IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 12, 2019, accepted April 7, 2019, date of publication April 11, 2019, date of current version April 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2910563

Galois Field-Based Image Encryption for Remote Transmission of Tumor Ultrasound Images

NAN WANG[1], GUIXIN DI[2], XIAOLAN LV[2], MIN HOU[2], DAN LIU[3], JUN ZHANG[1], AND XIAOJING DUAN[2]

[1]School of Mechanical and Electrical Engineering, Hebei Agricultural University, Baoding 071000, China
[2]Department of Functional Ultrasound, Affiliated Hospital of Hebei University, Baoding 071000, China
[3]Zhuhai People's Hospital, Zhuhai 519000, China

Corresponding author: Xiaojing Duan (cmwn@163.com)

This work was supported by the Science and Technology Project of Baoding under Grant 17ZF270 and Grant 18ZN020.

ABSTRACT The remote transmission of tumor ultrasound images is an important link in telemedicine. Based on the Galois field (GF), this paper proposes an encryption algorithm that ensures the security of tumor ultrasound images (TUIs) during the transmission. First, the grayscale image of the TUI was generated by the secure hash algorithm 1 (SHA-1) algorithm, and the resulting hash value was taken as the medical record summary, which was used to monitor the transmission of the TUI. Second, the 2D ciphertext image was expanded into 1D vectors, and the TUI was encrypted with the non-repetitive scrambling algorithm, coupled with two diffusion algorithms. The simulation results show that the coupled algorithm can ensure the safety of the TUIs in remote transmission.

INDEX TERMS Tumor ultrasound images (TUIs), Galois field (GF), image encryption, remote transmission, secure hash algorithm 1 (SHA-1) algorithm.

I. INTRODUCTION

With the development of health information technology, doctors are now able to exchange information with patients in the telemedicine environment. In this way, the repetitive testing, examination and medication are greatly reduced, and the medical resources are used more efficiently [1]. However, the information exchange may endanger the safety of the tumor ultrasound images (TUIs). During the transmission, the TUIs may be exposed to risks like theft, duplication, leakage and tampering. Thus, it is necessary to develop a TUIs encryption method that protects information authenticity, data integrity and patient privacy [2].

With high redundancy, huge amount of data and strong pixel correlation, the TUIs cannot be encrypted satisfactorily by the traditional encryption algorithms [3]. Neither can the TUIs be encrypted desirably by the recent digital image encryption methods [4]–[7], which have small key space and large error of information entropy. In fact, the TUIs encryption has not been studied intensively.

Chaotic encryption has long been proved as an effective alternative [8], but only Henon chaotic algorithm has been applied to encrypt the TUIs [9]. However, Henon, as a simple 2D nonlinear chaotic system, still faces the small key space and poor security of low-dimensional chaotic systems [10]. Arya *et al.* [11] generated a medical record summary by MD5 message-digest algorithm, yet this algorithm has been cracked and exposed to security risks.

In view of the above, this paper uses the secure hash algorithm 1 (SHA-1) to monitor the safety of TUIs transmission, and generate A 160-bit hash value as medical record summary. In addition, the TUIs were encrypted by two diffusion algorithms, namely, non-repetitive scrambling of 2D image into 1D vector and multiplication in Galois field (GF) (24). Then, the ciphertext image was converted from the TUIs by 3D Lorenz chaotic map [12]. After the conversion, the attacker can only see the ciphertext image, rather than the actual tumor ultrasound images. Finally, the decrypted image was coded by the SHA-1 and matched with the sender's UTI summary, to see if the UTIs had been tampered in the transmission process.

II. DESIGN OF ENCRYPTION PLAN

A. ENCRYPTION TECHNOLOGY

The SHA is a family of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard (FIPS).

The associate editor coordinating the review of this manuscript and approving it for publication was Sabah Mohammed.

This algorithm can create a 160-bit information summary through plaintext-string conversion, complementary operations and additional length calculation [13]. It was soon replaced by the slightly revised version SHA-1, a 160-bit hash function which resembles the earlier MD5 algorithm. However, any slight change of the plaintext information in the image will cause significant variation in the calculated hash value. If applied to the TUIs, the SHA-1 encryption process is equivalent to creating a ''fingerprint'' of the record. In this paper, the dynamic equations of Lorenz system mapping are introduced:

$$\begin{cases} x = a\,(y - x) + w \\ y = cx - y - xz \\ z = xy - bz \\ w = -yz + rw \end{cases} \tag{1}$$

where, a, b, c, w and r are parameters of the chaotic system. Equation set (1) is in the chaotic state when $a = 10$, $b = 8/3$, $c = 28$ and $-1.52 \leq \mathrm{r} \leq 0.06$.

The GF is an important, non-empty field in cryptography. The elements in the GF can be considered as the results of mode p GF (p), where p is a prime number. In practice, GF (p^w) is often employed to prevent data missing, with p being a prime number whose value is usually set to 2. The GF elements can be generated by primitive polynomials. The domain obtained by primitive polynomials has an additive unit of 0 and a multiplicative unit of 1. Our research selects the reduced polynomial $m(x) = x^4 + x + 1$in GF (2^4).

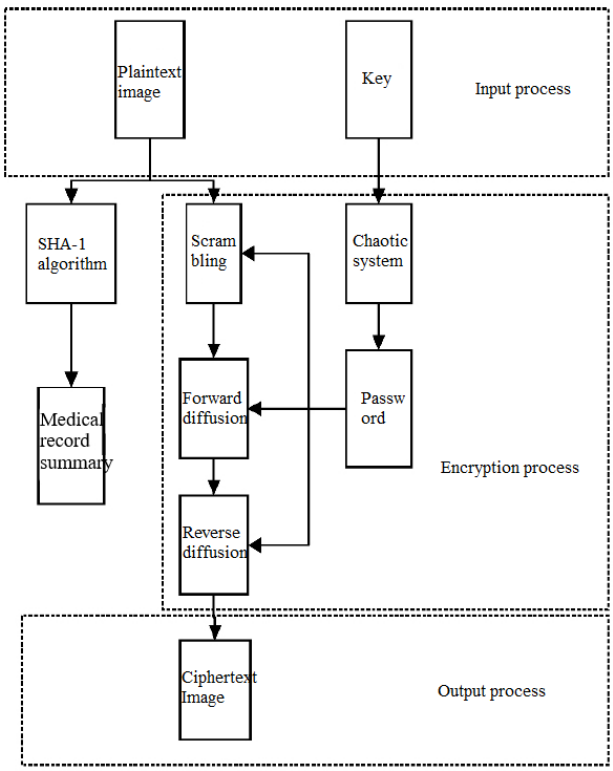


FIGURE 1. The flow of tumor ultrasound image encryption plan.

B. TUI ENCRYPTION

In our TUI encryption plan (Figure 1), the TUI was firstly converted into a grayscale image, and the hash value generated by the SHA-1, namely, 42817e38ab192e6b3bb2491578 ab3cf65a5cf7ec, was taken as the medical record summary. The summary was saved by the sender, while the TUI was decrypted by the receiver, who then encoded it with the SHA-1. Then, the hash value generated by the receiver was matched against the medical record summary.

The proposed encryption plan scrambles the pixel positions in the original image, and then changes the grayscale of the image for forward and reverse diffusions [14]. Next, the passwords were created with the initial parameter values of the chaotic Lorenz system as the keys. Let $M \times N$ (1,024 $*$ 768 pixels) be the size of the original image (format: .jpg). The encryption process involves the following steps:

(1) Initialize the parameter variables, x_0, y_0 and z_0, in the chaotic Lorenz system, taking them as the value of the given key K. Determine the pseudo-random sequences w_0 of $M \times N$ floating-point length, which is generated iteratively by hyperchaotic systems.

(2) Expand the 2D plaintext image matrix into 1D vectors by rows, and denote the result as $\boldsymbol{A}$. Generate the $M \times N$ in the chaotic system based on the pseudo-random sequence x_i ($i = 1, 2, \ldots, M \times N$). Retain the first pseudo-random number which is repeated in X only. Then, add the values in $\{1, 2, \ldots, M \times N\}$, which are not present in X, to the end of X in ascending order. Finally, swap $A(x_i)$ with $A(x_{\mathrm{MN}} - i + 1)$.

(3) Multiply the grayscales of the pixels by the GF (2^4) diffusion algorithm. The forward and reverse diffusion processes can be expressed as:

$$\begin{cases} C_{i,H} = C_{i-1,H} \times S_{i,H} \times P_{i,H} \\ C_{i,L} = C_{i-1,L} \times S_{i,L} \times P_{i,L} \\ C_i = (C_{i,H} \times 16 + C_{i,L}) \end{cases} \tag{2}$$

$$\begin{cases} C_{i,H} = C_{i+1,H} \times S_{i,H} \times P_{i,H} \\ C_{i,L} = C_{i+1,L} \times S_{i,L} \times P_{i,L} \\ C_i = (C_{i,H} \times 16 + C_{i,L}) \end{cases} \tag{3}$$

where, P is a 1D vector expanded from plaintext; C and S are cryptographic vectors, whose initial values C_0 and S_1 are derived from keys i $= 1, 2, \ldots, M \times N$; H and L are respectively the higher and lower 4 bits of the data.

To sum up, the ciphertext image of the TUI can be obtained through one scrambling and two diffusions. The decryption is the reverse of the encryption process.

III. SIMULATION EXPERIMENT

The proposed algorithm was simulated on the Matlab to verify its feasibility. Exhaustive attack method was used to attack the encrypted image. Figures 2-5 respectively show the plaintext image of the original TUI, the ciphertext image of the encrypted TUI, the ciphertext image of correct key decryption, and the ciphertext image of incorrect key decryption.

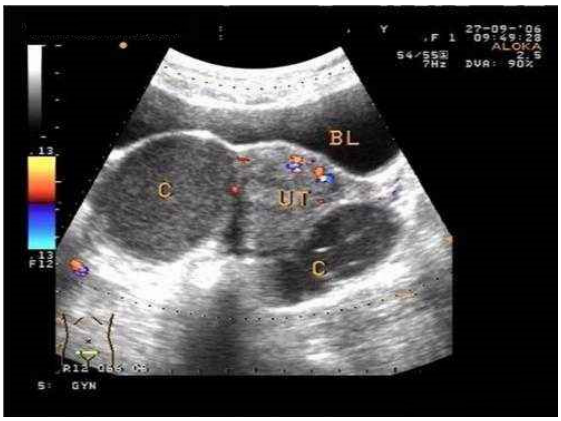


FIGURE 2. The plaintext image of the original gynecology tumor ultrasound image.

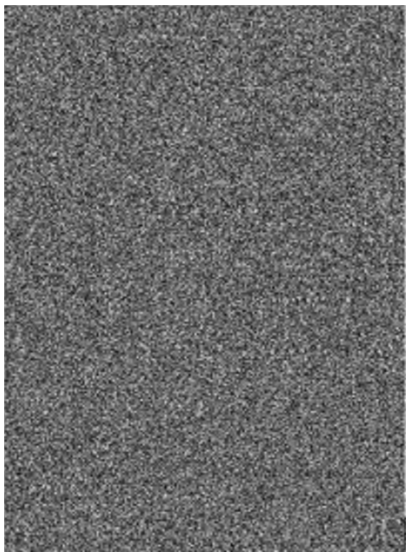


FIGURE 3. The ciphertext image of the encrypted gynecology tumor ultrasound image.

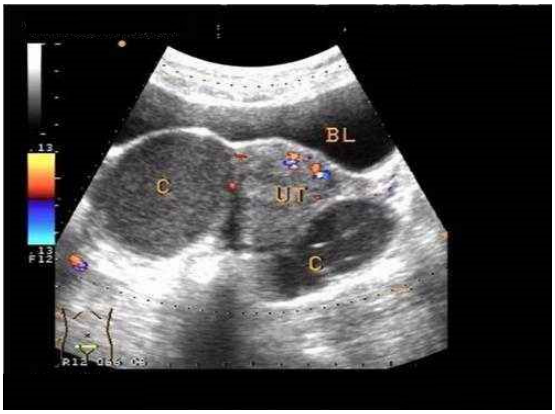


FIGURE 4. The ciphertext image of correct key decryption.

The ciphertext image of the encrypted TUI was sent to the receiver, who decrypted the image and encoded the generated hash value, 42817e38ab192e6b3bb2491578ab3cf65a5cf7ec, by the SHA-1. If the image is changed in propagation, the hash value should be changed to: b3df52208a35ba5a0ada56862a07a7a0b7f9d3bb (this value varies with the positions).

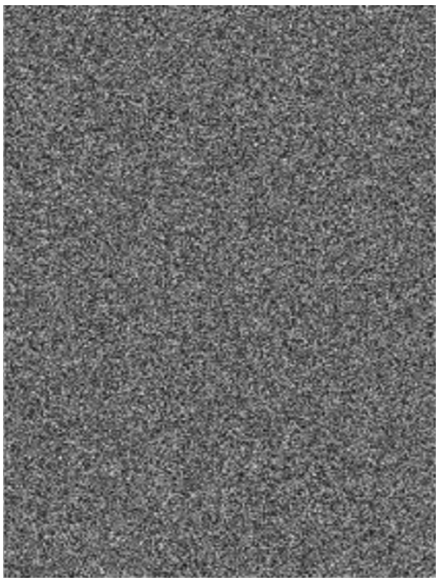


FIGURE 5. The ciphertext image of incorrect key decryption.

Then, the receiver looked up the hash value in the sender's medical record summary. If it was not found, the TUI must have been tampered during the transmission.

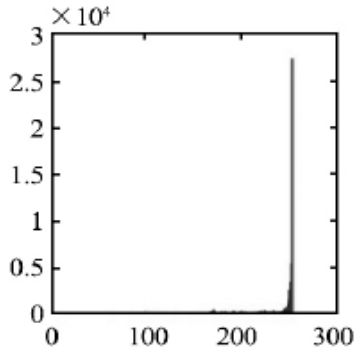


FIGURE 6. The plaintext histogram.

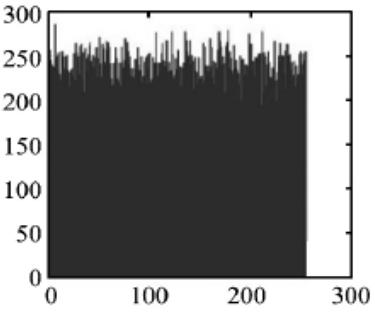


FIGURE 7. The ciphertext histogram.

IV. SAFETY ANALYSIS

A. HISTOGRAM ANALYSIS AND PEARSON'S CHI-SQUARED (X^2) TEST

Encryption covers up information by converting the plaintext image into noises. The correlation between histograms can

TABLE 1. The x^2 test results.

Image	x^2 value
The plaintext	3.238 2e+06
The ciphertext	259.3381

be evaluated by x^2 test. The x^2 generally has a negative correlation with the uniformity of the image pixel grayscale histogram, and the resistance to the attack of statistical analysis. Figures 6 and 7 respectively show the plaintext and ciphertext histograms of the TUI; Table 1 lists the x^2 values of the plaintext and ciphertext images of the TUI.

Obviously, the grayscale of the ciphertext image was closer to uniform distribution than that of the plaintext image, indicating the good effect of the encryption process.

B. CORRELATION ANALYSIS

The strong correlation between adjacent pixels in the plaintext image contains some information about the image. If it is manipulated by the attacker, the image content may be leaked [15]. Thus, a good encryption algorithm should weaken the pixel correlation of the image. To test the weakening effect of our algorithm, 2,000 pairs of adjacent pixels were randomly selected from the plaintext and ciphertext images of the TUI, and the horizontal, vertical, positive diagonal and negative diagonal pixel correlations were calculated:

$$r_{xy} = \frac{cov(u, v)}{\sqrt{D(u)}\sqrt{D(v)}} \tag{4}$$

where, cov (u, v) $= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(u))(y_i - E(v))$; D (u) $= \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))^2$; E (u) $= \frac{1}{N}\sum_{i=1}^{N}u_i$; $u = \{u_i\}$ and $v = \{v_i\}$ are two vectors. Note that N is an arbitrary logarithm of adjacent pixels, whose grayscales are (u_i, v_i), $i = 1, 2, \ldots, N$. The correlation images were plotted as Figure 8.

It can be seen that the pixel correlation decreased significantly after encryption, meaning that the image content has been protected well.

C. INFORMATION ENTROPY ANALYSIS

The uncertainty of image information can be measured by information entropy, which is positively correlated with the amount of information and the randomness of the events. To verify the effect of our algorithm, the information entropies of the plaintext and ciphertext images of the TUI were calculated as:

$$H = -\sum_{i=0}^{L} P(i)\, log2P(i) \tag{5}$$

where, L is the grayscale of the image; $P(i)$ is the occurrence probability of grayscale i. For the image with the grayscale $L = 256$, the simulated and theoretical information entropies H were both 8 for the ciphertext of TUI.

In addition, the classical image Lena was encrypted by the proposed algorithm and the algorithms in References [16] and [17]. As shown in Table 3, the information entropy of the image was closer to 8 after being encrypted by our algorithm than by the other two algorithms. This means our encryption algorithm can resist data attack more effectively than other algorithms.

TABLE 2. The correlation coefficients.

Image	Horizontal	Vertical	Positive diagonal	Negative diagonal
The plaintext	0.2638	0.7801	0.1201	0.1429
The ciphertext	0.0149	-0.0279	0.0032	0.0069

TABLE 3. Information entropy results.

Images	Information entropy
The plaintext of TUI	4.2915
The ciphertext of TUI	7.9862
The plaintext of Lena	7.3785
The ciphertext of Lena encrypted by our algorithm	7.9889
The ciphertext of Lena encrypted by the algorithm in Reference [16]	7.9833
The ciphertext of Lena encrypted by the algorithm in Reference [17]	7.9805

D. KEY SPACE AND SENSITIVITY ANALYSIS

Key space refers to the set of all legal keys. Its size is positively correlated with the encryption effect. In this paper, the keys are the initial parameter values of the Lorenz system: K $= \{x_0, y_0, z_0, w_0\}$, where $x_0 \in (-40, 40)$, $y_0 \in (-40, 40)$, $z_0 \in (-1, 81)$ and $w_0 \in (-250, 250)$. Since the step lengths of x_0, y_0 and z_0 are 10^{-13} and the step length of w_0 is 10^{-12}, the key space was calculated as 2.56×10^{59} and about 197 bit, which is larger than the key space in Reference [16] ($(10^{16})^2$). Thus, the proposed algorithm is proved effective in resisting violent attacks.

Then, some minor changes were made to the keys before TUI encryption. If the ciphertext image thus obtained differs greatly from that encrypted by the original keys, the encryption must be highly sensitive to the keys.

The difference in key sensitivity between images of the same size can be evaluated by the number of pixels' change rate (NPCR), unified averaged changed intensity (UACI) and blocked average changing intensity (BACI). The NPCR stands for the ratio of the number of different pixels to the total number of pixels:

$$NPCR(P_1, P_2) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|Sign(P_1(i,j) - P_2(i,j))| \times 100\% \tag{6}$$

where,

$$\text{Sign (x)} = \begin{cases} 1, & x > 0 \\ 0, & x = 0 \\ -1, & x < 0 \end{cases}$$

The UACI measures the mean ratio of the difference between the corresponding pixels to the maximum

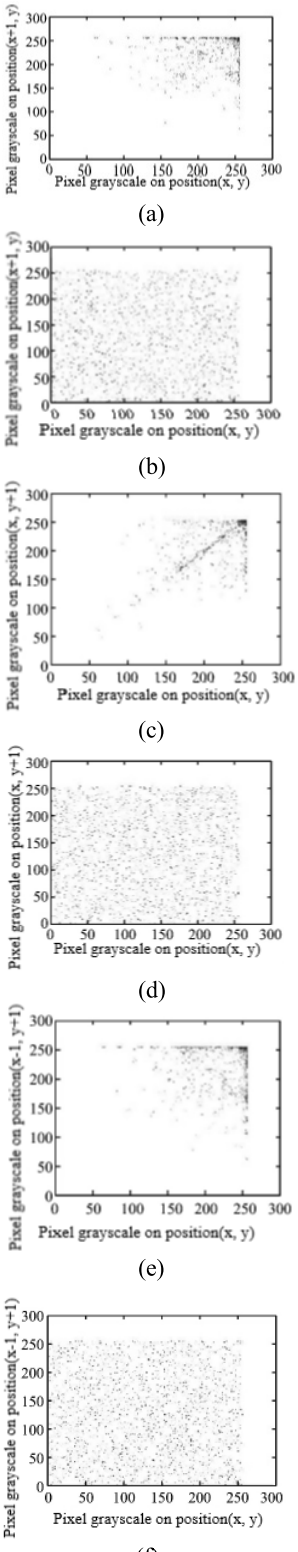


FIGURE 8. The correlation images. (a) Horizontal pixel correlation of plaintext image. (b) Vertical pixel correlation of ciphertext image. (c) Positive diagonal pixel coefficient of plaintext image. (d) Negative diagonal pixel coefficient of plaintext image. (e) Positive diagonal pixel coefficient of ciphertext image. (f) Negative diagonal pixel coefficient of ciphertext image.

difference (255) between the two images:

$$UACI\ (P_1, P_2) = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \times \frac{|(P_1\ (i,j) - P_2(i,j))|}{255 - 0} \times 100\% \quad (7)$$

The BACI can be calculated as:

$$BACI\ (P_1, P_2) = \frac{1}{(M-1)(N-1)} \sum_{i=1}^{(M-1)(N-1)} \frac{m_i}{255} \quad (8)$$

where, m is the small image block, $i = 1, 2, \ldots, (M-1)(N-1)$; $M \times N$ is the size of images P_1 and P_2. The BACI is often obtained in three steps: computing the absolute value of the difference image between the two images; decomposing the image; calculating the ratio of the absolute value of the difference between any two pixels of all small images to the maximum difference (255) between the two images.

TABLE 4. Results of key sensitivity analysis.

Initial value	Index		
	NPCR	UACI	BACI
x_0	99.589	33.429	26.757
y_0	99.602	33.467	26.726
z_0	99.603	33.470	26.781
w_0	99.603	33.471	22.782
Theoretical value	99.603	33.472	26.780

Here, 1,000 values are selected randomly from the key space, and the mean values of 1,000 NPCRs, UACIs and BACIs are calculated by changing x_0, y_0, z_0 by 10^{-13} and w_0 by 10^{-12}, respectively. The results are listed in Table 4.

The calculated results were close to the theoretical expectations of 99.603%, 33.472% and 26.780%, revealing that the ciphertext differs greatly after a slight change to the keys. It also shows that our encryption algorithm is highly sensitive to keys and resistant to differential attacks.

To sum up, the proposed algorithm is more efficient in dealing with common size images. Even if the target image is of a large size, our algorithm can outperform the general encryption algorithm in speed.

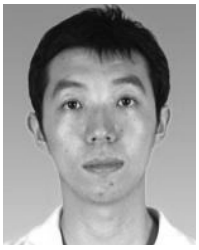
V. CONCLUSIONS

Focusing on security of TUI remote transmission, this paper develops a TUI encryption algorithm based on chaotic mapping and the GF. The algorithm combines encryption and monitoring of the transmitted TUI to enhance image security and reliability. The simulation results show that the proposed algorithm enjoys a large key space and effective resistance to violence, statistics and differential attacks, as well as a strong potential for application in telemedicine. The future research will further improve the encryption and decryption efficiency of the proposed algorithm.

REFERENCES

[1] A. Kevat, "Communication with patients and carers during consultations using electronic medical records: Ensuring preparedness for challenges and opportunities," *J. Paediatrics Child Health*, vol. 52, no. 7, p. 788, 2016.

[2] R. Amarasingham *et al.*, "An automated model to identify heart failure patients at risk for 30-day readmission or death using electronic medical record data," *Med. Care*, vol. 48, no. 11, pp. 981–988, 2010.
[3] Q. Zhang and L. Liu, "DNA coding and chaos-based image encryption algorithm," *J. Comput. Theor. Nanosci.*, vol. 10, no. 2, pp. 341–346, 2013.
[4] X.-J. Tong, Z. Wang, M. Zhang, and Y. Liu, "A new algorithm of the combination of image compression and encryption technology based on cross chaotic map," *Nonlinear Dyn.*, vol. 72, nos. 1–2, pp. 229–241, 2013.
[5] G. Sun and S. Bin, "A new opinion leaders detecting algorithm in multi-relationship online social networks," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 4295–4307, 2018.
[6] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "An efficient image encryption scheme using lookup table-based confusion and diffusion," *Nonlinear Dyn.*, vol. 81, no. 3, pp. 1151–1166, 2015.
[7] X.-J. Tong, P. Chen, and M. Zhang, "A joint image lossless compression and encryption method based on chaotic map," *Multimedia Tools Appl.*, vol. 76, no. 12, pp. 13995–14020, 2016.
[8] M. M. Churpek, T. C. Yuen, S. Y. Park, D. O. Meltzer, J. Hall, and D. P. Edelson, "Derivation of a cardiac arrest prediction model using ward vital signs," *Crit. Care Med.*, vol. 40, no. 7, pp. 2102–2108, 2012.
[9] M. F. M. Mursi, H. E. H. Ahmed, F. E. A. El-Samie, and A. H. A. El-Aziem, "Image encryption based on development of Hénon chaotic maps using fractional Fourier transform," *Int. J. Strategic Inf. Technol. Appl.*, vol. 5, no. 3, pp. 62–77, 2014.
[10] G. Geetha and K. Thamizhchelvy, "Design of digital signature algorithm by fractals and chaos theory," *Int. J. Comput. Appl.*, vol. 37, no. 5, pp. 50–57, 2012.
[11] P. K. Arya, K. Selvamani, and A. Kannan, "A SMS-based authentication approach for electronic health record in cloud environment," *J. Med. Imag. Health Inform.*, vol. 6, no. 7, pp. 1625–1630, 2016.
[12] G. Sun and S. Bin, "Router-level Internet topology evolution model based on multi-subnet composited complex network model," *J. Internet Technol.*, vol. 18, no. 6, pp. 1275–1283, 2017.
[13] H. Wang, S. Xiao, F. Lin, T. Yang, and L. T. Yang, "Group improved enhanced dynamic frame slotted ALOHA anti-collision algorithm," *J. Supercomput.*, vol. 69, no. 3, pp. 1235–1253, 2014.
[14] K. K. Singamaneni and P. S. Naidu, "Secure key management in cloud environment using quantum cryptography," *Ingenierie des Syst. d'Inf.*, vol. 23, no. 5, pp. 213–222, 2018.
[15] B. R. Devi, "Texture feature-based image searching system using wavelet transform approach," *Traitement du Signal*, vol. 35, no. 1, pp. 23–33, 2018.
[16] W.-S. Yap, R. C.-W. Phan, W.-C. Yau, and S.-H. Heng, "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map," *Nonlinear Dyn.*, vol. 80, no. 3, pp. 1483–1491, 2015.
[17] H. Zhu, C. Zhao, and X. Zhang, "A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem," *Signal Process., Image Commun.*, vol. 28, no. 6, pp. 670–680, 2013.



NAN WANG is currently pursuing the Ph.D. degree. He is currently a Lecturer with the School of Mechanical and Electrical Engineering, Hebei Agricultural University. His research interests include computational intelligence, image processing, and data analysis.

GUIXIN DI is currently pursuing the master's degree. She is currently a Chief Physician with the Department of Functional Ultrasound. Her research interests include abdominal, gynecological, obstetric fetal prenatal screening, and cardiovascular and superficial organs color Doppler imaging diagnosis.

XIAOLAN LV is currently pursuing the master's degree. She is currently a Physician with the Department of Functional Ultrasound, Affiliated Hospital of Hebei University. Her research interests include abdominal, gynecological, obstetric fetal prenatal screening, and cardiovascular and superficial organs color Doppler imaging diagnosis.

MIN HOU is currently pursuing the master's degree. She is currently a Physician with the Department of Functional Ultrasound, Affiliated Hospital of Hebei University. Her research interests include abdominal, gynecology, echocardiography, and fetal echocardiography.

DAN LIU is currently pursuing the master's degree. She is currently a Physician with Zhuhai People's Hospital. Her research interests include abdominal, gynecological, fetal prenatal screening, and superficial cardiovascular interventional ultrasound diagnosis.

JUN ZHANG is currently pursuing the bachelor's degree with the School of Mechanical and Electrical Engineering, Hebei Agricultural University. Her research interests include machine learning and pattern recognition.

XIAOJING DUAN is currently pursuing the bachelor's degree. She is also a Physician with the Department of Functional Ultrasound, Affiliated Hospital of Hebei University. Her research interests include abdominal, gynecological, obstetric fetal prenatal screening, and cardiovascular and superficial organs color Doppler imaging diagnosis.