Multimed Tools Appl (2018) 77:22787–22808
https://doi.org/10.1007/s11042-017-5534-8

A new simple chaotic system and its application in medical image encryption

Jizhao Liu[1] · **Yide Ma**[1] · **Shouliang Li**[1] · **Jing Lian**[1] ·
Xinguo Zhang[1]

Received: 21 May 2017 / Revised: 1 December 2017 / Accepted: 12 December 2017 /
Published online: 5 February 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract Today, medical imaging suffers from serious issues such as malicious tampering and privacy leakage. Encryption is an effective way to protect these images from security threats. Among the available encryption algorithms, chaos-based methods have strong cryptographic properties, because chaotic systems are sensitive to initial conditions and parameters. However, traditional chaotic systems are easy to build, analyze, predict and can be re-scaled to any desired frequency. Thus, encryption schemes using traditional chaotic systems have low security levels. In this work, we propose a new simple chaotic system that utilizes a hyperbolic sine as its nonlinearity; this nonlinearity has rarely appeared in previous studies. Furthermore, the new chaotic system uses a decorrelation operation to enhance its performance. Statistical testing verifies that the chaotic sequence has good pseudorandom characteristics. In this study, we propose a scheme for medical image encryption based on this new chaotic system. The results of tests show that this encryption method can encrypt images effectively in a single round and that the proposed scheme provides sufficient security against known attacks.

Keywords Chaos · Hyperbolic sine · Image encryption · Medical image

1 Introduction

Data security plays an important role in the development of hospital information system (HIS) [8]. Medical image security has become a major concern in recent years; it usually involves the following aspects: confidentiality (only authorized individuals can access patient data), integrity (proof that the medical information has not been modified) and authentication (which is concerned with identification; the two communication participants should identify each other, allowing the information's origin to be proven) [1, 26, 30].

✉ Yide Ma
yidema@gmail.com

[1] School of Information Science and Engineering, Lanzhou University, No. 222, TianShui Road (south), Lanzhou, China

A variety of methods can be applied to provide information security for medical images, including steganography, watermarking and encryption. Steganography and watermarking can imperceptibly embed authentication information so that unauthorized users have no access to the hospital information system [15, 19, 22]. There is a large number of image encryption methods because different applications require different levels of security. Gutub has proposed a variety of methods in which the scarcity of resources plays an effective role; each method has achieved good results [3].

In recent years, among others, the following image encryption schemes have been proposed [24]. 1. Arnold's cat map [9] schemes have low computational complexity, but they do not alter the pixel values of the image; therefore, their security level is not high enough. 2. Discrete cosine transform (DCT) [12, 17] schemes have low computational complexity and high-level security. However, computer calculation precision is limited; thus, these schemes will lose accuracy when using the transform and inverse transform. Therefore, the decrypted image will not be exactly the same as the original image. 3. Chaos-based methods, have a high sensitivity to initial conditions and parameters; their irrelevance, random-like nature and unpredictability can help considerably in improving the security of transmitted communications [28].

There are several problems with traditional chaos-based image encryption algorithms. First, traditional chaotic systems are easy to analyze and predict. For example, the most commonly used chaotic systems for generating pseudorandom sequences are one-dimensional chaotic maps, which include the tent map, the logistic map, and the Chebyshev map. These simple chaotic maps can be attacked via a nonlinear prediction method based on phase–space reconstruction [4, 7]. Second, discrete chaotic systems can exhibit computationally based dynamic degradation [13], which renders these encryption schemes unreliable. Thus, it is more suitable to construct pseudorandom sequence generators using high-dimensional chaotic systems.

In this paper, a new simple chaotic system based on the hyperbolic sine is proposed. Furthermore, a decorrelation operation is used to enhance the performance of the chaotic sequence. Statistical testing verifies that the system has good pseudorandom characteristics, which indicates that this system is more suitable for image encryption than are traditional chaotic maps. With four initial conditions and six control parameters, the proposed system has a large key space that makes brute-force attacks infeasible. Key sensitivity and pseudorandom behavior make this scheme resistant to known-plaintext attacks, chosen ciphertext attacks, statistical attacks, and differential attacks.

The rest of the paper is organized as follows: In Section 2, a new simple chaotic system is introduced, followed by its analysis. Section 3 provides an analysis of a pseudorandom sequence after the decorrelation operation. The proposed image encryption scheme is shown in Section 4. Simulation results and performance analyses are reported in Section 5. Finally, conclusions are drawn in Section 6.

2 A new simple chaotic system

Finding a simple example of chaos is an interesting task. For cryptographic purposes, using a design based on a simple chaotic system can reduce the computational complexity and increase the speed of calculation. Over decades, there had been ongoing debate over which system was the "simplest" example of chaos until Piper and Sprott proposed three simplicity metrics: mathematical simplicity, circuit simplicity, and practical simplicity [21]. Based on these characteristics, a special class of dynamical systems—the so-called jerk systems—proposed to at minimum provide mathematical simplicity. Their functional forms are described by $\mathrm{X} = \mathrm{J}\left(X, \dot{X}, \ddot{X}\right)$, where the first derivative of the position is called velocity $\dot{X}$, the second derivative of the position is called acceleration $\ddot{X}$, and the third and higher order derivatives of the position is called jerk X In 2011, Sprott and Munmuangsaen proposed a jerk system with an exponential nonlinearity [16, 23]; this system provides a good foundation for exploring the hyperbolic sine chaotic system.

2.1 Equations and phase space plot

The simplest dissipative chaotic flow with a hyperbolic sine nonlinearity is [14]

$$\dddot{x} + 0.75\ddot{x} + x + 1.2 \times 10^{-6}\sinh(\dot{x}/0.026) = 0. \tag{1}$$

It can be rewritten as three first-order ordinary differential equations

$$\begin{cases} \dot{x} = y \\ \dot{y} = z \\ \dot{z} = -0.75z - 1.2 \times 10^{-6}\sinh(y/0.026) - x. \end{cases} \tag{2}$$

We upgraded this system to a simple fourth-order chaotic system and removed some of the coefficients, such as 1.2×10^{-6} and 1/0.026. By searching its control parameter space, we found an example of a simple chaotic system with a hyperbolic sine nonlinearity, which is described by

$$\begin{cases} \dot{\mathrm{x}} = 6y - x \\ \dot{y} = z \\ \dot{z} = u \\ \dot{u} = -u - \sinh(z) - 6x. \end{cases} \tag{3}$$

Figure 1 shows some phase-space plots with distinct initial conditions. When the initial conditions are set to $(x_0, y_0, z_0, u_0) = (-0.7, -0.9, -1, -1.3)$ and $(x_0, y_0, z_0, u_0) = (0.7, 0.9, 1, 1.3)$, the system shows period-1 behavior. The attractors are antisymmetric about the origin. Moreover, the system could also show chaotic behavior under the initial conditions $(x_0, y_0, z_0, u_0) = (-7, -9, -10, -13)$ and $(x_0, y_0, z_0, u_0) = (7, 9, 10, 13)$, which are also antisymmetric about the origin. Therefore, the system has four coexisting attractors [10, 11, 20, 25].

2.2 Analysis

To find the equilibrium point, we set every time-derivative to zero. Therefore, the equilibrium point of this system is $(x, y, z, u) = (0, 0, 0, 0)$, for which the corresponding Jacobian matrix is

$$\mathrm{J}(s) = \begin{pmatrix} -1 & 6 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -6 & 0 & 0 & -1 \end{pmatrix}. \tag{4}$$

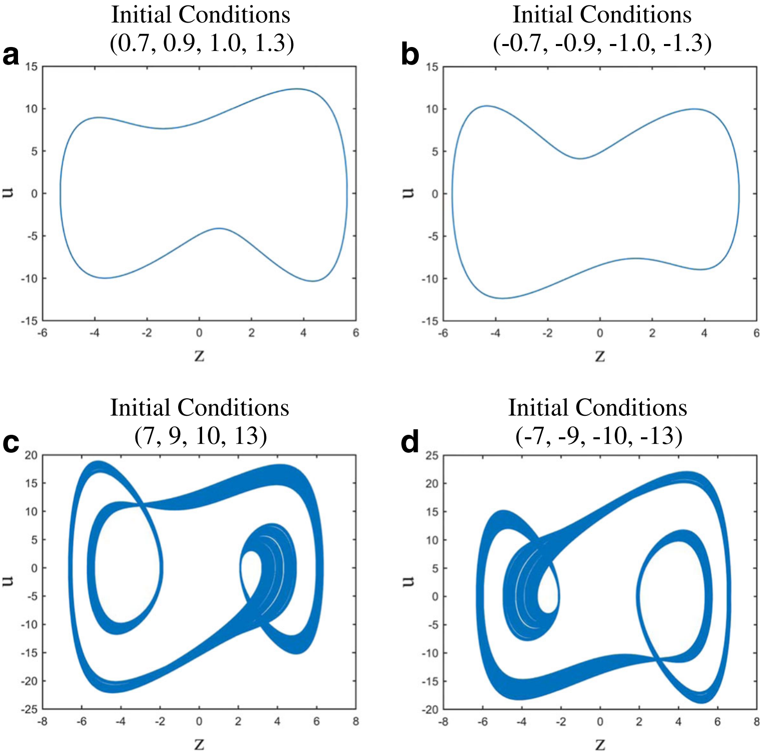


Fig. 1 Numerically calculated phase space plot of the system under different initial conditions

The resulting eigenvalues are $\lambda_1 = -2.2685 + 1.6963i$, $\lambda_2 = -2.2685 - 1.6963i$, $\lambda_3 = 1.2685 – 1.6963i$, and $\lambda_4 = 1.2685 + 1.6963i$. Because λ_1 and λ_2 are a pair of complex conjugate eigenvalues with a negative real part, and λ_3 and λ_4 are a pair of complex conjugate eigenvalues with positive real parts, the origin is a 2-D stable manifold and a 2-D unstable manifold, which suggests that the system is chaotic.

Lyapunov exponents characterize the rate of separation of infinitesimally close trajectories in state space as time tends to infinity. A positive large Lyapunov exponent indicates chaos. In this system, the Lyapunov exponents are (0.1268, 0, −0.9999, −1.1269) under the initial conditions $(x, y, z, u) = (7, 9, 10, 13)$, thereby suggesting that the system is chaotic.

3 The generation of a pseudorandom sequence and its analysis

By analyzing the sequences generated by Eq. (3), the authors realized that the randomness of the sequence is not ideal. Figure 2 shows the probability distribution of the variables x, y, z and u under the initial conditions $(x_0, y_0, z_0, u_0) = (7, 9, 10, 13)$. This illustrates that the sequence generated directly by Eq. (3) is not a uniform distribution.

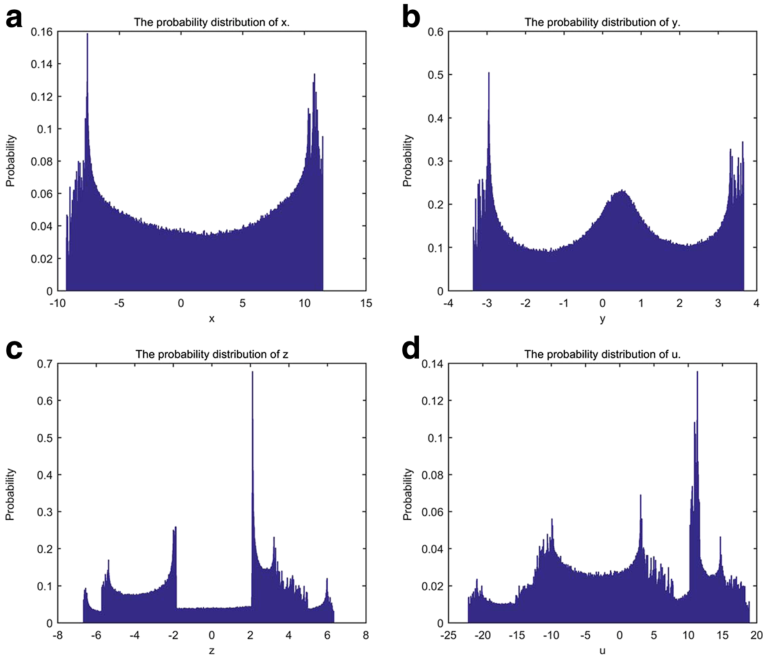


Fig. 2 The probability distributions of x, y, z and u

To generate sequences of uniformly distributed random variables and enhance the random statistical properties, we used the decorrelation operation, which is defined by the following equations:

$$S_{out} = S_{in} * 10^4 - floor\left(S_{in}{}^{*}10^4\right), \tag{5}$$

where S_{in} is the input sequence (which could be the variables (x, y, z or u) generated by Eq. (3)) and S_{out} is the output sequence. Figure 3 shows the waveform and probability distribution between S_{in} and S_{out}. In this case, we chose the variable u as the input sequence.

To further evaluate the performance of the chaotic sequence and the de-correlation operation, we used a test run of the SP 800–22 suite to test the random statistical characteristics of the sequence [4, 7]. The results are shown in Table 1.

After the de-correlation operation, the sequence exhibits improved randomness and ensures that the image encryption scheme will have improved resistance against known attacks. The results are shown in Table 1 and Fig. 3.

Table 1 Statistical performance

	Variable x	Variable y	Variable z	Variable u
Chaotic sequence by Eq. (3)	Failed	Failed	Failed	Failed
Pseudorandom sequence after de-correlation	Success	Success	Success	Success

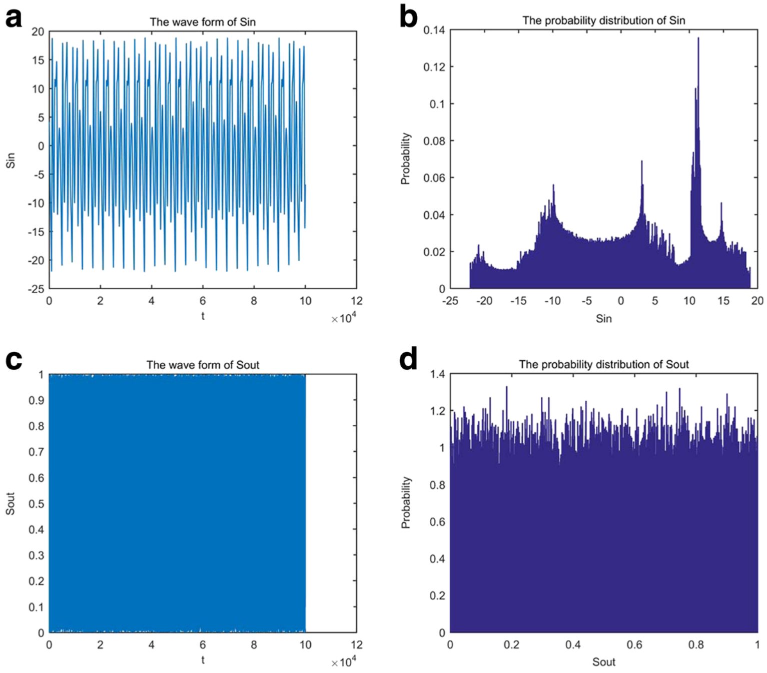


Fig. 3 The waveform and distribution of S_{in} and S_{out}

4 Image encryption scheme

In this section, an image encryption scheme will be proposed using the pseudorandom sequence from Section 3.

A flowchart of the encryption scheme is shown in Fig. 4.

The detailed encryption process includes the following steps.

Input: Plain image; Initial conditions for chaotic system; Control parameter for chaotic system

Output: Ciphered image

Step 1: Calculate the average pixel value of the plain image and generate the pseudorandom sequence.

Step 2: Transform the pseudorandom sequence and change pixel value of the image via XOR

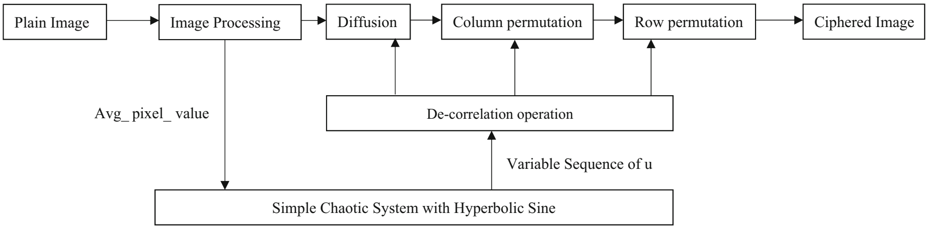


Fig. 4 A flowchart of the encryption scheme

Step 3: Sort the pseudorandom sequence for permutation
Step 4: Shift the pixel positions by column using the sorted elements.
Step 5: Shift the pixel positions by row using the sorted elements.

To provide a better understanding of this scheme, the pseudocode is provided in Table 2.

The decryption process of the proposed algorithm is the reverse process of the encryption algorithm. A flowchart of the decryption process is shown in Fig. 5.

The detailed decryption process includes the following steps.

Input: Plain image; Initial conditions for the chaotic system; Control parameter for the chaotic system; Average pixel value of the plain image
Output: Decrypted image
Step 1: Generate a pseudorandom sequence via the initial conditions and the average pixel values of the plain image
Step 2: Sort the pseudorandom sequence for row and column recovery.
Step 3: Shift the pixel positions by row
Step 4: Shift the pixel positions by column
Step 5: Transform the pseudorandom sequence and recover the pixel values of the image via XOR

To provide a better understanding of this scheme, the pseudo-code is provided in Table 3.

Because this cryptosystem is designed for use with grayscale images, it is suitable for encrypting all kinds of medical images. Figures 6, 7, and 8 show the encryption and decryption results of a 512*512 grayscale mammography image, a CT image and an MRI image, respectively. All the images are from a hospital and the DICOM database.

5 Performance analysis

As is well-known, an outstanding cryptosystem should resist all types of known attacks, including known-plaintext attacks, ciphertext attacks, statistical attacks, differential attacks, and various brute-force attacks. A corresponding security analysis has been performed on the proposed algorithm, including a key space analysis, a statistical analysis and a differential analysis.

5.1 Key space analysis

For a secure image cipher, the key space should be large enough to render a brute force attack infeasible. In this system, all the initial conditions and control parameters can be considered as secret keys. Because the basin of attraction of each initial condition is greater than 1, it could have more than $10^{15*4} = 10^{60}$ choices via a

Table 2 Image encryption scheme

Input: Plain image Org_Img, Initial conditions for the chaotic system, Control parameter for the chaotic system,

Output: Ciphered Image En_Img

```
[m,n] ← size(Org_Img);

Avg_pixel_value ← mean2(Org_Img)*10^(-5)     % mean2 is a function that returns the

                                               % average value of a matrix


x(1) ← x(1) + Avg_pixel_value

y(1) ← y(1)

z(1) ← z(1)

u(1) ← u(1)
s(1) ← u(1)*10^4 – floor(u(1)*10^4)

For i=1:1:m*n                          % Generate pseudorandom sequence that will
                                       % be used for diffusion and permutation

    [dx, dy, dz, du] ← Runge-Kutta (x(i), y(i), z(i), u(i))

    x(i+1) ← x(i) +dx

    y(i+1) ← y(i) +dy

    z(i+1) ← z(i) +dz

    u(i+1) ← u(i) +du
    s(i+1) ← u(i+1)*10^4 – floor(u(i+1)*10^4)
End
```

Table 2 (continued)

Input: Plain image Org_Img, Initial conditions for the chaotic system, Control parameter for the chaotic system,

Output: Ciphered Image En_Img

```
Count=1                                 % Count flag
For i=1:m                               % Diffusion Operation
    For j=i:n
        diff(Count) ← mod (s(Count)*10^14, 256) % transform s, which could be used for XOR
        En_Dif(i,j)=bitxor(Org_Img(i,j), diff (Count));   % Bitwise exclusive OR
        Count= Count+1;
    End
End


S_index ← Sort(s)

For i=1:n                                     % Column-wise permutation
    For j=1:m

        En_per_col (i,j) ← Sort (En_Dif, S_index)

    End
End
For i=1:m                                     % Row-wise permutation
    For j=1:n

        En_Img (i,j) ← Sort (En_per_col, S_index)

    End
End
```

resolution of 10^{-15}, in terms of a numeric calculation. Moreover, if a range of control parameters were to be considered for the key space, the key space of this system would far exceed 10^{90}. Such a large key space provides sufficient security against brute-force attacks.

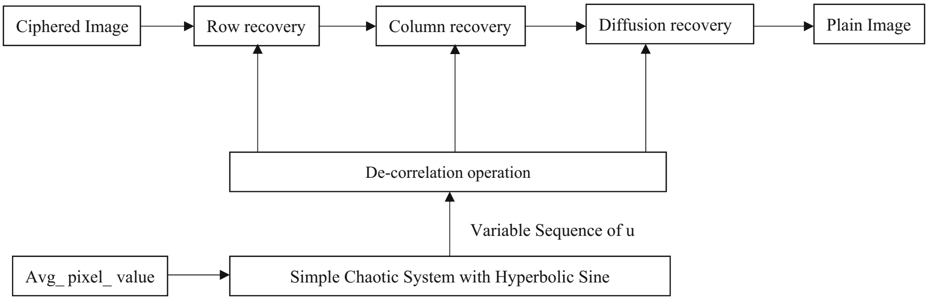


Fig. 5 The flowchart of the decryption scheme

5.2 Key sensitivity analysis

The key space includes all initial conditions and control parameters. Due to the mutual independence of the secret keys, the practical approach is to analyze each key with a tiny change while leaving the other keys unchanged.

To perform a sensitivity analysis using the initial condition (x, y, z, u) = (7, 9, 10, 13), we made a slight change of Δx = 10^(−15). The modified key is (x + Δx, y, z, u) = (7 + 10^ (−15), 9, 10, 13). The difference in the output sequence between the two initial conditions is shown in Fig. 9.

In Fig. 9, the sequence of the differences between the two variables is a pseudo-random sequence, and we verified that the distribution has random statistical characteristics.

To test the key sensitivity further, we used these two keys to encrypt the same image. The results show that 95% of the pixels are different. The difference between the two encrypted images is shown in Fig. 10.

Therefore, the difference between ciphertexts encrypted via different keys is sufficiently large to maintain high security against this kind of known-plaintext attack.

5.3 Histogram analysis

The histogram of an image reveals the distribution of its pixel values. An ideal encrypted image should have a uniform but completely different histogram compared to the plain image to prevent the adversary from extracting any meaningful information from the fluctuating histogram of the cipher image [29].

Figure 11 shows the histograms of the plain and ciphered images of a CT image.

For the quantitative analyses of histograms, we employ variances of histograms to evaluate the uniformity of the ciphered images. Lower variance values indicate a higher uniformity in the encrypted images. The variance of the histograms is presented as follows:

$$\mathrm{var}(Z) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}\left(\mathrm{z}_{\mathrm{i}}-z_j\right)^2 \tag{6}$$

Table 3 Image decryption scheme

Input: Ciphered image En_Img, Initial conditions for the chaotic system, control parameter for the chaotic system, Avg_pixel_value of Org_Img

Output: Plain Image Org_Img

```
[m,n] ← size(En_Img);

x(1) ← x(1) + Avg_pixel_value

y(1) ← y(1)

z(1) ← z(1)

u(1) ← u(1)

s(1) ⟵ u(1)*10^4 – floor(u(1)*10^4)

For i=1:1:m*n                    % Generate a pseudorandom sequence that will
                                 % be used for decryption
    [dx, dy, dz, du] ← Runge-Kutta (x(i), y(i), z(i), u(i))

    x(i+1) ← x(i) +dx

    y(i+1) ← y(i) +dy

    z(i+1) ← z(i) +dz

    u(i+1) ← u(i) +du

    s(i+1) ⟵ u(i+1)*10^4 – floor(u(i+1)*10^4)
End

S_index ← Sort(s)

For i=1:m                        % Row-wise permutation recovery
   For j=1:n
      De_per_row (i,j) ← Sort (En_Img, S_index)
```

Table 3 (continued)

Input: Ciphered image En_Img, Initial conditions for the chaotic system, control parameter for the chaotic system, Avg_pixel_value of Org_Img

Output: Plain Image Org_Img

```
    End
End

For i=1:n                              % Column-wise permutation recovery
    For j=1:m
        De_per_col (i,j) ← Sort (De_per_row, S_index)
    End
End

Count=1                                % Count flag
For i=1:m                              % Diffusion recovery
    For j=i:n
        diff(Count) ← mod (s(Count)*10^14, 256) % transform s, which could be used for XOR
        Org_Img (i,j)=bitxor(De_per_col (i,j), diff (Count)); % Bitwise exclusive OR
        Count= Count+1;
    End
End
```

where Z is the vector of the histogram values and z_i and z_j are the numbers of pixels whose gray values are equal to i and j, respectively. In this experiment, we used an initial condition of $(x, y, z, u) = (7, 9, 10, 13)$ and calculated the variances of the plain images and the encrypted images.

The variance value is 1,293,577.2343 for the histogram of the plaintext image "Lena" and 3903.0000 for the histogram of the ciphered image. Therefore, these simulation results indicate that any statistical attack on the proposed scheme are useless.

5.4 Correlation analysis

A high correlation typically exists between pixels of an image, and this correlation is an intrinsic feature. Thus, a secure encryption scheme should obscure this relationship

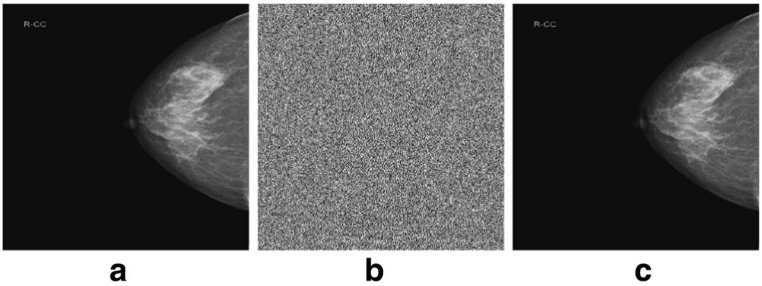


Fig. 6 Encryption and decryption results for a mammography image: (**a**) Plain image; (**b**) Encrypted image; (**c**) Decrypted image

to improve the resistance against statistical analysis. For this calculation, we use the following equations:

$$\begin{cases} \mathrm{E}(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \\ Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right) \\ \gamma_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)D(y)}} \end{cases}. \tag{7}$$

The correlations between adjacent pixels in the plain image and the encrypted image are shown in Fig. 12. Table 4 provides the correlation coefficients of the original and encrypted images shown in Fig. 10. This correlation analysis proves that the encryption scheme satisfies zero co-correlation, which is a private high-level security.

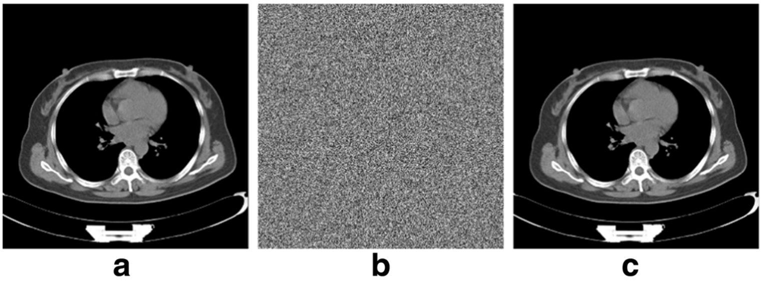


Fig. 7 Encryption and decryption results for a CT image: (**a**) Plain image; (**b**) Encrypted image; (**c**) Decrypted image

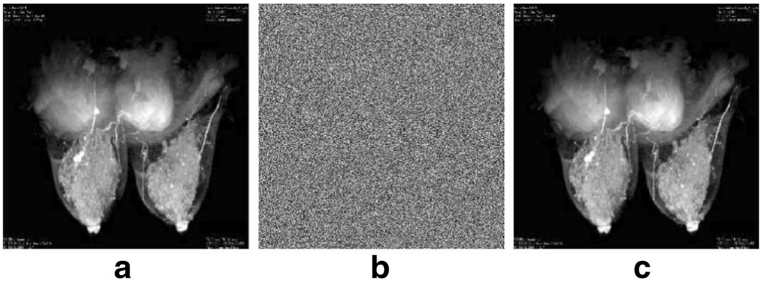


Fig. 8 Encryption and decryption results for an MRI image: (**a**) Plain image; (**b**) Encrypted image; (**c**) Decrypted image

5.5 Differential attack analysis

In general, the relationship between a plain image and an encrypted image can be traced to the differences caused by a specific change to the plain image. Two evaluating indicators are usually used to test the effect of a 1-bit change in the plain-image on the corresponding cipher-image. They are the number of pixel change rates (NPCR) and the unified average changing intensity (UACI) [27]. NPCR and UACI are calculated as follows:

$$\begin{aligned} NPCR &= \frac{\sum_{i,j} D(i,j)}{\mathrm{W} \times \mathrm{H}} \times 100\% \text{ and} \\ UACI &= \frac{1}{W \times H}\left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255}\right] \times 100\%, \end{aligned} \tag{8}$$

where c_1 and c_2 are two images with the same size (M × N). If c_1 (i, j) = c_2 (i, j), then D(i, j) = 1; otherwise D(i, j) = 0. The NPCR and UACI score of CT image are 99.5804% and 33.3227%.

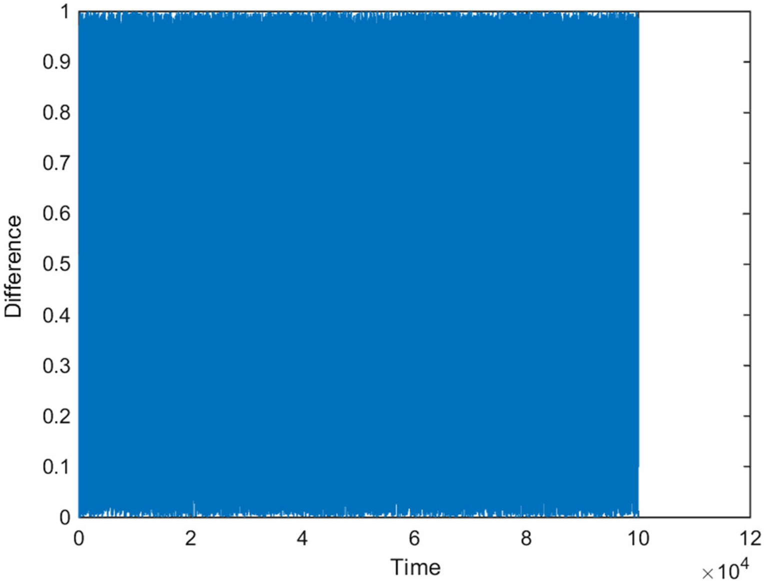


Fig. 9 The difference between two variables of x and x + Δx

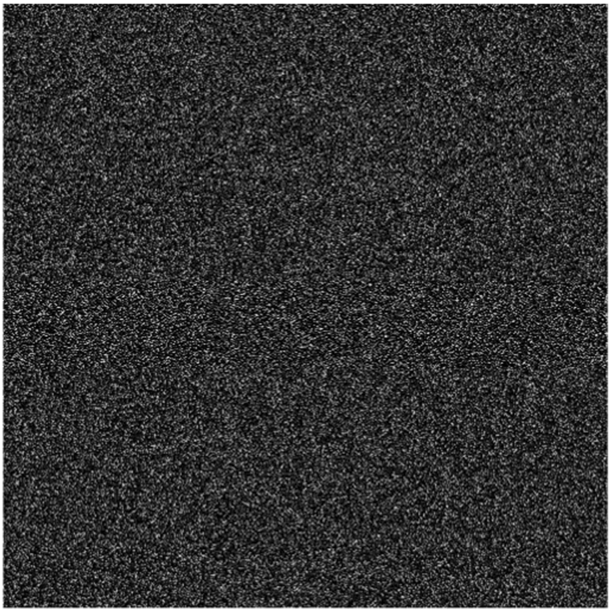


Fig. 10 The difference between the two encrypted images

5.6 Overall performance

As revealed in Sections 5.1–5.5, the proposed scheme has a large key space ($>>2^{100}$), which can provide sufficient security against brute-force attacks. The key is highly sensitive, which provided a high level of security against known plaintext attacks. Histogram and correlation analysis indicate that the proposed scheme removes the intrinsic features of plain images; thus, any statistical attacks on the proposed scheme are useless. Finally, the NPCR and UACI scores are close to ideal values, which indicates that the proposed scheme provides sufficient security against differential attack. Therefore, this proposed scheme provides sufficient security against all known attacks.

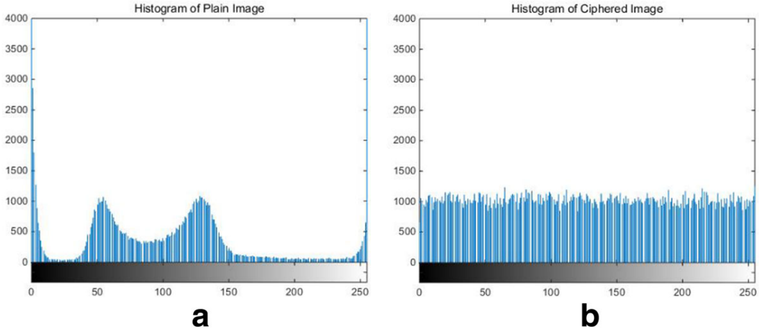


Fig. 11 Histograms of plain and encrypted images of a CT image

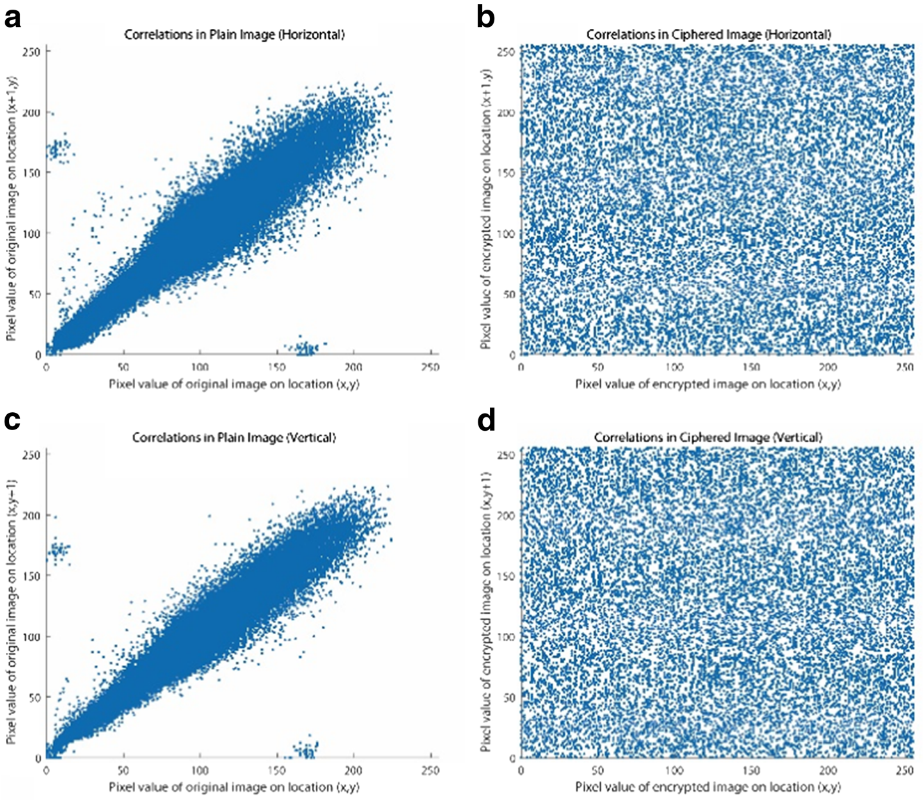


Fig. 12 Correlation analysis for plain and encrypted CT image versions: (**a**) Correlations of the horizontal adjacent pixels for the plain image; (**b**) Correlations of the horizontal adjacent pixels for the encrypted image; (**c**) Correlations of vertical adjacent pixels for the plain image; (**d**) Correlations of the vertical adjacent pixels for the encrypted image

5.7 Comparison results, discussion and future work

5.7.1 Comparison results

In this section, we compared the performance of our algorithm to several typical image encryption algorithms. We evaluate the performance of our proposed method by conducting several tests based on image quality and other evaluation metrics. To compare the correlation values, we used the following equation

$$\mathrm{CC} = \frac{|C_h| + |C_v| + |C_d|}{3}. \tag{9}$$

Table 4 Correlation coefficients of adjacent pixels in the plain and encrypted image

Figure name	Direction	Plain-image	Ciphered image
CT image	Horizontal	0.978292	0.002500
CT image	Vertical	0.955481	0.006207
CT image	Diagonal	0.940737	0.003071

Table 5 Comparison of the proposed image encryption method with recent state-of-the-art encryption algorithms (the test image is "Lena")

Method name	Key space	Entropy	Correlation coefficient(CC)	NPCR	UACI
Ideal value	$>2^{100}$	≈8	≈0	≈99.6	≈33.4
Proposed algorithm	$>2^{300}$	7.9969	0.0025	99.6140	33.4805
Ref [29]	$>2^{400}$	N/A	0.0006	99.7826	33.4964
Ref [6]	2^{711}	7.9998	0.0019	99.6090	33.4500
Ref [5]	2^{711}	7.9978	0.0031	99.6100	33.5000

The image encryption method described in [29] uses a chaotic system of mixed linear–nonlinear coupled map lattices for diffusion of the image encryption. In [6], a secure video summarization framework was introduced that used a 2-D chaotic map to generate a set of permutation keys to shift the positions of the plain keyframe pixels, followed by a diffusion per block using arithmetic matrix multiplication over the finite field. A novel image encryption scheme proposed in [5] was based on the Zaslavsky chaotic map, while [18] described a cryptosystem using a newly enhanced chaotic map designed from an existing one-dimensional chaotic economic map.

A performance comparison of all these algorithms is shown in Tables 5 and 6.

5.7.2 Discussion

Tables 5 and 6 show that the key space of the proposed algorithm is the smallest of the compared algorithms. This is because we could not determine the exact key space value but could estimate only the most conservative value. We have tried and failed to figure out the basin of the attraction and the whole control parameter space, which would allow us to estimate the exact value of the key space. Because using Lyapunov exponents is the most reliable method of indicating chaos and is defined via infinite time, the algorithm does not run very fast. Assuming that the entire initial condition space and control parameter space is 1; the key space would be 10^{60}. Assuming that it would take 1 ms to calculate the Lyapunov exponent of every secret key, more than $1.15*10^{42}$ days would be required to calculate the key space. Our estimate shows the most conservative values; however, the true key space may be far greater that the value found in this paper.

The entropy, correlation coefficient, NPCR and UACI scores of the proposed algorithm are not the highest among the compared algorithms, but its scores are very close to the ideal values of those metrics. The differences in score between our algorithm and the ideal value are 0.0048% (entropy), 0.0014% (NPCR), and 0.24%. Because this encryption scheme is very simple and can encrypt an image in a single round, we believe that only the chaotic system described in Section 2 and the pseudorandom sequence generated in Section 3 have this good performance.

Table 6 Comparison of the proposed image encryption method with recent state-of-the-art encryption algorithms (the test image is an MRI image)

Method name	Key space	Entropy	Correlation coefficient(CC)	NPCR	UACI
Ideal value	$>2^{100}$	≈8	≈0	≈99.6	≈33.4
Proposed algorithm	$>2^{300}$	7.9961	0.0020	99.6326	33.4377
Ref [18]	2^{1275}	15.1771	0.0068	100.0	50.0832

5.7.3 Future work

Chaos theory can be applied outside of the natural sciences. For example, chaotic invariants and relevance vector machines (RVM) could be used in human action recognition [2]. Because this paper has proposed a new simple chaotic system, one could attempt to use this system to solve problems of action recognition.

6 Conclusion

In this paper, a new simple chaotic system with a hyperbolic sine and its encryption scheme are proposed. Because the chaotic sequence does not fit a uniform distribution and the randomness of the sequence is not quite ideal, a decorrelation operation is used to improve the randomness of the sequence. Due to the given features in the dynamics of the pseudorandom proposed sequence, cryptosystem security has been enhanced. A key space analysis, key sensitivity analysis, histogram analysis, correlation analysis and differential attack analysis showed that this algorithm is highly resistant to known attacks such as known-plaintext attacks, ciphertext attacks, statistical attacks, differential attacks, and various other brute-force attacks.

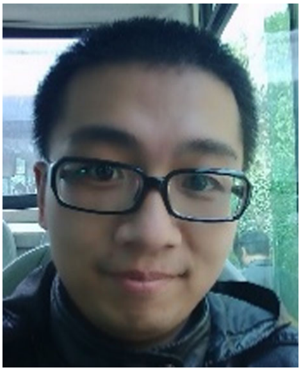
Based on these advantages, the proposed method could be used as an assistive tool for telemedical systems or in secure medical systems. In future work, we intend to implement the method in hardware or extend it via parallel execution to reduce the execution time of the encryption algorithm. Although the proposed scheme focuses on medical image encryption, it is not limited to this area. Additional future work could explore related applications in other information security fields.

Acknowledgements The authors would like to thank Wenlong Xin for providing knowledge of the medical images. All the medical images used are from the First Hospital affiliated with Lanzhou University and the DICOM database. This study was supported by Fundamental Research Funds for the Central Universities No. lzujbky-2016-238) and the National Natural Science Foundation of China (No. 61175012).

References

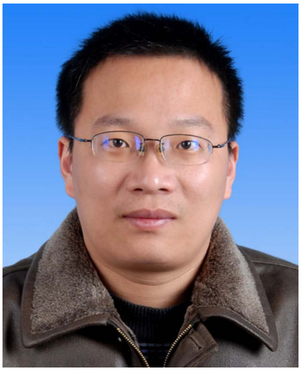
1. Collen MF, Ball MJ (eds) (2015) The history of medical informatics in the United States. Springer, Berlin
2. Cui J, Liu Y, Xu Y, Zhao H, Zha H (2013) Tracking generic human motion via fusion of low- and high-dimensional approaches. IEEE Transactions on Systems Man & Cybernetics Systems 43(4):996–1002
3. Gutub AAA, Tabakh AA, Al-Qahtani A, Amin A (2013) Serial vs. parallel elliptic curve crypto processor designs. In IADIS International Conference: Applied Computing, pp 67–74
4. Hamza R (2017) A novel pseudo random sequence generator for image-cryptographic applications. J Inf Secur Appl 35:119–127

5. Hamza R, Titouna F (2016) A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Information Security Journal: A Global Perspective 25(4–6):162–179
6. Hamza R, Muhammad K, Lv Z, Titouna F (2017) Secure video summarization framework for personalized wireless capsule endoscopy. Pervasive Mob Comput 41:436–450
7. Hu HP, Liu LF, Ding ND (2013) Pseudorandom sequence generator based on the chen chaotic system. Comput Phys Commun 184(3):765–768
8. Jiunn-Woei L, Yen DC, Wang Y-T (2014) An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. Int J Inf Manag 34(1):28–36
9. Kumar S, Sharma RK (2017) Securing color images using two-square cipher associated with Arnold map. Multimed Tools Appl 76(6):8757–8779
10. Li C, Sprott JC (2014) Coexisting hidden attractors in a 4-D simplified Lorenz system. Int J Bifurcation Chaos 24(03):1450034
11. Li C, Sprott JC (2014) Finding coexisting attractors using amplitude control. Nonlinear Dynam 78(3):2059–2064
12. Lima JB, Madeiro F, Sales FJR (2015) Encryption of medical images based on the cosine number transform. Signal Process Image Commun 35:1–8
13. Liu Y, Luo Y, Song S, Cao L, Liu J, Harkin J (2017) Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation. Int J Bifurcation Chaos 27(03):1750033
14. Liu J, Sprott JC, Wang S, Ma Y (2018) Simplest chaotic system with a hyperbolic sine and its applications in DCSK Scheme. IET Communications. https://doi.org/10.1049/iet-com.2017.0455
15. Mantos PL, Maglogiannis I (2016) Sensitive patient data hiding using a ROI reversible steganography scheme for DICOM images. J Med Syst 40(6):156
16. Munmuangsaen B, Srisuchinwong B, Sprott JC (2011) Generalization of the simplest autonomous chaotic system. Phys Lett A 375(12):1445–1450
17. Pan SM, Wen RH, Zhou ZH, Zhou NR (2017) Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform. Multimed Tools Appl 76(2): 2933–2953
18. Parvees MM, Samath JA, Bose BP (2016) Secured medical images-a chaotic pixel scrambling approach. J Med Syst 40(11):232
19. Parvez MT, Gutub AAA (2011) Vibrant color image steganography using channel differences and secret data distribution. Kuwait J Sci Eng 38(1B):127–142
20. Pham VT, Volos C, Jafari S, Kapitaniak T (2017) A novel cubic–equilibrium chaotic system with coexisting hidden attractors: analysis, and circuit implementation. J Circuits Syst Comput 27(04):1850066. https://doi.org/10.1142/S0218126618500664
21. Piper JR, Sprott JC (2010) Simple autonomous chaotic circuits. IEEE Trans Circuits Syst II Express Briefs. 57(9):730–734
22. Sajjad M, Muhammad K, Baik SW, Rho S, Jan Z, Yeo SS, 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
23. Sprott JC (2011) A new chaotic jerk circuit. IEEE Trans Circuits Syst II Express Briefs 58(4): 240–243
24. Sun XH (2013) Image encryption algorithms and practices with implementations in C#. Sciencepress, Beijing
25. Wang X, Vaidyanathan S, Volos C, Pham VT, Kapitaniak T (2017) Dynamics, circuit realization, control and synchronization of a hyperchaotic hyperjerk system with coexisting attractors. Nonlinear Dynam 89(3):1673–1687
26. Weaver CA, Ball MJ, Kim GR, Kiel JM (2016) Healthcare information management systems. Springer International Publishing, Cham
27. Wu Y, Noonan JP, Agaian S (2011) NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology. Journal of Selected Areas in Telecommunications (JSAT) 2:31–38
28. Xu Y, Wang H, Li Y, Pei B (2014) Image encryption based on synchronization of fractional chaotic systems. Commun Nonlinear Sci Numer Simul 19(10):3735–3744
29. Zhang YQ, Wang XY (2014) A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf Sci 273(8):329–351
30. Zhang Y, Qiu M, Tsai CW, Hassan MM, Alamri A (2015) Health-CPS: healthcare cyber-physical system assisted by cloud and big data. IEEE Syst J 11(1):88–95



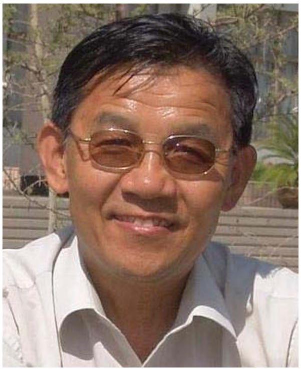
Jizhao Liu received the B.S. and M.S. degree from Lanzhou University, Lanzhou, China, in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree at Lanzhou University. His research activities and interests are currently focused on chaotic system and image encryption.

Yide Ma received the B.S. and M.S. degrees in radio technology from the University of Electronics Science and Technology, Chengdu, China, in 1984 and 1988, respectively, and the Ph.D. degree from the Department of Life Science, Lanzhou University, Lanzhou, China, in 2001. He is currently a Professor with the School of Information Science and Engineering, Lanzhou University. He has authored over 150 papers in major journals and international conferences and several textbooks, including Applications of Pulse-Coupled Neural Networks (Springer\& Higher Education Press (Beijing, China), 2010, in English) and Principle and Application of Microcomputer (Beijing, China: Higher Education Press, 2011, in Chinese). His current research interests include artificial neural networks, digital image processing, pattern recognition, digital signal processing, and computer vision.



Shouliang Li received the B.S. degree the M.S. degree from Lanzhou University, Lanzhou, China, and now is working towards to the Ph.D. degree in Lanzhou University. Currently, he is an engineer in School of Information Science and Engineering, Lanzhou University, Lanzhou, China. His research interests include nonlinear circuits and computer simulations.

Jing Lian received the B.S. and M.S. degrees in communication and information engineering from Lanzhou Jiaotong University, Gansu, China, in 2005 and 2010, respectively. He is currently pursuing the Ph.D. degree in radio physics at Lanzhou University. His current research interests include artificial neural networks, image processing, object recognition.



Xinguo Zhang received the B.S. degree from Lanzhou University, Lanzhou, China. He is retired from Lanzhou University, before that, he is a senior engineer in School of Information Science and Engineering, Lanzhou University, Lanzhou. His research interests include the design and analysis of nonlinear circuits and nonlinear signal processing.