Secure and Energy-Efficient Data Transmission System Based on Chaotic Compressive Sensing in Body-to-Body Networks

Haipeng Peng, Ye Tian, Jürgen Kurths, Lixiang Li, Yixian Yang, and Daoshun Wang

***Abstract*—Applications of wireless body area networks (WBANs) are extended from remote health care to military, sports, disaster relief, etc. With the network scale expanding, nodes increasing, and links complicated, a WBAN evolves to a body-to-body network. Along with the development, energy saving and data security problems are highlighted. In this paper, chaotic compressive sensing (CCS) is proposed to solve these two crucial problems, simultaneously. Compared with the traditional compressive sensing, CCS can save vast storage space by only storing the matrix generation parameters. Additionally, the sensitivity of chaos can improve the security of data transmission. Aimed at image transmission, modified CCS is proposed, which uses two encryption mechanisms, confusion and mask, and performs a much better encryption quality. Simulation is conducted to verify the feasibility and effectiveness of the proposed methods. The results show that the energy efficiency and security are strongly improved, while the storage space is saved. And the secret key is extremely sensitive, 10^{-15} perturbation of the secret key could lead to a total different decoding, the relative error is larger than 100%. Particularly for image encryption, the performance of the modified method is excellent. The adjacent pixel correlation is smaller than 0.04 in different directions including horizontal, vertical, and diagonal; the entropy of the cipher image with a 256-level gray value is larger than 7.98.**

***Index Terms*—Body to body network (BBN), chaotic compressive sensing (CCS), image encryption, secure and energy-efficient transmission.**

I. Introduction

WIRELESS body area networks (WBANs) include many sensors implanted in a body or wore on a body, and body to body network (BBN) is formed by several connected WBANs [1]. WBAN is proposed based on the requirement of remote medical treatment, implanted sensors in a body or wearable sensors on a body can monitor physiological states, such as heart rate, pulse rate, body temperature, blood pressure, electrocardiogram (ECG) and electroencephalogram (EEG) [2]. These sensors send the collected data to hospitals or medical centers. Doctors can diagnose a possible appearing disease using the data remotely, and then propose a treatment plan, which can facilitate the patients and save medical resources. WBAN can also be applied in other scenarios such as babies or the aged monitor, and the collected data can also be sent to a medical database which can be used for research.

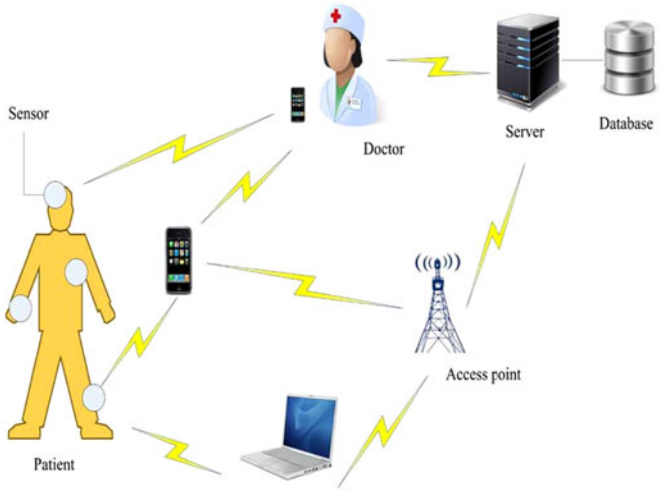


Fig. 1. WBAN deployment diagram. The patient equipped with sensors can send the collected data to doctors or database. The sensors can be equipped to monitor heart rate, pulse rate, body temperature, blood pressure. The collected data can be transmitted to the cell phone or laptop, and then to the database or doctor by infrastructure network.

The transmission distance of sensors in WBAN is limited, so the transmission of WBANs should rely on the infrastructure network. In Fig. 1, sensors distributed in different parts of the patient's body collect data and send it to the terminals like cell phones, laptop computers, etc by ZigBee or Bluetooth. These terminals then send the data to the doctors or the medical database by access points. Doctors can use the received data and the historical data from the database to diagnose a disease and

Manuscript received October 16, 2016; revised January 3, 2017; accepted January 31, 2017. Date of publication May 8, 2017; date of current version May 24, 2017. This work was supported by the National Key Research and Development Program of China under Grant 2016YFB0800602, the National Natural Science Foundation of China under Grants 61573067 and 61472045, the Beijing City Board of Education Science and Technology Project under Grant KM201510015009, and the Beijing City Board of Education Science and Technology Key Project under Grant KZ201510015015. This paper was recommended by Associate Editor S. Ostadabbas.

H. Peng, Y. Tian, L. Li, and Y. Yang are with the Information Security Center, State Key Laboratory of Networking and Switching Technology, and National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: penghaipeng@bupt.edu.cn; tianye172@bupt.edu.cn; li_lixiang2006@163.com; 365257599@qq.com).

J. Kurths is with Potsdam Institute for Climate Impact Research, D14473 Potsdam, Germany (e-mail: kurths@pik-potsdam.de).

D. Wang is with the Department of Computer Science and Technology, Tsinghua University, Beijing, CO 10084, China (e-mail: daoshun@mail.tsinghua.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TBCAS.2017.2665659

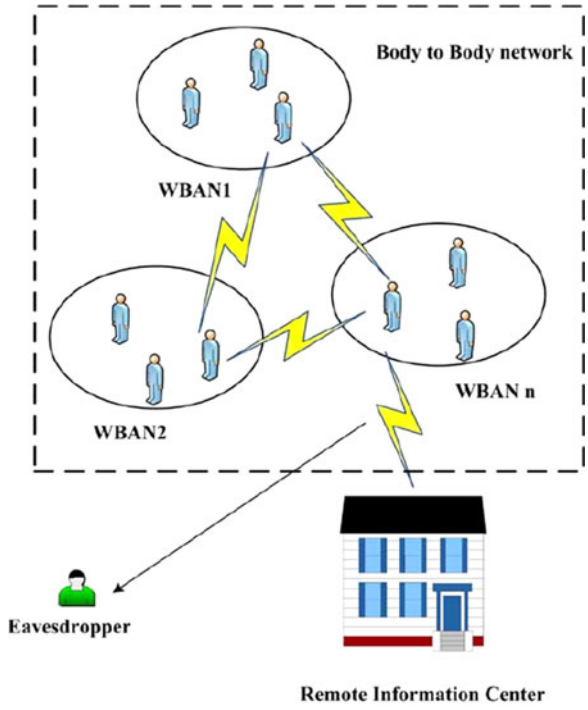


Fig. 2. BBN diagram. Several persons form a WBAN, and several WBANs form a BBN. The sensors can collect body data of persons and environment information. The persons in BBN can communicate with each other in WBAN or inter-WBANs. The collected body data or environment information can be sent to remote information center by relay channels. The eavesdropper can intercept some information because of the wireless links.

propose a treatment plan. Also basic medical research can be conducted using the data from the database.

WBAN can extend the site-fixed and time-specific medical treatment to mobile and real-time one, which can facilitate the patients, especially under emergency, and save medical resources especially in remote areas. There are many projects about WBAN for health care like CodeBlue project in Harvard university which can fulfill multi-hop transmission by the router nodes [3]. Base on CodeBlue, advanced health and disaster aid network is being developed in Johns Hopkins university [4]. But a very limited number of sensors can be put on each patient because of the limited bandwidth. Wearable health monitoring systems (WHMS) in Alabama university targets a larger-scale system for health monitor, but the power consumption can hamper the system realization [5].

The above projects mainly focus on health care. And the node number is limited, power consumption is inevitable for larger-scale and multi-hop transmission demand. Along with the expanding applications, WBAN evolves to BBN, which consists of many WBANs as showed in Fig. 2. BBN can not only be used for remote medical treatment, but also be used for entertainment, interactive games and sports [1]. In Fig. 2, every persons implants or wears sensors, three or more persons form a WBAN and all WBANs form the BBN. Sensors can collect the body data of the persons and the environment information. Every WBAN can send their data to the remote information center by relay link in BBN. For instance, in Fig. 2, WBAN 1 can send their data to WBAN 2 directly or WBAN n indirectly, and ultimately to the remote information center by other relay links. The center uses this data to make decision and then sends the advices to the persons. Some previous works about BBN are as follows. A channel model for WBAN cooperative transmission in BBN is proposed and its performance is evaluated in [6]. Interference reducing between neighboring WBANs is analyzed in [7]. Interference mitigation and coexistence strategies in IEEE 802.15.6 is proposed in [8]. A multi-hop body-to-body routing protocol for BBN is presented in [9].

Compared with WBAN, the network scale of BBN is expanded, and the sensors not only have to transmit their own data but also have to help other sensors to relay data. The links in BBN are easy to be eavesdropped like in Fig. 2. There will be two problems.

(1) Energy consuming: the relay task will consume much energy while the energy of the sensors is limited and the replacement of implanted equipment is very difficult especially in some scenarios. Energy harvesting for BBN has been proposed in [10]–[13], which means that the node in WBAN can collect energy from sources related to body, like biochemical sources, thermal and vibration. But special hardware devices, known as energy harvesters and power management circuits have to be used for these energy harvesting schemes. Moreover, for BBN transmission, the data transmission inter-WBANs and routing results in further energy consumption. So energy saving is still needed for BBN data transmission. Several energy-efficient solutions have been proposed. An energy-efficient MAC protocol for medical emergency monitoring in BBN is proposed in [14]. Energy efficient routing algorithms in BBN are presented in [15]–[17]. Power optimization considering data rate is proposed in [18], and an adaptive power control algorithm is proposed in [19].

(2) Security: the data in BBN is private and critical, e.g., the body data is not allowed to be leaked, and the private information should avoid to be intercepted. Several security solutions for WBAN have been proposed. A solution to attain link layer encryption and authentication of the data in biomedical sensor networks is proposed [20]. Security suites are implemented under IEEE 802.15.6 which can be used for WBAN [20]. Secure medical information management system for WBAN is presented to guarantee the data confidentiality and integrity [21]. Wireless channel properties based secret key generated technique is proposed for WBAN [22]. An efficient and anonymous authentication scheme is proposed which can withstand the impersonation attack [23]. A secure and privacy-preserving body sensor data collection and query scheme using an improved homomorphic encryption technology is presented, which can resist various security threats from telemetry interface [24].

In consequence of the above two problems, the transmission system must be energy-efficient and secure in BBN, while most of the above previous works focus on only one of the problems. Compressive sensing can fulfill the energy-efficient task and also has a slight encryption performance [25], [26]. The design and implementation of CS based data acquisition and reconstruction for bio-signals are presented in [27]. A dynamic knob in CS is proposed to improve the adaptivity

towards bio-signal dynamics [28]. Low-complexity CS techniques based on matrix-inversion-free technique for monitoring electrocardiogram (ECG) signals are presented [29]. A multichannel CS scheme for biological signals to preserve the energy efficiency is proposed [30]. However, CS can not be satisfied with the network scale of BBN, because the number of nodes is very large, a node will have to preserve many measurement matrices as keys for different senders and also will have to preserve measurement matrices for different receivers, which will need a huge storage space. Fortunately, chaotic compressive sensing can solve this problem instead of the traditional compressive sensing, which only requires the sender and the receiver to preserve the matrix generation parameters including the chaotic parameter, initiation value, sampling initial position and distance as a key. This will save huge storage space. And because of the sensitivity of chaos, chaotic compressive sensing is more secure than the traditional compressive sensing in some extent.

In this paper, chaotic compressive sensing is proposed to be used in BBN to solve the huge storage space problem and fulfill the energy-efficiency and security simultaneously. The recovery performance of chaotic compressive sensing is analyzed with different SNR. Compared with the traditional Gaussian random matrix, the recovery performance of chaotic matrix is similar, the incoherence property is almost uniform, the compression ratio is approximate equal, but it only needs to store a few parameters, the storage space is saved. Benefiting from the sensitivity of chaos, the security performance including key space and key sensitivity is excellent. In addition, for the requirement of image transmission in BBN, a modified chaotic compressive sensing using two encryption mechanisms, confusion and mask, is proposed, which performs well in the aspects of gray histogram, adjacent pixel correlation and image entropy.

The rest of the paper is organized as follows. Section II describes the basics of chaotic compressive sensing briefly. The details of chaotic compressive sensing used in BBN and a modified method for image encryption transmission are introduced in Section III. Simulation experiments and performance evaluation are discussed in Section IV, and the last section concludes this paper.

II. Fundamental Knowledge

Chaotic Compressive Sensing is a kind of compressive sensing method which uses measurement matrices generated from chaotic sequences. In this section compressive sensing and chaos theory will be introduced respectively.

A. Compressive Sensing

Compressive sensing was proposed in [31], [32]. Suppose $x \in R^N$ is a discrete signal, projecting x by a $M \times N$ matrix Φ,

$$y = \Phi x \tag{1}$$

where $M < N$, $y \in R^M$, Φ is called the measurement matrix. x can not be solved from y directly because the number of equation is less than the number of unknowns ($M < N$). But if x is sparse or sparse on some orthogonal basis, that is

$$x = \Psi s \tag{2}$$

where Ψ is a $N \times N$ orthogonal matrix ($\Psi\Psi^T = I,\ \Psi^T\Psi = I$) called the sparsity matrix, and the sparsity means that K values of s are nonzero and the other $N - K$ values are zero, here $K \ll N$, x can be recovered from y under the condition that Φ satisfies the restricted isometry property (RIP) [31]. The Discrete Fourier transform (DFT) and Discrete Wavelet transform (DWT) matrices are often used as sparsity matrix. Based on (1) and (2),

$$y = \Phi x = \Phi\Psi s = \Theta s \tag{3}$$

though the number of equations is still less than the number of unknowns, resulting from s is sparse, s can be recovered by

$$\min_{\tilde{s}} \|\tilde{s}\|_{l_0} \quad \text{subject to} \quad y = \Theta\tilde{s}. \tag{4}$$

According to [33], the problem (4) can be transformed to a convex optimization problem,

$$\min_{\tilde{s}} \|\tilde{s}\|_{l_1} \quad \text{subject to} \quad y = \Theta\tilde{s} \tag{5}$$

which can be solved using the BP algorithm [34]. It only needs RIP to recover s. RIP is that

$$1 - \delta_k \le \frac{\|\Theta v\|_2}{\|v\|_2} \le 1 + \delta_k, \tag{6}$$

where $\delta_k \in (0, 1)$, v is an arbitrary sparsity signal. Based on this condition, it can get s and use equation (2) to recover x. In addition, greedy algorithms like MP, OMP, ROMP can also be used for compressive sensing to recover s. This kind of algorithm is faster than BP, but is less accurate. Based on compressive sensing, in BBN communication, the sender only needs to transmit y instead of x to the receiver, and the receiver can recover x from y. Because the amount of data transmitted are decreasing, it can save energy used for transmitting data [25].

Because both sender compressing and receiver recovery need a measurement matrix, it is significant for the performance of compressive sensing. Many works have studied the measurement matrix [35]–[38]. It must satisfy RIP, but the verification of RIP is difficult. In addition to RIP, spark is used to measure the performance of the measurement matrix [39]. The spark of a matrix is the smallest number of columns of this matrix that are linearly dependent. If and only if $spark(\Theta) > 2K$, there exists at most one K-sparsity signal s such that $y = \Theta s$ [39]. But the computation of spark is also an NP-hard problem. So incoherence, the equivalent condition of RIP, is used. If the measurement matrix Φ is incoherent with Ψ, then the RIP is satisfied. In [40], the mutual coherence coefficient of Θ can be used to analyze the coherence quantitatively. The mutual coherence coefficient is defined as

$$\mu(\Theta) = \max_{1 \le i \ne j \le N} \frac{|\langle \theta_i, \theta_j \rangle|}{\|\theta_i\|_2 \|\theta_j\|_2}, \tag{7}$$

where θ_i denotes the ith column of Θ. For any vector y, if $\mu(\Theta) < 1/(2K - 1)$, there exists at most one K-sparsity signal s such that $y = \Theta s$ [41]. Gaussian random matrix has good

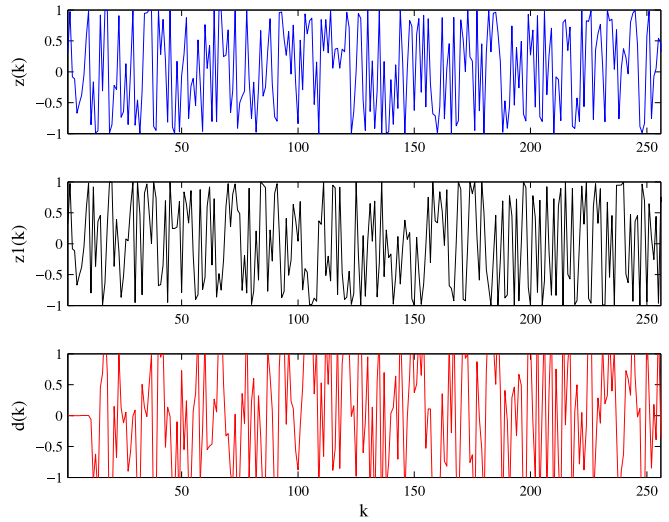


Fig. 3. Chebyshev sequence. The initiation value of $z(k)$ is 0.32, the initiation value of $z1(k)$ is 0.32000000000001, the chaotic parameter of $z(k)$ is 20, the chaotic parameter of $z1(k)$ is also 20. the length of chaos sequences is 256. $d(k)$ is the difference between $z(k)$ and $z1(k)$.

incoherence property with all sparse matrices, so it has been used as the measurement matrix frequently [42].

B. Chaos Theory

Chaos is a kind of complex dynamical behavior with special properties. A chaotic sequence is pseudorandom and finite, which is suitable for constructing the measurement matrix [43]. Chaotic system can generate measurement matrices by the deterministic method which means a sequence can be generated by a deterministic system while this sequence is pseudorandom meeting the condition of the measurement matrix. So it can simplify the constructing process of the measurement matrix. For example, the following is a Chebyshev chaotic system [44]

$$z_{k+1} = \cos(w \arccos z_k), \tag{8}$$

where $w \geq 2$, $z_k \in [-1, 1]$. For a given parameter w and initiation value z_0, based on (8), the sequence z_k, $k = 1, 2, 3...$, can be generated. Using this sequence, sampled sequence can be obtained by the sampling distance d and the sampling initial position n_0

$$x_n = z_{n_0+dn}. \tag{9}$$

Mapping this sequence to a matrix by some map function, this matrix can be used as the measurement matrix.

There is an important property in chaotic system, it is the sensitivity of the initial value and the chaotic parameter. It means that a tiny perturbation of the initial value or system parameter can result in a new sequence which is quite different from the original one. For instance, in equation (8), fixing w, if we perturb z_0 with a tiny value, that is, the first sequence is generated from $z_0 = 0.32$, the second is generated from $z_0 = 0.32000000000001$, the third signal $d(k)$ represents the difference of these two sequences. As shown in Fig. 3, the first two sequences are quite different from each other after $k > 10$. This sensitivity is very suitable for encryption [45], the sequence can be used as a secret key to encrypt the plain text. A tiny perturbation will generate another key, which can not decrypt the ciphertext encrypted by the original key.

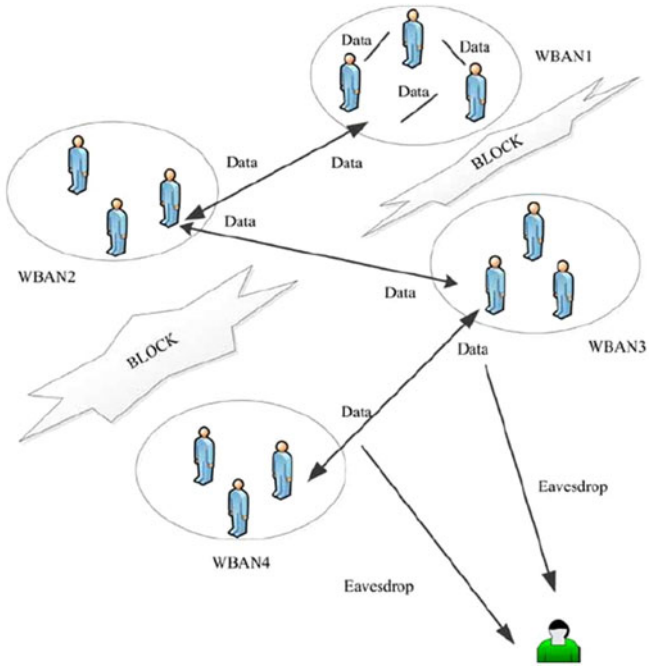


Fig. 4. BBN communication links. Some WBANs can not communicate with each other directly because of blocks, and they have to rely on relay nodes. So the transmission distance is extended, and the data are needed to be encrypted to prevent information being leaked to the unfaithful relay nodes and the eavesdroppers.

Beside Chebyshev, there are many other chaotic systems which are easy to be calculated and used [46], like the Logistic map $z_{k+1} = \mu z_k(1 - z_k)$, $\mu \in (0, 4]$, or the Tent map, $z_{k+1} = z_k/b, 0 < z_k < b, z_{k+1} = (1 - z_k)/(1 - b), b < z_k < 1$, where $0 < b < 1$. These systems can generate chaotic sequences which can be used for constructing measurement matrices.

III. Chaotic Compressive Sensing Applied in BBN

In this section, the details of our method, chaotic compressive sensing applied for BBN, are introduced, which include energy-efficiency, security and image encryption. Firstly, the traditional idea for secure and energy-efficient transmission is introduced, then the CCS method, and finally, the CCS image encryption.

A. Traditional Transmission Method

The difference between BBN and WBAN is the communication link. The links in BBN are very complex, and numerous nodes need to communicate with each other. As shown in Fig. 4, nodes not only need to send or receive data inside the WBAN, but also need to communicate with nodes in other WBANs, which will result in the transmission distance extended. The extended transmission distance needs more transmission energy. More frequently, one node can not send data to another node directly, and it needs other nodes to relay its data. For example, in Fig. 4, resulting from the electromagnetic environment

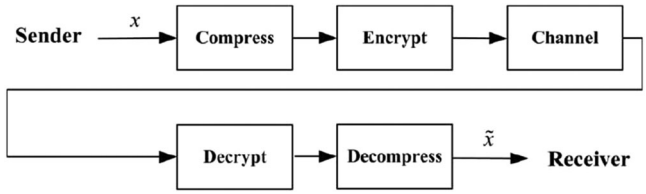


Fig. 5. The traditional method for encryption and compression data transmission needs two steps. The sender compresses the data and then encrypts the compressed data. The receiver decompresses the received data through the channel and then decrypts the decompressed data.

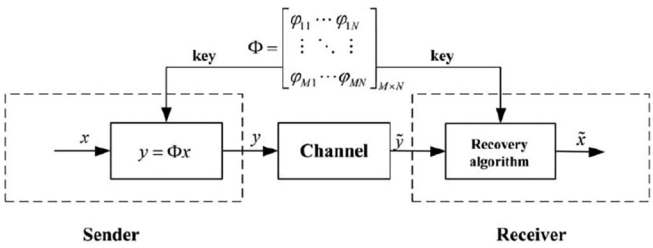


Fig. 6. Compressive sensing based energy-efficient and encryption transmission. Compressive sensing can fulfill the compression and encryption simultaneously. The amount of transmitted data can be decreased, which can save transmission energy fundamentally. And the measurement Φ can transform plain data x to cypher data y. The receiver can recover the original data by one step using recovery algorithms like OMP, ROMP, etc.

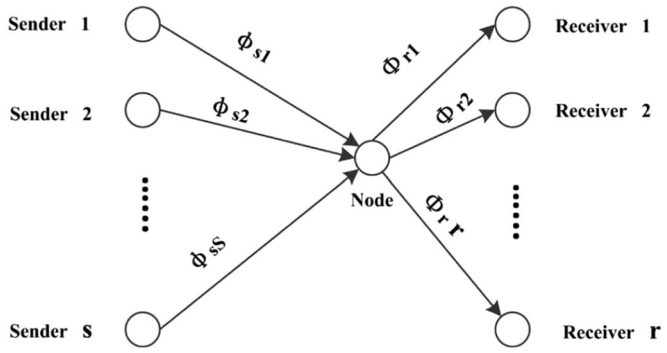


Fig. 7. The number of the matrices. Using the traditional compressive sensing, a node need to store many matrices for different nodes in BBN. For different users, the node should keep different matrices, the number of the matrices is extremely increased with the communication users increasing.

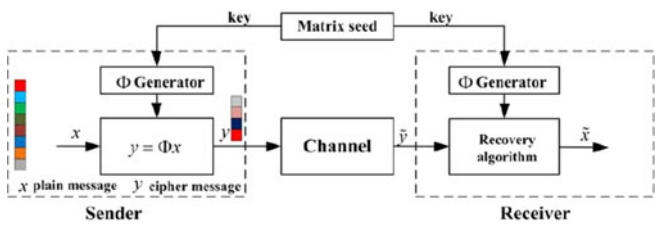


Fig. 8. Chaotic compressive sensing encryption and compression scheme. x denotes the plain message, and y denotes the cipher message. Different colors denote different data, and y is encrypted and compressed simultaneously by Φ, which is generated by the chaotic matrix generator with the matrix seed.

or the network topography, the node in WBAN 1 has to rely on WBAN 2 when sending data to WBAN 3, and WBAN 3 is needed when WBAN 2 wants to transmit data to WBAN 4, which also needs more energy. If some relay nodes are powered off, other nodes will be affected, even the whole network is down. On the other hand, data transmitted in BBN is private content concerning the body. Because the links in BBN are open, which are easy to be eavesdropped as shown in Fig. 4, the data needs to be encrypted. Therefore, the transmission needs to solve the problems of energy-efficiency and security simultaneously.

As shown in Fig. 5, the traditional idea is compressing and encrypting data x before transmission at the sender, after receiving the data through the channel, then decrypting and decompressing at the receiver. However, this method has to be processed in two steps, i.e. compression and encryption. Compressive sensing can fulfill energy-efficiency and security in one step. In Fig. 6, the measurement matrix Φ can compress the data because of $\Phi \in R^{M\times N}$, the dimension of y is smaller than that of x, $(M \ll N)$, and the sending data decreases, which will decrease the energy fundamentally [25]. Meanwhile, resulting from the randomness of Φ, y is quite different from x, so Φ can encrypt x. At the receiver, recovery algorithms such as BP, OMP, ROMP, can be used to recover x in one step. However, the measurement matrix is used as a secret key in this method. For each transmission pair, a measurement matrix has to be kept, and every matrix has MN elements. With the increment of the number of the communication nodes, each node has to keep a massive number of measurement matrices as secret keys.

B. Chaotic Compressive Sensing Method

Compressive sensing can fulfill energy-efficiency and security simultaneously [25], but it is not sufficient in BBN. Nodes in BBN need to communicate with other even remote nodes by relay nodes because of the limited device transmitting distance. Sometimes communication with nearby nodes also needs relay nodes resulting from the environment and topography. So there are numerous relay nodes in BBN, but the sender only wants the receiver to decrypt the message, and it does not want the relay node to decrypt the message. Each sender-receiver pair shares one measurement matrix, which will prevent the message from being leaked to relay nodes. However, this will lead to another problem. For example, for the node in Fig. 7, there are s users to send data to the node, and the node needs to send data to r users. So the node has to keep $s + r - c$ matrices $\Phi_{M\times N}$, where c is the number of users which communicate with this node in a two-way mode. Hence, $(s + r - c)\,MN$ matrix elements have to be kept for the node in Fig. 7. With the extension of the network, the node needs to keep more matrices, which will need more space for storing these matrices.

Chaotic compressive sensing can be used to solve the above problem. As shown in Fig. 8, the matrix seed is the chaotic matrix generation parameter, and the sender and the receiver only need to store the matrix seed rather than the whole measurement matrix, which can save considerable storage space. The matrix seed includes four parts, the initiation value, the chaotic parameter, the sampling initiation position, and the sampling distance.

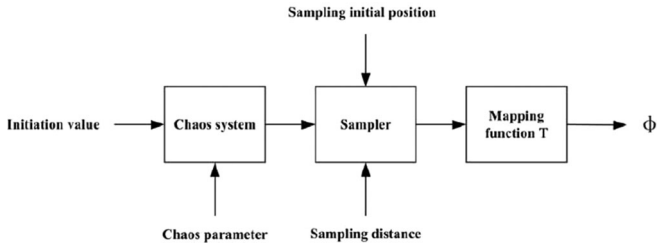


Fig. 9. Chaotic matrix generator. This generator consists three parts, chaotic system, sampler and mapping function. The user only needs to keep the matrix seed including initiation value, chaos parameter, sampling initial position and sampling distance rather than the whole measurement matrix.

The Φ generator is introduced in Fig. 9, and the matrix Φ can be generated in a deterministic way rather than a stochastic one. Only the initiation value and the chaotic parameter are needed for the chaotic system (Chebyshev, Logistic, Tent and so on) to generate a chaotic sequence. Then input the sequence to the sampler with two parameters, the sampling initiation position and the sampling distance, and a sampled sequence is obtained. The third step is to use a function to map a sequence to a matrix, which is the measurement matrix. As shown in the following

$$\Phi = T(S(n_0, d, C(z_0, \varepsilon))), \tag{10}$$

where z_0 is the initiation value, ε is the chaotic parameter, C denotes the chaotic system, n_0 is the sampling initial position, d is the sampling distance, S denotes the sampler, and T denotes the mapping function. Saving space is one advantage of chaotic compressive sensing, and there is another advantage, i.e. security. In a BBN, the enemy or competitor may get some parameters by some method, but if not all of the above parameters are obtained, the message can not be decrypted. Moreover, resulting from the sensitivity of the chaotic system, a tiny perturbation for the chaotic parameter or the initial value will generate a quite different sequence, with a perturbed parameter to recover x, and the message also can not be decrypted.

C. Image Compressive Encryption

Image transmission is required in some BBN scenarios such as military, health care, disaster relief. So chaotic compressive sensing is required to encrypt an image. Different from a text message, the image has its own characteristics like adjacent pixels correlation. Hence, chaotic compressive sensing has to be adjusted to satisfy image encryption. In order to make the encrypted image having a random-like distribution of gray values, and adjacent pixels having zero-correlation property, the following modification is processed

$$Y = \alpha\Phi_1 X + \beta\Phi_2, \tag{11}$$

where X is the original $N \times N$ image, Φ_1, Φ_2 are both $M \times N$ chaotic compressive matrices, Φ_1 is the measurement matrix, and Φ_2 is the mask matrix, Y is the $M \times N$ encrypted image, α, β are adjustment parameters. The use of Φ_1, Φ_2, α, β can make Y meet the image encryption requirement, meanwhile, the data amount of Y is M/N of that of X, the decrement of data transmission can save the energy. This is our proposed image compressive encryption method.

In this method, two encryption mechanisms are used. First, use Φ_1 to confuse the image X; second, use Φ_2 to mask the image. By adjusting the parameters α, β, the distribution of each gray value can reach approximately an uniform state. Compared with the traditional chaotic compressive sensing encryption, we use two chaotic matrices to enhance image encryption security. In fact, our method includes the traditional method, i.e. when $\alpha = 1, \beta = 0$, it degenerates to the traditional method. The traditional method only uses a matrix to multiple the original image X, provided no other encryption methods like permutation or diffusion. The encryption performance of the traditional method is not very good. The adjacent pixel correlation is high, and the gray values are concentrated on some interval, which can be seen in the next section. If using this traditional method, other encryption methods should be used before or after CS, which transforms two steps described in Fig. 5.

At the receiver, based on equation (11), we get

$$\frac{Y - \beta\Phi_2}{\alpha} = \Phi_1 X. \tag{12}$$

Note $\frac{Y-\beta\Phi_2}{\alpha}$ as Y', namely $Y' = \Phi_1 X$. Then X can be solved using a compressive sensing recovery algorithm like OMP. Since image X is sparse in the wavelet domain, suppose W is the DWT matrix ($WW^T = I$, $W^T W = I$), and

$$X = W^T S W, \tag{13}$$

where S is sparse. Because an image processed by DWT, a series of sub-images of different frequency are obtained. The points of sub-image with high frequency are close to zero. For an image, the main energy is concentrated on the low frequency. The low frequency part is on the top left corner of S. And other elements of S are close to zero. For the columns from the right part of S, the elements are close to zeros. For the columns from the left part of S, only the top elements are not close to zero. So each column of S can be regarded as sparse. Based on $Y' = \Phi_1 X$ and equation (13), we get

$$Y'W^T = \Phi_1 W^T S. \tag{14}$$

Using $Y'W^T$ and $\Phi_1 W^T$, S can be solved by the OMP algorithm, and X can be recovered using equation (13).

IV. Simulation and Evaluation

In this section, the feasibility and the security of chaotic compressive sensing are evaluated by simulations. A frequency domain sparsity signal and an image lena is used in the experiment. The frequency domain sparsity signal is generated by Matlab, the image lena is widely used in previous works [47], [48]. Three chaotic maps, i.e. Chebyshev, Logistic, Tent, are used to generate measurement matrices, which are compared with the Gaussian random matrix. In the first subsection, the feasibility is verified, the security is analyzed in the next subsection, the last subsection gives the results of the image encryption and analyzes the performance.

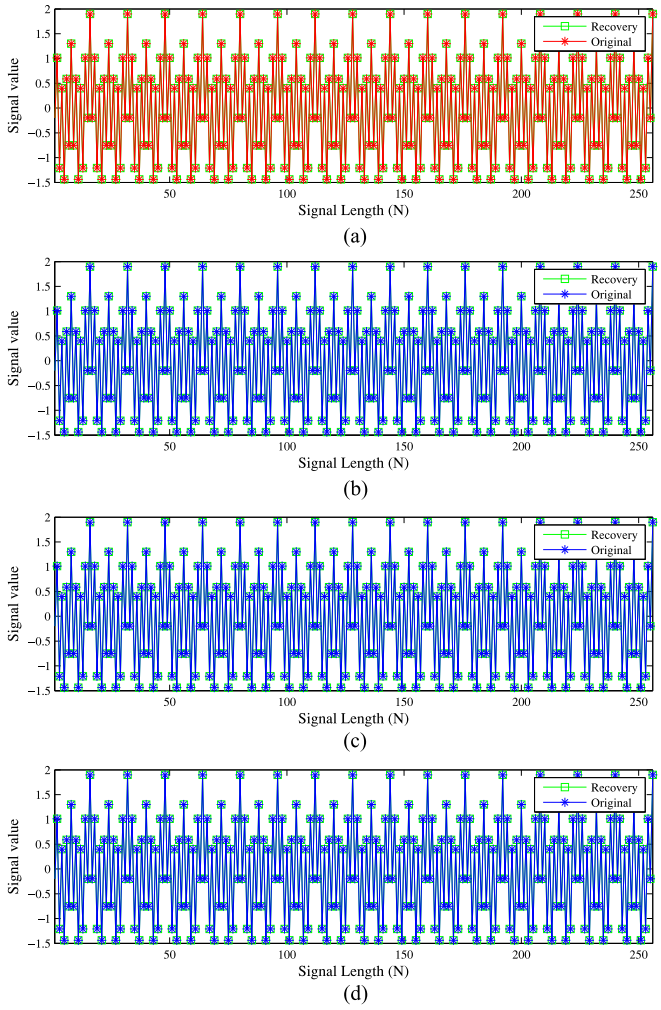


Fig. 10. Recovery results without noise. (a) is the recovery result using the Gaussian matrix. (b) is the recovery result using the Chebyshev matrix. (c) is the recovery result using the Logistic matrix. (d) is the recovery result using the Tent matrix.

A. *Feasibility of CCS*

Feasibility verification includes the recovery error, the incoherence of the measurement matrix and the sparsity matrix, and the compressive ratio. The experiment results of these aspects were analyzed one by one. In this experiment, the signal length N is 256, the sparsity K is 7, and the recovery algorithm is OMP. The size of all of the four measurement matrices are 64×256. The Gaussian matrix are generated randomly. The Chebyshev matrix is generated by the Chebyshev system. The initial value is 0.32, the chaotic parameter is 20. The sampling initial position is 1, the sampling distance is 4. The Logistic matrix is generated by Logisitc system. The initial value is 0.32, the chaotic parameter is 4. The sampling parameters are the same as those of the Chebyshev matrix. The Tent matrix is generated by Tent system. The initial value is 0.32, the chaotic parameter is 0.3. The sampling parameters are the same as those of the Chebyshev matrix. Fig. 10 shows the recovery results in the noise free case, from which we can see the performances of three chaotic matrices are similar to the performance of the Gaussian

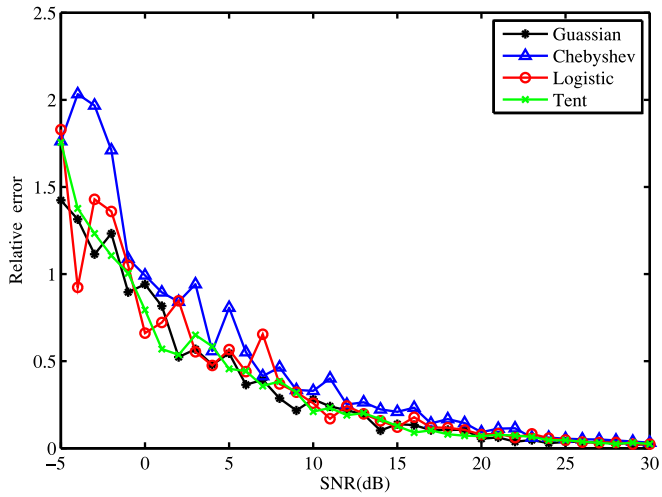


Fig. 11. Recovery performance with noise. The recovery performance is measured by the relative error. The measurement matrices are the Gaussian matrix, the Chebyshev matrix, the Logistic matrix and the Tent matrix. The SNR is from -5 to 30 dB.

matrix. To evaluate the recovery performance, we use the relative error

$$\delta = \frac{\|\hat{x} - x\|_2}{\|x\|_2}, \tag{15}$$

where x is the original signal, which is the frequency domain sparsity signal in this experiment, $\hat{x}$ is the recovery signal, and $\|\bullet\|_2$ denotes the l_2 norm of a vector. In Fig. 10, the relative error of the Gaussian matrix is 4.44×10^{-15}, the relative error of the Chebyshev matrix is 3.84×10^{-15}, the relative error of the Logistic matrix is 4.01×10^{-15}, and the relative error of the Tent matrix 3.63×10^{-15}, which indicates that the recovery result is extremely accurate without noise.

Fig. 11 shows the recovery performance with different signal to noise ratio (SNR) by using the above three chaotic matrices and the Gaussian matrix. The noise is the additive white Gaussian noise (AWGN), and the scale of SNR is from -5 dB to 30 dB. At -5 dB, $\delta > 1$ for all the four matrices. But it decreases with the increment of SNR. From -5 dB to 10 dB, relative errors are greater than 0.25, after 10 dB, errors of the three chaotic matrices and the Gaussian matrix tend to be the same, and when SNR is greater than 25 dB, all errors tend to be zero. It implies that the recovery performance of the chaotic matrix is similar to that of the Gaussian matrix with noise.

In the next part, the incoherence of the measurement matrix and the sparsity matrix (DFT matrix, DWT matrix) is measured by the mutual correlation coefficient (MCC) of Θ, $\Theta = \Phi\Psi$. The smaller the MCC is, the better the performance of measurement matrix is. The measurement matrices are the above four matrices. In Fig. 12, Ψ is DFT matrix, in Fig. 13, Ψ is the DWT matrix, Fig. 14 shows the relationship between the chaotic parameter and MCC. Figs. 12 and 13 show the histograms of the correlation coefficient (CC) of all two columns in Θ, MCC is the maximum of all the correlation coefficient (CC). From Fig. 12, CCs of the chaotic matrices are concentrated on the

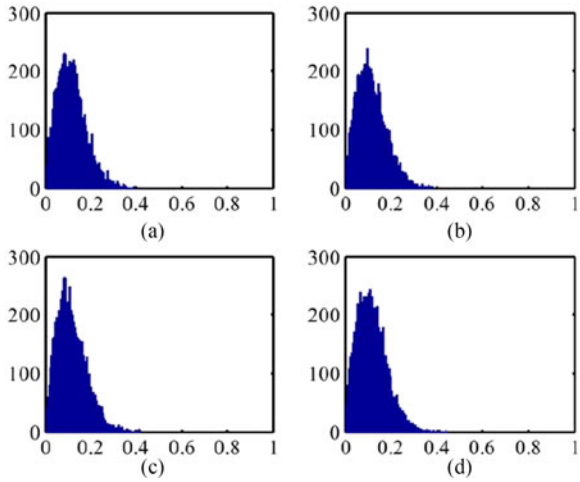


Fig. 12. Histograms of coherence coefficient of columns from Θ, the sparsity matrix is DFT matrix. (a) The measurement matrix is the Gaussian matrix. (b) The measurement matrix is the Chebyshev matrix. (c) The measurement matrix is the Logistic matrix. (d) The measurement matrix is the Tent matrix.

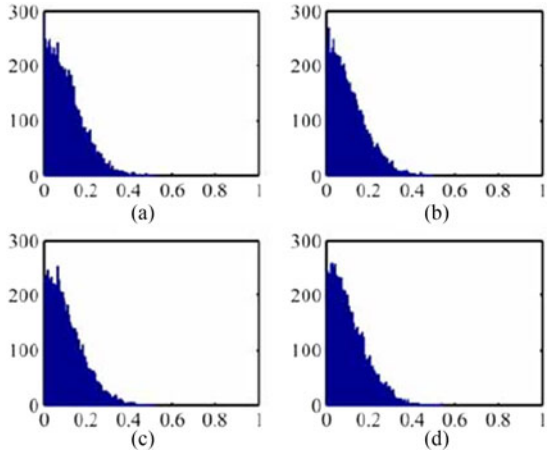


Fig. 13. Histograms of coherence coefficient of columns of Θ. the sparsity matrix is DWT matrix. (a) The measurement matrix is the Gaussian matrix. (b) The measurement matrix is the Chebyshev matrix. (c) The measurement matrix is the Logistic matrix. (d) The measurement matrix is the Tent matrix.

interval $(0, 0.2)$, which are similar to the Gaussian matrix. MCC of Chebyshev is 0.3815, smaller than MCC of Gaussian 0.4018, Logistic MCC is 0.4118, and Tent MCC is 0.4417. Similarly, compared with the sparsity matrix DFT in Fig. 12, seen from Fig. 13, CCs are concentrated on $(0, 0.2)$, nearer to 0. MCC of Chebyshev is 0.4917, Logistic is 0.5115, smaller than Gaussian 0.5322, Tent is 0.5415.

Fig. 14 shows the relationship between the chaotic parameter and MCC. In Fig. 14(a), when $\varepsilon < 1.5$, MCC is large, after $\varepsilon > 2$, MCC tends to be stable, about at 0.4 (DFT), 0.5 (DWT). This stable interval is the same as the interval in which the system is chaotic, so only if the parameters are set in this interval, the incoherence condition of compressive sensing is satisfied. Similarly, Logistic in Fig. 14(b) and Tent in Fig. 14(c) have the same property. In Fig. 14(b), the stable interval is (3.9, 4], in Fig. 14(c) the stable interval is [0.2, 0.8].

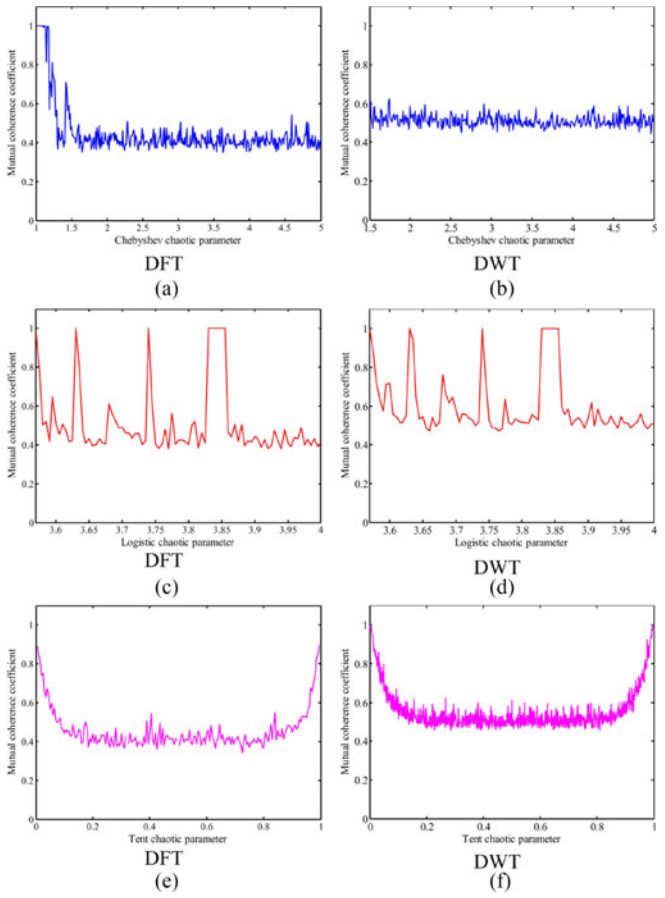


Fig. 14. Relationship between MCC and chaotic parameter of three kinds of chaotic matrices. DFT matrix is left part of this figure, DWT right. The initiation value is 0.32 in all of this experiment. (a) The measurement matrix is Chebyshev, the chaotic parameter of Chebyshev is tested from 1 to 5. (b) The measurement matrix is Logistic, the chaotic parameter of Logistic is tested from 0 to 4. (c) The measurement matrix is Tent, the chaotic parameter of Tent is tested from 0 to 1.

The feasibility of the measurement matrix can also be measured by the compression ratio, that is M/N. The compression ratio can also measure how much energy can be saved in BBN data transmission. The data amount of the encrypted signal is M/N of that of the original signal. Figs. 15 and 16 show the recovery performance with different M/N. In Fig. 15, the original signal is still the above frequency sparse signal with the length $N = 256$, and the length of the encrypted signal is M, the range of M is from 30 to 100. The length of the encrypted signal is equal to the row number of the measurement matrix. From Fig. 15, after $M = 46$ the error of Gaussian tends to be zero. After $M = 49$ the error of Chebyshev tends to be zero, after $M = 51$, the error of Logistic tends to be zero, after $M = 45$, the error of Tent tends to be zero. Because $N = 256$, the compression ratios of precise recovery of the Gaussian matrix, the Chebyshev matrix, the Logistic matrix, Tent matrix are 0.18, 0.19, 0.20, 0.17. The sender only needs about M/N of original transmission energy without considering other factors.

In Fig. 16, the original image is the image lena, and peak signal to noise ratio (PSNR) is used to measure image recovery performance, which is a metric widely used in image

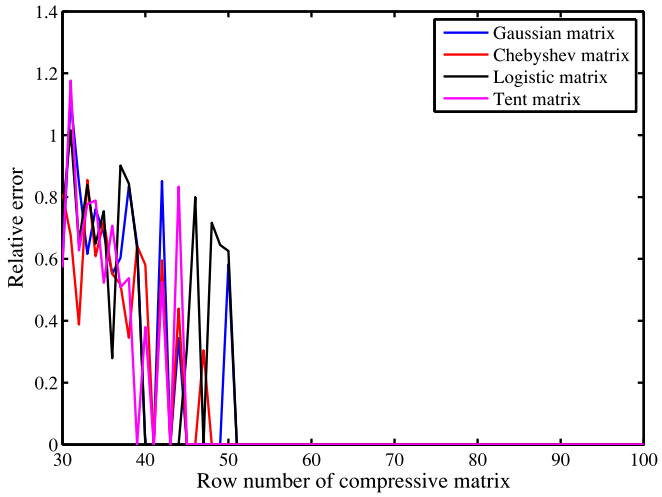


Fig. 15. Compression ratio of the frequency sparse signal. The compressed signal is the frequency domain sparsity signal, the length of the signal is 256, and the performance of recovery is measured by the relative error. The row number of the measurement matrix is tested from 30 to 100. The column number of the measurement matrix is equal to the signal length 256. The measurement matrices are the Gaussian matrix, the Chebyshev matrix, the Logistic matrix, and the Tent matrix.

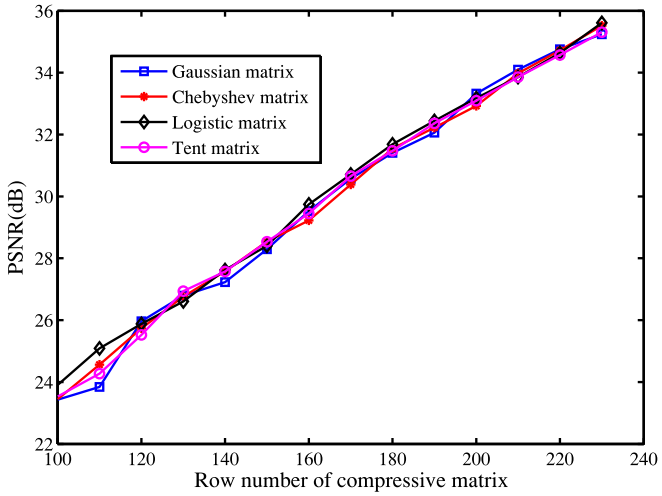


Fig. 16. Compression ratio of the image. The compressed signal is the image lena with the size of 256×256, and the performance of recovery is measured by PSNR. The measurement matrices are the Gaussian matrix, the Chebyshev matrix, the Logistic matrix, and the Tent matrix.

compression and compressive sensing [47], [49], [50]. The definition of PSNR is as follows,

$$\text{PSNR} = 10 \lg \left[\frac{M_1 \times N_1 \times 255^2}{\sum_{i=0}^{M_1-1} \sum_{j=0}^{N_1-1} (P(i,j) - D(i,j))^2} \right] \quad (16)$$

where M_1, N_1 denote the image width and height, respectively, $P(i,j)$ is the gray value of the original image, and $D(i,j)$ is the gray value of the recovered image. The mean square error (MSE) of the image recovery is defined as

$$\text{MSE} = \frac{1}{M_1 \times N_1} \sum_{i=0}^{M_1-1} \sum_{j=0}^{N_1-1} (P(i,j) - D(i,j))^2. \quad (17)$$

So the relationship of PSNR and MSE is

$$\text{PSNR} = 10 \lg \frac{255^2}{\text{MSE}}. \quad (18)$$

If the MSE of the image recovery approaches zero, the PSNR value approaches infinity. So the greater PSNR of the recovery image is, the more accurate the recovery is. A small value of the PSNR implies high numerical differences between the original image and the recovered image. As shown in Fig. 16, recovery performance of four matrices is similar. When $M = 100$, PSNR is about 24 dB for all matrices. After $M \geq 170$, PSNR is larger than 30 dB. In this experiment, the image size is 256×256, and the compression ratio is 0.66 when $M = 170$. The sender can adjust the compression ratio for different PSNR requirement to save transmission energy, which is a tradeoff between recovery accuracy and energy saving.

B. Security Analysis of CCS

The key space and the key sensitivity will be analyzed in this part. Based on equation (10), the key is determined by the parameters z_0, ε, n_0, d and the mapping function T. If z_0 is composed of K_1 decimal numbers, ε consists of K_2 decimal numbers, the range of n_0 is $[1, K_3]$, the range of d is $[1, K_4]$, and there are K_5 kinds of mapping functions, then the key space,

$$S = 10^{(K_1+K_2)} \times K_3 \times K_4 \times K_5. \quad (19)$$

Theoretically, K_3, K_4 can take any large value, and the key space will become infinite. However, resulting from the limited processing capacity of the equipment in BBN, K_3, K_4 can not be too large. By simulation calculation, for Chebyshev, if $n_0 < 10^{-16}$ or $\varepsilon < 10^{-17}$, two Chebyshev sequences can not be distinguished. So The maximum of K_1 of Chebyshev is 16, the maximum of K_2 of Chebyshev is 17. Similarly, the maximum of K_1 of Logistic is 16, the maximum of K_2 of Logistic is 15, the maximum of K_1 of Tent is 15, the maximum of K_2 of Tent is 16 by simulation calculation. Supposed that K_3, K_4, K_5 are 100, 10, 10, respectively, the key space of CCS with Chebyshev is 10^{37}, the key space of CCS with Logistic 10^{35}, and the key space of CCS with Tent is 10^{35}.

If the key space is needed to be extended in some scenarios which need more secure transmission, then the multi-dimensional chaotic system can be used. The multi-dimension chaotic system has multiple parameters, so the key space can be extended. Take Henon chaotic system for instance [51]. There are two parameters a, b, and the initiation value is (x_0, y_0), if the number of parameters increases, then the key space is extended. The Henon system is as follows,

$$\begin{cases} x_{n+1} = 1 + y_n - a x_n^2 \\ y_{n+1} = b x_n \end{cases} \quad (20)$$

It needs to compute two sequences, the one-dimensional chaotic system needs to compute one sequence. For

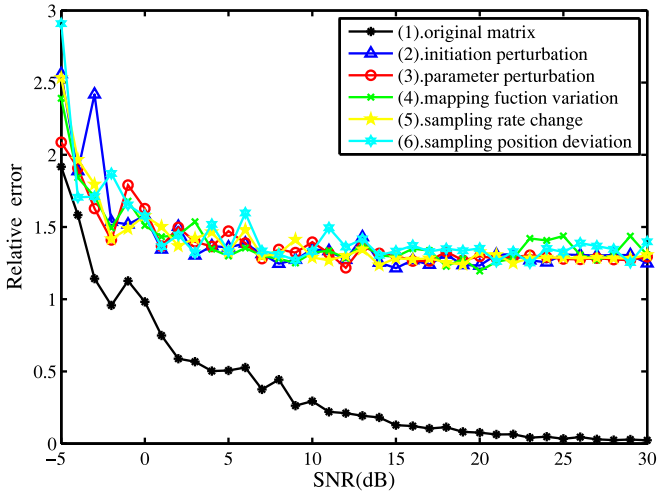


Fig. 17. Key sensitivity of CCS with the Chebyshev chaotic system. Five kinds of perturbation matrices are compared with the original matrix. The performances are measured by the relative error with different SNR. Curve (1) denotes the result of the original encrypted matrix. Curves (2)–(6) denote the results of the five kinds of perturbation matrices.

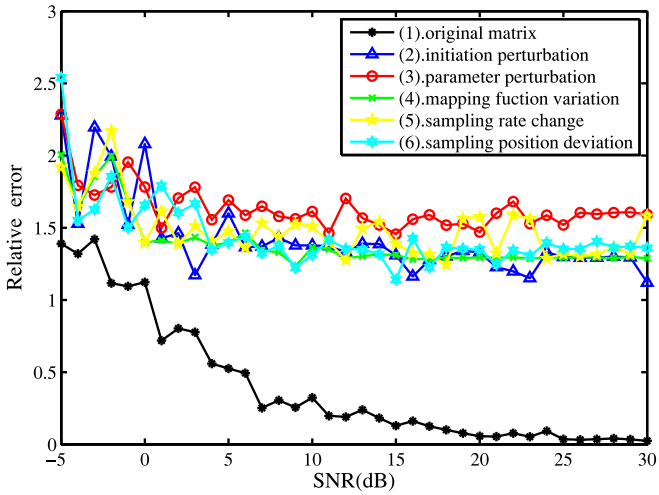


Fig. 18. Key sensitivity of CCS with the Logistic chaotic system. Five kinds of perturbation matrices are compared with the original matrix. The performances are measured by the relative error with different SNR. Curve (1) denotes the result of the original encrypted matrix. Curves (2)–(6) denote the results of the five kinds of perturbation matrices.

one-dimensional system such as Logistic, it needs to compute n time to obtain a sequence with length n, so the time complexity is $O(n)$. For the two dimensional chaotic system, it needs to compute $2n$ time to obtain two sequences with length n, so the time complexity is $2O(n)$, that is also $O(n)$.

Figs. 17–19 show the sensitivity of the key. In this experiment, the sender uses matrix generation parameters as a secret key to encrypt data, and the receiver uses a perturbation matrix to decrypt the received data. In these three figures, the original matrix denotes the matrix used by the sender, then we change one parameter with a tiny value of the parameters used for chaotic matrix generator to generate another matrix, which is called the perturbation matrix. Initiation perturbation matrix denotes

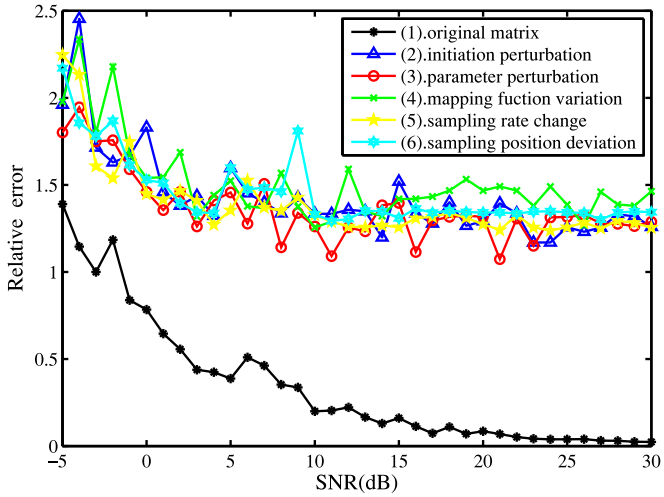


Fig. 19. Key sensitivity of CCS with the Tent chaotic system. Five kinds of perturbation matrices are compared with the original matrix. The performance is measured by the relative error with different SNR. Curve (1) denotes the result of the original encrypted matrix. Curves (2)–(6) denote the results of the five kinds of perturbation matrices.

the matrix generated by perturbing initiation with a tiny value, parameter perturbation matrix denotes the matrix generated by perturbing the chaotic parameter with a tiny value, and then mapping function variation matrix denotes the matrix generated by using another mapping function from sequence to matrix. The last two matrices denote the matrices which are generated by changing the sampling distance and sampling initial position. The SNR range is from -5 dB to 30 dB. The perturbation of the initiation for all three kinds of chaotic matrix is 10^{-14}. the perturbation of the chaotic parameter for Chebyshev is 10^{-12}, the perturbation of the chaotic parameter for Logistic is 10^{-12}, the perturbation of the chaotic parameter for Tent is 10^{-14}. The mapping function variation is from column by column to row by row. Column by column means the matrix are generated by columns from the chaos sequence. Row by Row means the matrix are generated by rows from the chaos sequence. The perturbation of the sampling initial position for all three kinds of matrices is 20, the perturbation of the sampling distance for all three kinds of matrices is 1. These perturbation matrices are used at receiver, and the relative error of Chebyshev matrix with different SNR is in Fig. 17, the relative error of Logistic matrix with different SNR is in Fig. 18, the relative error of the Tent matrix with different SNR is in Fig. 19. As shown in these figures, using the original matrix to decrypt the cipher data, when SNR is larger than 15 dB, the error decreases to 20%, and when SNR is 30 dB, the error tends to be zero. However, using these five kinds of perturbation matrices, even at high SNR, 30 dB, the error is still about 100%. These experimental results show that, a tiny error of the matrix generation parameter will result in a high error decoding, and the key is sensitive, which can prevent the eavesdropper from decoding the message by using a key similar to the encryption key to decrypt the data transmitted.

The security of CCS depends on the sensitivity of the initiation and the parameter, so we need to quantify the sensitivity

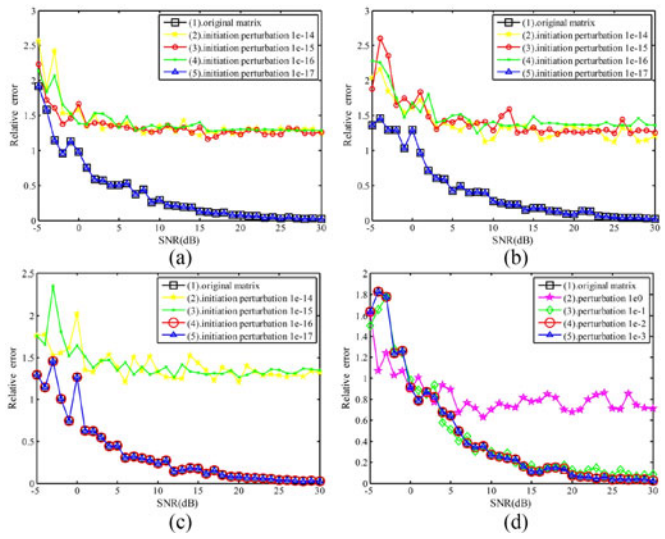


Fig. 20. Relative error of tiny initiation value perturbation matrices. Orders of magnitude of initiation value for chaotic matrices are 10^{-14}, 10^{-15}, 10^{-16}, and 10^{-17}. (a) The recovery results of the Chebyshev matrix with the initiation perturbation. (b) The recovery results of the Logistic matrix with the initiation perturbation. (c) The recovery results of the Tent matrix with the initiation perturbation. (d) The recovery results of the Gaussian matrix with changed elements, Orders of magnitude of elements changed is 10^{0}, 10^{-1}, 10^{-2}, 10^{-3}.

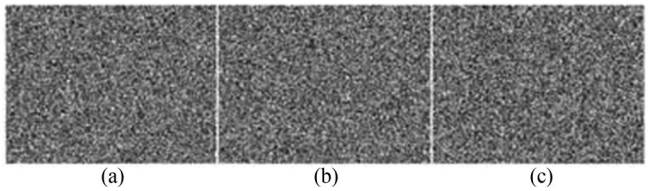


Fig. 21. Encrypted images with chaotic matrices. (a) The measurement matrix Φ_1 is the Chebyshev matrix, the mask matrix Φ_2 is the Tent matrix. (b) The measurement matrix Φ_1 is the Logistic matrix, the mask matrix Φ_2 is the Tent matrix. (c) The measurement matrix Φ_1 is the Tent matrix, the mask matrix Φ_2 is another Tent matrix.

Fig. 22. Recovery images with correct decrypted matrices. (a) The original image. (b) Recovery image using the correct Chebyshev matrix and the correct mask matrix, (c). Recovery image using the correct Logistic matrix and the correct mask matrix. (d) Recovery image using the correct Tent matrix and the correct mask matrix.

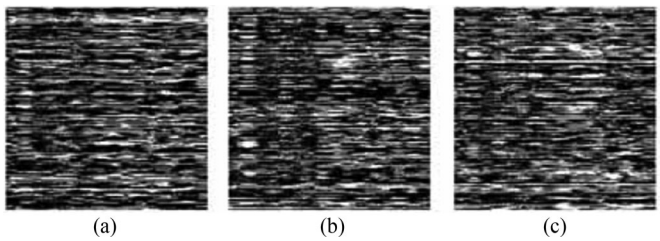


Fig. 23. Recovery images using measurement matrices with initiation value perturbation. (a) Φ_1 is the Chebyshev matrix with 10^{-15} perturbation, (b) Φ_1 is the Logistic matrix with 10^{-15} perturbation, (c) Φ_1 is the Tent matrix with 10^{-15} perturbation. The 10^{-15} perturbation of the measurement matrix can lead to the failure of decryption.

when designing the encryption key. Fig. 20 shows the quantization result. The initiation perturbation values are 10^{-14}, 10^{-15}, 10^{-16}, and 10^{-17}. Decrypt the cipher data with original matrix and perturbation matrices, The recovery results of Chebyshev is in Fig. 20(a), Logistic in Fig. 20(b), Tent in Fig. 20(c). In Fig. 20(a), from 10 dB to 30 dB, the errors of the perturbation matrix 10^{-14}, 10^{-15}, 10^{-16} are from 100% to 150%, the error curve of 10^{-17} coincides with the error curve of the original matrix, which implies that if the perturbation of intercepted initiation is larger than 10^{-16}, the eavesdropper can not decrypt the intercepted data. Similarly, Fig. 20(b) and (c) show the results of Logistic, Tent. In Fig. 20(b), error curves of the Logistic are similar to those of Chebyshev. In Fig. 20(c), the errors of the perturbation matrix 10^{-14}, 10^{-15} are larger than 100%, curves of 10^{-16}, 10^{-17} coincide with the error curve of the original matrix. For comparison, the result of the Gaussian matrix is shown in Fig. 20(d), error curves of smaller than 0.1 approximately coincide the error of original matrix, which shows if the Gaussian matrix is used as the key, it is easy for the eavesdropper to decrypt the data by using an intercepted approximate key.

C. Image Encryption Result and Analysis

In this part, the image encryption results are shown, and the security of the proposed method is analyzed by image histograms, adjacent pixels correlation and image entropy. The plain image is an image of lena by 256×256, and the gray value is from 0 to 255. The sizes of all of the encrypted matrices are 190×256. Fig. 21 shows the encrypted images. In Fig. 21(a), Φ_1 is a Chebyshev matrix, the initiation value is 0.32, the chaotic parameter is 20, the sampling initial position is 1, the sampling distance is 4, Φ_2 is a Tent matrix, the initiation value is 0.32, the chaotic parameter is 0.4, the sampling initial position is 1, the sampling distance is 4. In Fig. 21(b), Φ_1 is a Logistic matrix, the initiation value is 0.32, the chaotic parameter is 4, the sampling initial position is 1, the sampling distance is 4; Φ_2 is a Tent matrix, the initiation value is 0.32, the chaotic parameter is 0.44, the sampling initial position is 1, the sampling distance is 4. In Fig. 21(c), Φ_1 is a Tent matrix, the initiation value is 0.32, the chaotic parameter is 0.3, the sampling initial position is 1, the sampling distance is 4; Φ_2 is another Tent matrix, the initiation value is 0.32, the chaotic parameter is 0.45, the sampling initial position is 1, the sampling distance is 4. And $\alpha = 0.01$, $\beta = 253.9$ in all of Fig. 21(a)–(c).

Fig. 22 shows the recovery results, Fig. 22(a) is the original image, Fig. 22(b)–(d) are the recovery images using the original encryption matrices, Φ_1 and Φ_2. PSNRs of the recovery images in Fig. 22(b)–(d) are 32.29 dB, 32.47 dB, 32.41 dB, respectively. Fig. 23 shows the results using the perturbation matrices of Φ_1. All the perturbation values are 10^{-15} in Fig. 23(a)–(c),

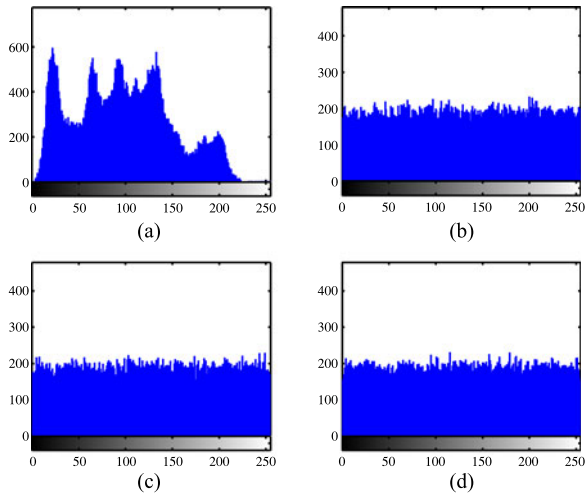


Fig. 24. Histograms of original and encrypted images. The size of the original image is 256×256, the sizes of the encrypted images are 190×256. The gray value is from 0 to 255, and the numbers of each gray value in histograms of encrypted image are almost equal. (a) The histogram of the original image. (b) The histogram of the Chebyshev encrypted image. (c) The histogram of the Logistic encrypted image. (d) The histogram of the Tent encrypted image.

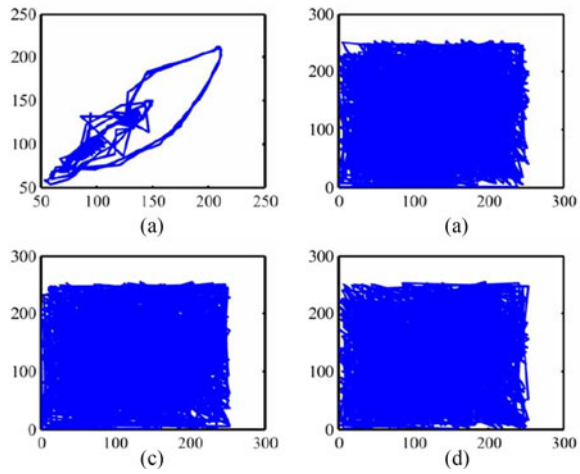


Fig. 25. Horizontal adjacent pixels correlation. The horizontal axis denotes gray values of a set of pixels chosen randomly, and the vertical axis denotes gray values of horizontal adjacent position of the set of pixels. (a) The horizontal adjacent pixel correlation of the original image. (b) The horizontal adjacent pixel correlation of the Chebyshev encrypted image. (c) The horizontal adjacent pixel correlation of the Logistic encrypted image. (d) The horizontal adjacent pixel correlation of the Tent encrypted image.

TABLE I
ADJACENT PIXEL CORRELATION

Adjacency Image	original	Chebyshev	Logistic	Tent
horizontal	0.9342	0.0055	0.0014	0.0081
vertical	0.9679	0.0057	−0.0026	0.0351
diagonal	0.9122	−0.0025	0.0020	0.0028

which implies that using matrices with a 10^{-15} initiation value perturbation can not decrypt the image.

Fig. 24 shows the histograms of the original image and encrypted images, Fig. 24(a) is the histogram of the original image, which has obvious characteristics, Fig. 24(b)–(d) are histograms of encrypted images, which are quite different from Fig. 24(a). In Fig. 24(b)–(d), the distribution of each gray value is approximately uniform, which implies that the numbers of each gray value are approximately equal, and the image encryption performance of the proposed method is excellent. To further illustrate the performance, the adjacent pixels correlation is analyzed.

Choose adjacent pixels randomly forming a pair of pixel vectors X, Y, the adjacency types include horizontal, vertical, diagonal. The adjacent pixels correlation is calculated by

$$r_{XY} = \frac{\operatorname{cov}(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}} \tag{21}$$

where $E(X) = \frac{1}{N}\sum_{i=1}^{N} X_i$, $E(Y) = \frac{1}{N}\sum_{i=1}^{N} Y_i$, $\operatorname{cov}(X,Y) = \frac{1}{N}\sum_{i=1}^{N}(X_i - E(X))(Y_i - E(Y))$, $D(X) = E(X^2) - (E(X))^2$, $D(Y) = E(Y^2) - (E(Y))^2$. The calculation results are in Table I. From Table I, the adjacent pixel correlation of the original image is high, larger than 0.9, close to 1, while the peers of the encrypted images are low, close to zero, which implies that the adjacent pixels are approximately incoherent with each other, and the pixel scrambling of the proposed encryption method performs well.

Choose 1000 adjacent pixel pairs randomly from four images, the original image, the Chebyshev encrypted image, the Logistic encrypted image, the Tent encrypted image, respectively. For Fig. 25(a), the pixels pairs chosen from original image are horizontal adjacent. Draw these pixel pairs in the coordinate system. For example, suppose the gray value of a selected point is 240, and the gray value of its horizontal adjacent point is 150, we draw a point at the position (240, 150) in the coordinate system. Draw all 1000 pairs in the coordinate system, Fig. 25(a) is obtained. For Fig. 25(b), the pixel pairs are chosen from the Chebyshev encrypted image. For Fig. 25(c), the pixel pairs are chosen from the Logistic encrypted image. For Fig. 25(d), the pixel pairs are chosen from the Tent encrypted image. The adjacent type in Fig. 26 is vertical, and the adjacent type in Fig. 27 are diagonal. In Figs. 26 and 27, the same as Fig. 25, the pixel pairs are chosen from the original image in Figs. 26(a) and 27(a), the pixel pairs are chosen from the Chebyshev encrypted image in Figs. 26(b) and 27(b), the pixel pairs are chosen from the Logisitc encrypted image in Figs. 26(c) and 27(c), the pixel pairs are chosen from the Tent encrypted image in Figs. 26(d) and 27(d). Points distribution of each (a) is concentrated, while (b), (c), (d) is disperse. It implies that the pixels correlation of the original image is high, but the pixels correlation of the encrypted image is low.

Last, the image entropy is calculated as follows

$$H = -\sum_{i=0}^{L-1} p(m_i)\log_2 p(m_i) \tag{22}$$

where L is the number of gray levels, m_i is the gray value, $i = 0, 1, 2, 3 \ldots L-1$, and $p(m_i)$ is the probability of each gray value, $\sum_{i=0}^{L-1} p(m_i) = 1$. The image entropy can be used to

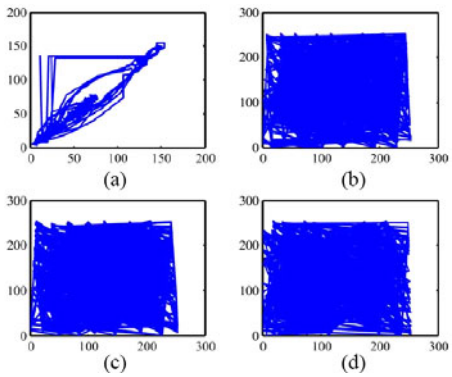


Fig. 26. Vertical adjacent pixels correlation. The horizontal axis denotes gray values of a set of pixels chosen randomly, and the vertical axis denotes gray values of vertical adjacent position of the set of pixels. (a) The vertical adjacent pixel correlation of the original image. (b) The vertical adjacent pixel correlation of the Chebyshev encrypted image. (c) The vertical adjacent pixel correlation of the Logistic encrypted image. (d) The horizontal adjacent pixel correlation of the Tent encrypted image.

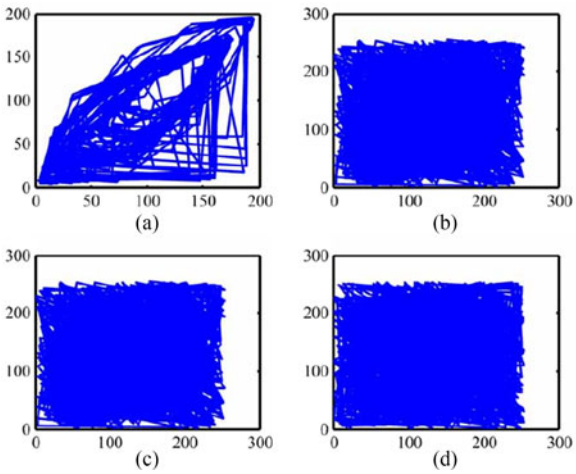


Fig. 27. Diagonal adjacent pixels correlation. The horizontal axis denotes gray values of a set of pixels chosen randomly, and the vertical axis denotes gray values of diagonal adjacent position of the set of pixels. (a) The diagonal adjacent pixel correlation of the original image. (b) The diagonal adjacent pixel correlation of the Chebyshev encrypted image. (c) The diagonal adjacent pixel correlation of the Logistic encrypted image. (d) The diagonal adjacent pixel correlation of the Tent encrypted image.

measure the distribution characteristics of gray values. If the probabilities of every gray value are equal, the image entropy reaches the maximum, $\log_2 L$. It can be used to analyze the performance of the image encryption, and the closer to $\log_2 L$ the image entropy is, the better the encryption performance is. In this experiment, four images are tested, and $L = 256$. Four original images are chosen from the Matlab 2009b image database. The original image in Fig. 28(a) is the image coins. Three cipher images are encrypted by Chebyshev, Logistic and Tent, respectively. The entropy of the image coins is 6.3256, entropies of three encrypted image are 7.9860, 7.9849, 7.9853. The original image in Fig. 28(b) is the image cameraman. The entropy of the image cameraman is 7.0097, entropies of three encrypted images are 7.9874, 7.9865, 7.9866. The original image in Fig. 28(c) is the image autumn. The entropy of the

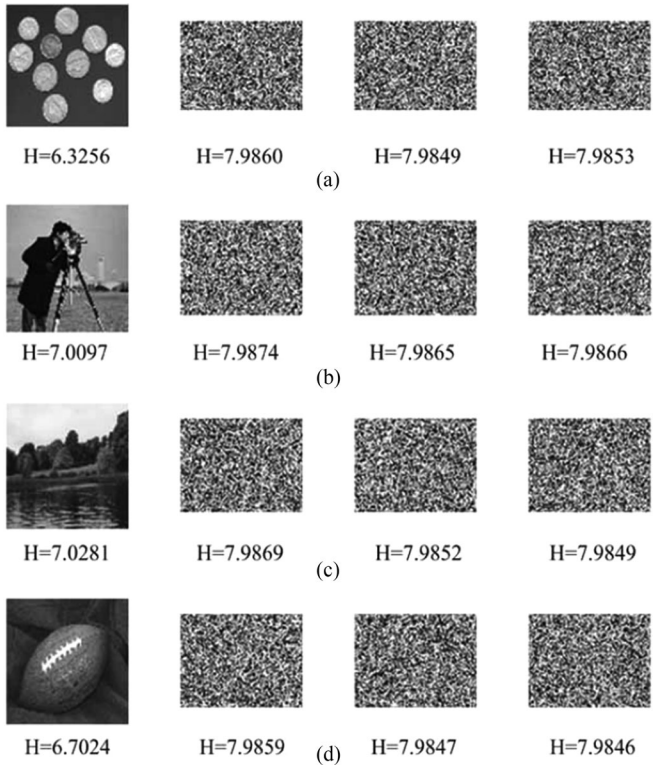


Fig. 28. Image entropy of different images. In (a)–(d), three cipher images are encrypted by Chebyshev, Logistic and Tent, respectively. The entropies of four plain images are from 6.3256 to 7.0281, and all the entropies of encrypted images are larger than 7.98, close to 8. (a) The original image is the image coins. (b) The original image is the image cameraman. (c) The original image is the image autumn. (d) The original image is the image football.

Fig. 29. The encryption and decryption results of the traditional method. (a) Cipher image using the traditional method. (b) Recovery image, the PSNR = 32.01 dB.

image autumn is 7.0281, entropies of three encrypted images are 7.9869, 7.9852, 7.9849. The original image in Fig. 28(d) is the image football. The entropy of the image football is 6.7024, entropies of three encrypted images are 7.9859, 7.9847, 7.9846. As shown in Fig. 28, the entropies of encrypted images using different chaotic matrices are close to 8, which implies that the encryption performance is excellent for different images.

For comparison, the encryption results of the traditional method without the mask matrix Φ_2 are shown in Figs. 29 and 30. The original image is the image lena with 256 gray levels from 0 to 255. The measurement matrix is a Chebyshev matrix. From Fig. 29(a), the performance of the cipher image is not as good as that of Fig. 21. Fig. 29(b) is the recovery image, the

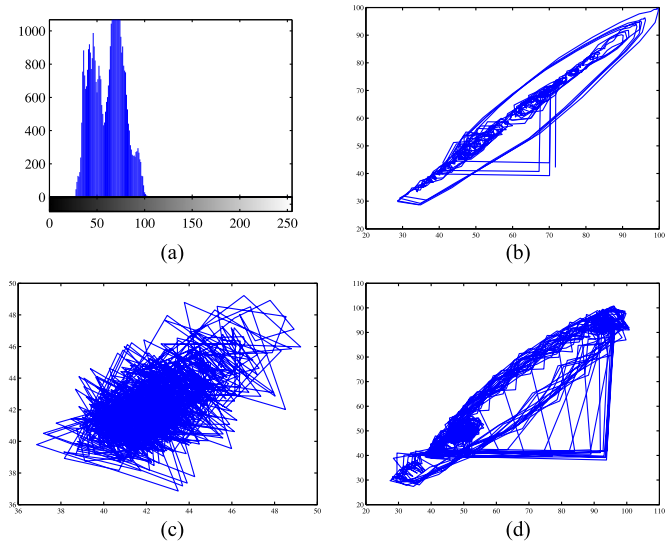


Fig. 30. Histogram and adjacent pixel correlation of the encrypted image using the traditional method. (a) Cipher image histogram. (b) The horizontal adjacent pixel correlation. (c) The vertical adjacent pixel correlation. (d) The diagonal adjacent pixel correlation.

PSNR of the recovery image is 32.01 dB. Fig. 30 shows the histogram and the adjacent correlation of the cipher image. From Fig. 30(a), the distribution of the gray value is not uniform, and is concentrated on an interval, the image entropy is 5.8780. From Fig. 30(b)–(d), the adjacent pixel correlations are high, the horizontal correlation is 0.9830, the vertical correlation is 0.9842, the diagonal correlation is 0.9657.

V. Conclusion

With the development from WBAN to BBN, energy saving of nodes and security of transmission data are challenging tasks. In this paper, chaotic compressive sensing is proposed to solve the energy-efficiency and security problems simultaneously. Compared with the traditional compressive sensing which needs to store the whole matrix, our proposed method can save storage space by only storing matrix generation parameters. Particularly in BBN, where each pair of nodes needs a matrix, chaotic compressive sensing saves more space. In image transmission, the modified method is proposed to improve the security of image compressive encryption by utilizing two mechanisms. The simulation results show that the encryption performance is excellent. Future works could be carried out to develop CCS in mobile context, like sports games, in which the mobility of the body and the body gesture should be taken into account. Moreover, for saving energy further, the routing protocols are needed for BBN. Although future research is needed, this work indicates that CCS is available in BBN to fulfill the energy-efficiency and security and saving the storage space.

Acknowledgment

The authors would like to thank the editorial board and reviewers.

References

[1] A. Meharouech, J. Elias, and A. Mehaoua, "Future body-to-body networks for ubiquitous healthcare: A survey, taxonomy and challenges," in *Proc. 2nd Int. Symp. Future Inf. Commun. Technol. Ubiquitous HealthCare*, May 2015, pp. 1–6.

[2] D. P. Tobn, T. H. Falk, and M. Maier, "Context awareness in WBANS: A survey on medical and non-medical applications," *IEEE Wireless Commun.*, vol. 20, no. 4, pp. 30–37, Aug. 2013.

[3] H. Cao, V. Leung, C. Chow, and H. Chan, "Enabling technologies for wireless body area networks: A survey and outlook," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 84–93, Dec. 2009.

[4] T. Gao *et al.*, "The advanced health and disaster aid network: A light-weight wireless medical system for triage," *IEEE Trans. Biomed. Circuits Syst.*, vol. 1, no. 3, pp. 203–216, Sep. 2007.

[5] A. Milenković, C. Otto, and E. Jovanov, "Wireless sensor networks for personal health monitoring: Issues and an implementation," *Comput. Commun.*, vol. 29, no. 13, pp. 2521–2533, 2006.

[6] J. i. Naganawa, K. Wangchuk, M. Kim, T. Aoyagi, and J. I. Takada, "Simulation-based scenario-specific channel modeling for WBAN cooperative transmission schemes," *IEEE J. Biomed. Health Informat.*, vol. 19, no. 2, pp. 559–570, Mar. 2015.

[7] G. R. Tsouri, S. R. Zambito, and J. Venkataraman, "On the benefits of creeping wave antennas in reducing interference between neighboring wireless body area networks," *IEEE Trans. Biomed. Circuits Syst.*, vol. 11, no. 1, pp. 153–160, Feb. 2017.

[8] M. M. Alam and E. B. Hamida, "Interference mitigation and coexistence strategies in IEEE 802.15.6 based wearable body-to-body networks," in *Proc. Int. Conf. Cogn. Radio Oriented Wireless Netw.*, 2015, pp. 665–677.

[9] D. B. Arbia, M. M. Alam, R. Attia, and E. B. Hamida, "A novel multi-hop body-to-body routing protocol for disaster and emergency networks," in *Proc. Int. Conf. Wireless Netw. Mobile Commun.*, Oct. 2016, pp. 246–252.

[10] V. Goudar, Z. Ren, P. Brochu, M. Potkonjak, and Q. Pei, "Optimizing the output of a human-powered energy harvesting system with miniaturization and integrated control," *IEEE Sens. J.*, vol. 14, no. 7, pp. 2084–2091, Jul. 2014.

[11] A. Khaligh, P. Zeng, and C. Zheng, "Kinetic energy harvesting using piezoelectric and electromagnetic technologies-state of the art," *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 850–860, Mar. 2010.

[12] E. Ibarra, A. Antonopoulos, E. Kartsakli, J. J. P. C. Rodrigues, and C. Verikoukis, "QoS-aware energy management in body sensor nodes powered by human energy harvesting," *IEEE Sens. J.*, vol. 16, no. 2, pp. 542–549, Jan. 2016.

[13] H. Mosavat-Jahromi, B. Maham, and T. Tsiftsis, "Maximizing spectral efficiency for energy harvesting-aware WBAN," *IEEE J. Biomed. Health Informat.*, 2016, to be published.

[14] C. Zhang, Y. Wang, Y. Liang, M. Shu, and C. Chen, "An energy-efficient MAC protocol for medical emergency monitoring body sensor networks," *Sensors*, vol. 16, no. 3, 2016, Art. no. E385.

[15] R. Rajagopalan, "Energy efficient routing algorithm for patient monitoring in body sensor networks," in *Proc. IEEE 13th Int. Conf. Wearable Implantable Body Sens. Netw.*, Jun. 2016, pp. 141–146.

[16] V. Ayatollahitafti, M. A. Ngadi, J. bin Mohamad Sharif, and M. Abdullahi, "An efficient next hop selection algorithm for multi-hop body area networks," *PloS One*, vol. 11, no. 1, 2016, Art. no. e0146464.

[17] Y. Liao, M. S. Leeson, M. D. Higgins, and C. Bai, "An incremental relay based cooperative routing protocol for wireless in-body sensor networks," in *Proc. IEEE 12th Int. Conf. Wireless Mobile Comput., Netw. Commun.*, 2016, pp. 1–6.

[18] D. Liu, Y. Geng, and K. Pahlavan, "End-to-end power optimization in non-homogenous relay environment for wireless body area networks (WBANs)," in *Proc. 10th Int. Symp. Med. Inf. Commun. Technol.*, Mar. 2016, pp. 1–5.

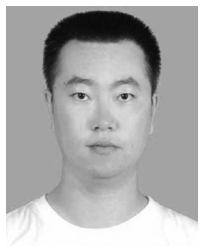
[19] A. H. Sodhro, Y. Li, and M. A. Shah, "Energy-efficient adaptive transmission power control for wireless body area networks," *IET Commun.*, vol. 10, no. 1, pp. 81–90, 2016.

[20] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informat. J.*, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1110866516300482

[21] X. Liu, Y. Zhu, Y. Ge, D. Wu, and B. Zou, "A secure medical information management system for wireless body area networks," *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 1, pp. 221–237, 2016.

[22] S. A. Salehi, M. A. Razzaque, I. Tomeo-Reyes, N. Hussain, and V. Kaviani, "Efficient high-rate key management technique for wireless body area networks," in *Proc. 22nd Asia-Pacific Conf. Commun.*, Aug. 2016, pp. 529–534.
[23] L. Wu, Y. Zhang, L. Li, and J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks," *J. Med. Syst.*, vol. 40, no. 6, pp. 1–12, 2016.
[24] H. Zhu, L. Gao, and H. Li, "Secure and privacy-preserving body sensor data collection and query scheme," *Sensors*, vol. 16, no. 2, 2016, Art. no. 179.
[25] A. M. R. Dixon, E. G. Allstot, D. Gangopadhyay, and D. J. Allstot, "Compressed sensing system considerations for ECG and EMG wireless biosensors," *IEEE Trans. Biomed. Circuits Syst.*, vol. 6, no. 2, pp. 156–166, Apr. 2012.
[26] R. Dautov and G. R. Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography," *IEEE J. Biomed. Health Informat.*, vol. 20, no. 1, pp. 135–142, Jan. 2016.
[27] F. Pareschi, P. Albertini, G. Frattini, M. Mangia, R. Rovatti, and G. Setti, "Hardware-algorithms co-design and implementation of an analog-to-information converter for biosignals based on compressed sensing," *IEEE Trans. Biomed. Circuits Syst.*, vol. 10, no. 1, pp. 149–162, Feb. 2016.
[28] A. Wang, F. Lin, Z. Jin, and W. Xu, "Ultra-low power dynamic knob in adaptive compressed sensing towards biosignal dynamics," *IEEE Trans. Biomed. Circuits Syst.*, vol. 10, no. 3, pp. 579–592, Jun. 2016.
[29] Y. C. Cheng, P. Y. Tsai, and M. H. Huang, "Matrix-inversion-free compressed sensing with variable orthogonal multi-matching pursuit based on prior information for ECG signals," *IEEE Trans. Biomed. Circuits Syst.*, vol. 10, no. 4, pp. 864–873, Aug. 2016.
[30] M. Shoaran, M. H. Kamal, C. Pollo, P. Vandergheynst, and A. Schmid, "Compact low-power cortical recording architecture for compressive multichannel data acquisition," *IEEE Trans. Biomed. Circuits Syst.*, vol. 8, no. 6, pp. 857–870, Dec. 2014.
[31] E. J. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.
[32] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[33] Y. Tsaig and D. L. Donoho, "Extensions of compressed sensing," *Signal Process.*, vol. 86, no. 3, pp. 549–571, 2006.
[34] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.
[35] H. Yuan, H. Song, X. Sun, K. Guo, and Z. Ju, "Compressive sensing measurement matrix construction based on improved size compatible array LDPC code," *IET Image Process.*, vol. 9, no. 11, pp. 993–1001, 2015.
[36] W. Yan, Q. Wang, and Y. Shen, "Shrinkage-based alternating projection algorithm for efficient measurement matrix construction in compressive sensing," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 5, pp. 1073–1084, May 2014.
[37] G. Li, Z. Zhu, D. Yang, L. Chang, and H. Bai, "On projection matrix optimization for compressive sensing systems," *IEEE Trans. Signal Process.*, vol. 61, no. 11, pp. 2887–2898, Jun. 2013.
[38] D. Xie, H. Peng, L. Li, and Y. Yang, "Semi-tensor compressed sensing," *Digital Signal Process.*, vol. 58, pp. 85–92, 2016.
[39] D. L. Donoho and M. Elad, "Optimally sparse representation in general (nonorthogonal) dictionaries via l1 minimization," in *Proc. Nat. Acad. Sci.*, vol. 100, no. 5, 2003, pp. 2197–2202.
[40] D. L. Donoho and X. Huo, "Uncertainty principles and ideal atomic decomposition," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2845–2862, Nov. 2001.
[41] J. A. Tropp, "Greed is good: Algorithmic results for sparse approximation," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2231–2242, Oct. 2004.
[42] E. J. Candes, Y. C. Eldar, D. Needell, and P. Randall, "Compressed sensing with coherent and redundant dictionaries," *Appl. Comput. Harmonic Anal.*, vol. 31, no. 1, pp. 59–73, 2011.
[43] L. Yu, J. P. Barbot, G. Zheng, and H. Sun, "Compressive sensing with chaotic sequence," *IEEE Signal Process. Lett.*, vol. 17, no. 8, pp. 731–734, Aug. 2010.
[44] X. Li, L. Bao, D. Zhao, D. Li, and W. He, "The analyses of an improved 2-order Chebyshev chaotic sequence," in *Proc. Int. Conf. Comput. Sci. Netw. Technol.*, Dec. 2011, vol. 2, pp. 1224–1227.
[45] M. Frunzete, L. Yu, J. P. Barbot, and A. Vlad, "Compressive sensing matrix designed by tent map, for secure data transmission," in *Proc. Signal Process. Algorithms, Archit., Arrangements, Appl.*, Sep. 2011, pp. 1–6.
[46] G. Chen, D. Zhang, Q. Chen, and D. Zhou, "The characteristic of different chaotic sequences for compressive sensing," in *Proc. 5th Int. Congr. Image Signal Process.*, Oct. 2012, pp. 1475–1479.
[47] X. Yuan, H. Jiang, G. Huang, and P. A. Wilford, "SLOPE: Shrinkage of local overlapping patches estimator for lensless compressive imaging," *IEEE Sens. J.*, vol. 16, no. 22, pp. 8091–8102, Nov. 2016.
[48] L. Y. Zhang, K. W. Wong, Y. Zhang, and J. Zhou, "Bi-level protected compressive sampling," *IEEE Trans. Multimedia*, vol. 18, no. 9, pp. 1720–1732, Sep. 2016.
[49] B. Shahrasbi and N. Rahnavard, "Model-based nonuniform compressive sampling and recovery of natural images utilizing a wavelet-domain universal hidden Markov model," *IEEE Trans. Signal Process.*, vol. 65, no. 1, pp. 95–104, Jan. 2017.
[50] X. Fei, Z. Wei, and L. Xiao, "Iterative directional total variation refinement for compressive sensing image reconstruction," *IEEE Signal Process. Lett.*, vol. 20, no. 11, pp. 1070–1073, Nov. 2013.
[51] J. Khan, J. Ahmad, and S. O. Hwang, "An efficient image encryption scheme based on Henon map, skew tent map and s-box," in *Proc. 6th Int. Conf. Model., Simul., Appl. Optim.*, May 2015, pp. 1–6.

Haipeng Peng received the M.S. degree in system engineering from Shenyang University of Technology, Shenyang, China, in 2006, and the Ph.D. degree in signal and information processing from Beijing University of Posts and Telecommunications, Beijing, China, in 2010. He is currently an Associate Professor at the School of Cyberspace Security, Beijing University of Posts and Telecommunications. He has coauthored 50 scientific papers. His research interests include information security, network security, complex networks, and control of dynamical systems.



Ye Tian received the B.S. degree in communication engineering from Nanchang University, Nanchang, China, in 2011. He is working toward the M.S. degree in information security at Beijing University of Posts and Telecommunications, Beijing, China. His major research interests include compressive sensing and image encryption.

Jürgen Kurths studied mathematics at the University of Rostock, Rostock, Germany, and received the Ph.D. degree from the GDR Academy of Sciences, Berlin, Germany, in 1983. He was a Full Professor at the University of Potsdam from 1994 to 2008. He has been a Professor of nonlinear dynamics at Humboldt University of Berlin, Berlin, and the Chair of the research domain Transdisciplinary Concepts of the Potsdam Institute for Climate Impact Research, Potsdam, Germany, since 2008, and a Sixth-Century Chair of the University of Aberdeen, Aberdeen, U.K., since 2009. He has authored or coauthored more than 500 papers that are cited more than 18 000 times (H-factor: 57). His primary research interests include synchronization, complex networks, and time-series analysis and their applications. He is a Fellow of the American Physical Society. He received the Alexander von Humbolts Research Award from CSIR, India, in 2005, and an honorary doctorate in 2008 from N. I. Lobachevsky State University of Nizhny Novgorod and one in 2012 from Saratov State University. He became a member of the Academia Europaea in 2010 and of the Macedonian Academy of Sciences and Arts in 2012. He is an Editor of *PLoS ONE*, the *Philosophical Transactions of the Royal Society A*, the *Journal of Nonlinear Science*, and *Chaos*.

Lixiang Li received the M.S. degree in circuit and system from Yanshan University, Qinhuangdao, China, in 2003, and the Ph.D. degree in signal and information processing from Beijing University of Posts and Telecommunications, Beijing, China, in 2006. She is currently a Professor at the School of Cyberspace Security, Beijing University of Posts and Telecommunications. In 2011, she visited Potsdam Germany. She has coauthored 70 scientific papers. She is involved in research on swarm intelligence and network security. Her research has been supported by ten national foundations for recent five years. She has been the National Excellent Doctoral Theses winner, Henry Fok Education Foundation Award winner, Hong Kong Scholar Award winner, and Beijing Higher Education Program for Young Talents winner. She was selected in the Program for New Century Excellent Talents in University

Yixian Yang received the M.S. degree in applied mathematics and the Ph.D. degree in electronics and communication systems from Beijing University of Posts and Telecommunications, Beijing, China, in 1986 and 1988, respectively. He is the Managing Director of the Information Security Center, Beijing University of Posts and Telecommunications. He has authored more than 40 national and provincial key scientific research project and contributed to more than 300 high-level papers and 20 monographs. His main research interests include coding and cryptography, information and network security, and signal and information processing. He is a Yangtze River scholar Program professor, National Outstanding Youth Fund winner, and the National Teaching Master.

Daoshun Wang received the B.S. degree from the Department of Mathematics, Lanzhou University, Lanzhou, China, in 1987, and the Ph.D. degree from the Department of Mathematics, Sichuan University, Chengdu, Sichuan, China, in 2001. He is currently an Associate Professor in the Department of Computer Science and Technology, Tsinghua University, Beijing, China. His research interests include visual cryptography, digital watermarking, and label anti-counterfeiting.