.00072	0.0013	0.00074

V. CONCLUSION

In this paper, by selecting the encryption region for the plaintext image and only encrypting the parts that need to be encrypted, the purpose of reducing the encryption operation expenses and improving the encryption efficiency is achieved. The SHA-3 algorithm is used to calculate the plaintext image to generate the initial value of the encryption system, and the initial value is applied to the hyperchaotic image encryption system, which improves the connection between the plaintext and the encryption system. The generated chaotic sequence is improved to have better random uniform distribution characteristics. At the same time, the improved chaotic sequence is combined with the ciphertext interleaving diffusion mechanism, and a parallel encryption method is used. Improved plaintext sensitivity and encryption efficiency. After experimental verification and analysis, the algorithm has the characteristics of high encryption efficiency and large key space. The correlation between the adjacent pixels of the encrypted image is close to zero, and the statistical distribution of the encrypted image is even, which shows that the algorithm is highly sensitive to the key and has strong resistance to differential attacks. The encryption algorithm proposed in this paper meets the needs of secure transmission of medical images.

REFERENCES

[1]. Sandyarani K, Kumar P N. Efficient substructure sharing methods for optimizing the composite S-Box, mixcolumn and inverse

mixcolumn in rijndael advanced encryption standard[J]. Journal of Computational & Theoretical Nanoscience, 2018, 15(3): 798-810.

[2]. Zhou Yu. Talking about the problems and countermeasures in the construction of regional medical information platform in the new era[J]. Science and Information, 2019,23(15): 145-145.

[3]. Wang Qian. Research on medical image encryption algorithm based on Bit-Plane decomposition and hyper chaos[J]. Computer Simulation, 2019, 36(1):209-212.

[4]. Shukla M K, Siva D, Mahajan A, et al. A novel scheme of image encryption based on synchronization of fractional order chaotic systems[C]// 2018 International Conference on Intelligent Circuits and Systems (ICICS). IEEE Computer Society, 2018.

[5]. Kaur M, Kumar V. An efficient image encryption method based on improved Lorenz chaotic system[J]. Electronics Letters, 2018, 54(9): 562-564..

[6]. Xing Y, Li M, Wang L. Chaotic-Map image encryption scheme based on AES key producing schedule[C]// 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). IEEE, 2018.

[7]. Lin Yangfei, Ye Shaozhen. A selective encryption on medical image data[J]. Electronic Technology Application, 2015,5(3):125-128.

[8]. Fridrich, Jiri. Symmetric ciphers based on Two-Dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos, 1998, 8(6): 1259-1284.

[9]. Yin Q, Wang C. A new chaotic image encryption scheme using breadth-first search and dynamic diffusion[J]. International Journal of Bifurcation and Chaos, 2018, 28(4): 18-47.

[10]. Wang X Y, Wang T. A novel algorithm for image encryption based on couple chaotic systems [J]. International Journal of Modern Physics B, 2012, 26(30): 125-175.

[11]. Sun S. Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules[J]. Optical Engineering, 2017, 56(11): 116-117.

[12]. Zhang Cuoling, Wei Liangfen. Research on digital image encryption algorithm base on Lorenz hyper chaos[J]. Journal of Hubei University, 2017, 38(6): 551-556.

[13]. Ye G, Pan C, Huang X, et al. A chaotic image encryption algorithm based on information entropy[J]. International Journal of Bifurcation & Chaos, 2018, 28(1): 10-18.

[14]. Gong L, Deng C, Pan S, et al. Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform[J]. Optics & Laser Technology, 2018, 103(43): 48-58.

[15]. Xiuli Chai, Zhihua Gan, Yang Lu, et al. A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system [J]. Chinese Physics B, 2016, 25(10): 103-105.

[16]. Li Junwei. Image encryption algorithm based on hyper-chaotic system[J]. Modern Electronic Technology, 2017, 40(15): 72-75.

[17]. Zhu Congxu, Hu Yuping, Sun Kehui. New image encryption algorithm based on hyperchaotic system and ciphertext interdiffusion[J]. Journal of Electronics and Information Technology, 2012, 34(7):1735-1743.

[18]. Bayat-Sarmadi S, Mozaffari-Kermani M, Reyhani-Masoleh A. Efficient and concurrent reliable realization of the secure cryptographic SHA-3 algorithm[J]. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, 2014, 33(7): 1105-1109.

[19]. Haoxiang Wang, Guoliang Cai, Sheng Miu, et al. Nonlinear feedback control of a novel hyperchaotic system and its circuit implementation[J]. Chinese Physics B, 2010, 19(3): 150-157.

[20]. Wang Yong, Fang Xiaoqiang, Wang Ying. Hyperchaotic system and AES combined with Image encryption algorithm[J]. Computer Engineering and Applications, 2019, 55(8): 170-176.

[21]. Zhu Congxu, SunKehui. Cryptographic analysis and improvement of a class of hyperchaotic image encryption algorithms[J]. Acta Physica Sinica, 2012, 61(12): 76-87.

[22]. Rehman A U, Liao X, Kulsoom A, et al. Selective encryption for gray images based on chaos and DNA complementary rules[J]. Multimedia Tools & Applications, 2015, 74(13): 4655-4677.