IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 17, 2019, accepted March 9, 2019, date of publication March 19, 2019, date of current version April 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2906265

Fingerprint Recognition Strategies Based on a Fuzzy Commitment for Cloud-Assisted IoT: A Minutiae-Based Sector Coding Approach

SHA SHI[1,2,3], JIA CUI[4], XIN-LI ZHANG[5], YANG LIU[4], JING-LIANG GAO[6], AND YUN-JIANG WANG[3,6]

[1]Engineering Research Center of Molecular and Neuro Imaging, Ministry of Education, Xidian University, Xi'an 710068, China
[2]School of Life Science and Technology, Xidian University, Xi'an 710068, China
[3]Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518055, China
[4]National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China
[5]Xinxiang Medical University, Xinxiang 453003, China
[6]The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

Corresponding author: Yun-Jiang Wang (yunjiangw@xidian.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61771377, Grant 61502376, and Grant 61701375, in part by the Projects of International Cooperation and Exchanges of Shannxi Province under Grant 2017KW-003 and Grant 2016KW-037, and in part by the Fundamental Research Funds for the Central Universities of China.

ABSTRACT In parallel with the rapid developments of cloud-assisted IoT, the corresponding security and privacy issue emerges as a challenge. Biometric recognition technologies are interesting and promising to reinforce traditional cryptographic and personal authentication systems for cloud-assisted IoT. However, the biometric information, if compromised, cannot be canceled and substituted easily. In this paper, based on fuzzy commitment protocol, a fingerprint recognition scheme using minutiae-based sector coding strategy is proposed for cloud-assisted IoT. In our approach, the minutiae of a fingerprint are classified into many designed sectors and then encoded according to their features. With the idea of fuzzy commitment, the key encryption process is accomplished by using BCH codes and Hash mappings. Our scheme, not only provides a flexible way to realize the fingerprint recognition between the complexity and security by designing error-correcting codes with different parameters, but also offers a good balance between the genuine accept rate (GAR) and the false acceptance rate (FAR) with customized sector coding strategies.

INDEX TERMS Internet of Things, information security, biometrics, error-correction codes.

I. INTRODUCTION

The emergence of the Internet of Things (IoT) has profoundly affected our daily lives in many aspects including finance, transportation, health, industry and so on [1]–[4]. Along with the rapid developments of IoT, more clever data processing techniques are required to lighten the load of smart things [3], [5], [6]. Cloud-assisted IoT is a promising scheme which may greatly boost advancements of IoT. On the other hand, probably more important, the security and privacy issue associated with the cloud-assisted IoT systems remains an outstanding challenge [7]–[9].

The biometrics are widely used in the identity authentication system due to their unique and stability [10], [11]. It is well known that biometric templates cannot be revoked and republished as easily as classical keys [12]. Suffering from the hardness of replacing biometric template, repeated use of the same biometric features in different applications aggravates the risk of information leakage [13]. That is exactly the challenge faced by fingerprint recognition, which is, though already one of the most mature and popular biometric authentication techniques [14], [15].

Fingerprint-based identity authentication systems still attract lots of attention in recent years. In 2015, Barman et al proposed a fingerprint-based crypto-biometric system for network security, where the cryptographic key can be generated from a cancelable fingerprint template of both communicating parties [16]. In the same year, Cao and A. K. Jain introduced a strategy to reconstruct the original fingerprint image. In their approach, the orientation patch dictionary

The associate editor coordinating the review of this manuscript and approving it for publication was Kuo-Hui Yeh.

is used to reconstruct the orientation field from minutiae, while the continuous phase patch dictionary is used to reconstruct the ridge pattern [17]. In 2017, the case of fingerprint recognition of young children is considered in [18]. In 2018, Chugh et al introduced a convolutional neural network to the fingerprint recognition and proposed a new approach for fingerprint spoof detection [19], in which the local patches centered and aligned using fingerprint minutiae. In the same year, the group of A. K. Jain proposed an automated latent fingerprint recognition algorithm that utilizes convolutional neural networks again for ridge flow estimation and minutiae descriptor extraction and extracted complementary templates to represent the latent [20], [21]. It is clear that it is still necessary and worthwhile to improve the fingerprint recognition with the help of protection techniques for biometric templates [22]–[24].

Fuzzy commitment is one of the popular biometric encryption schemes by using error-correcting codes to implement the provable security [25]. With the help of the error-correcting capacity of the associated error-correcting codes [14], the fuzzy commitment scheme quantifies the differences of biometric data with the distances of codewords and allows the fuzziness of biometric templates to promote the performance of the identity recognition system. More precisely, in the fuzzy commitment scheme, the fuzzy range depends on the error-correcting capability of the corresponding code: the stronger the error-correcting capability of the associated error-correcting code, the lower the false rejection rate (FRR) is the corresponding biometric encryption system. And on the other hand, the stronger error-correcting capability will also result in higher false accept rate (FAR) for the biometric encryption system. Thus, according to different application scenarios, error-correcting codes with different error-correcting capacities are required.

For a fingerprint recognition based on fuzzy commitment, one of the key steps to template protection as well as cryptographic key generation is to associate the features of the fingerprint with an error-correcting code [10], [14]. So far, a minutiae-based method using minutiae information to identify and verify users offers a reliable identity authentication strategy [26]. To avoid the errors caused by the rotation or translation versions of each fingerprint image, the conventional minutiae-based matching algorithms take the Cartesian positions and orientations of minutiae as matching features to align fingerprint images [26], [27]. It is well recognized that the impressions captured at different times or by different sensors are also very likely to be deformed due to various pressure power or corruptions [13]. Therefore, to associate the features of the fingerprint with the error-correcting codes efficiently, it is interesting and worth to study the design of error-correcting codes that associated with a fingerprint recognition system based on fuzzy commitment.

In this paper, we introduce a new strategy for designing the error-correcting code according to the minutiae information of a fingerprint. In particular, based on fuzzy commitment protocol, a fingerprint cryptosystem using minutiae-based sector coding is proposed. In our strategy, the minutiae in a fingerprint is classified into many designed sectors, and the minutiae information in each sector is encoded by a designed sequence. The key encryption process is accomplished by using BCH codes and the Hash function. The numerical results show that our protocol not only provides a secure strategy for storing fingerprint information but also offers a good balance between Genuine Accept Rate (GAR) and False Acceptance Rate (FAR) flexibly by choosing BCH codes with different parameters.

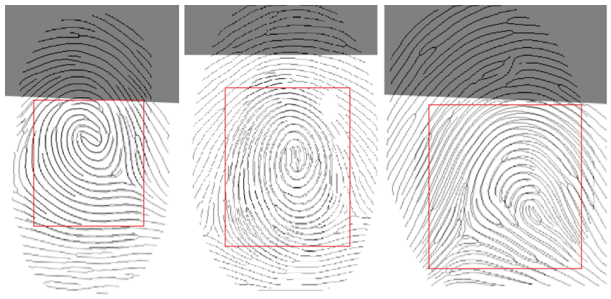


FIGURE 1. The red rectangles indicate the overlap regions of aligned fingerprint Images, which are just parts of areas extending outward from the core point of each corresponding fingerprint.

The structure of this paper is as follows. In Section II we first introduce the basic idea of our sector coding strategy and then we show how to encode the minutiae information of each sector with an ordered binary sequence. A fuzzy commitment scheme based on our fingerprint sector minutiae encoding is given in Section III. The discussion on our proposed strategy and the corresponding security analysis are given in Section IV. Finally, we conclude our work in Section V.

II. SECTOR CODING BASED ON FINGERPRINT MINUTIAE

Typically, the conventional fingerprint recognition takes the Cartesian positions and orientations of minutiae as matching features. Thus the alignment is necessary to be done first, and then the matching scores of corresponding character points could be computed [28]. It is evident that the fingerprint acquisition regions obtained by each time are not necessarily identical, just as shown in Figure 1. Thus only their overlap regions are considered as the valid region to compute the matching scores [27].

In this paper, we also need to choose the core point of a fingerprint as the original coordinate point first. The valid fingerprint region is classified into many designed sectors, and then the minutiae information in each sector is encoded by a binary sequence. The basic idea of the fingerprint image processing based on sector minutiae is as follows: When a fingerprint image is captured, the minutiae will be extracted first, and then the core reference point will be chosen by which, one accomplishes the coordinates transformation. Next, we start to treat the sector division problem which composing two key operations: concentric zoning and ray partition. Then one can

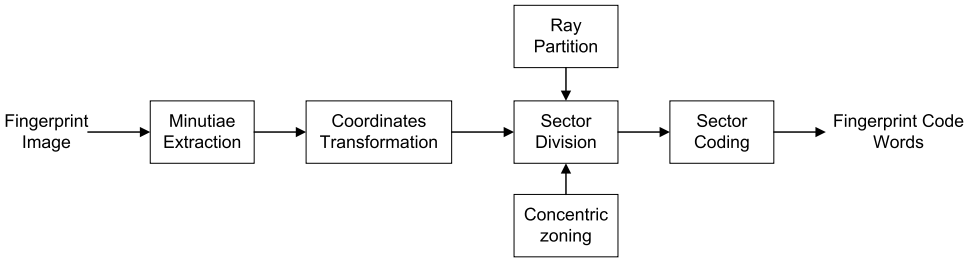


FIGURE 2. Fingerprint image processing based on sector minutiae.

encode the information in each sub-sector according to the features of minutiae in it. Finally one can obtain n ordered binary sequences that to be processed by using n randomly chosen code words. We illustrate the basic idea in Fig. 2, and the details are introduced below.

A. VALID IMAGE REGION AND MINUTIAE EXTRACTION

While there is no guarantee that the captured fingerprint images have an identical valid region, the fingerprint images can be cropped and given tags of valid region. Then, fingerprint minutiae extraction algorithms are imported to extract minutiae information of the associated fingerprint images. Here, the format of minutiae information is represented as:(x_i, y_i, θ_i, T), where the x_i, y_i indicates the position, θ_i the direction and T the minutiae types.

B. CORE REFERENCE POINT IN FINGERPRINT IMAGES

Having chosen the valid regions of fingerprint images, we are in a position to find the core point of an image with the Poincare Index (PI) algorithm [29]. The coordinate axis is built by taking the core point of a fingerprint image as the origin of coordinate, concerning the stream curves around the core point. The coordinate conversion of minutiae will be performed in the new coordinate system. The conversion formulas are as follow:

$$x' = x_0 + (x - x_0) \times \cos\theta_0 - (y - y_0) \times \sin\theta_0 \quad (1)$$

$$y' = y_0 + (x - x_0) \times \sin\theta_0 - (y - y_0) \times \cos\theta_0 \quad (2)$$

$$\theta' = (\theta + \theta_0) \mod 2\pi \quad (3)$$

$$T' = T \quad (4)$$

Here, (x_0, y_0, θ_0), (x, y, θ) and (x', y', θ') indicate the coordinate of the core point of a fingerprint image, the coordinate of the concerning point in the fingerprint image and the new coordinate of the concerning point, respectively. It is obvious that the minutiae type of the concerning point remains the same, thus $T' = T$.

C. SECTOR DIVISION

In this subsection, we introduce the sector division method. First, we draw two circles named as an inner circle with radius r and outer circle with radius R in such a way that the valid region is surrounded by these two circles. Second, the valid regions are further divided into n circular rings with the same width by concentric circles. Finally, the second partition is performed by drawing rays with the center being the start point in such a way that the angels between rays are constant, say θ. It is easy to see that by the two partitions, the valid region of a fingerprint image is parted into $n \times (360/\theta)$ sectors. As an example, the sector division with the origin as the center is shown below in Fig. 3, of which $r = 10$, $R = 50, n = 4, \theta = 30°$. Obviously, $4 \times (360/30) = 48$ sectors could be obtained after the division. In Fig. 4, we show the distributions of fingerprint minutiae in the partitioned sectors. It is evident that, if the minutiae come from the same fingerprint, then the two distributions are almost the same. On the other hand, if the minutiae come from different fingerprint images, the distribution differences can easily be checked.

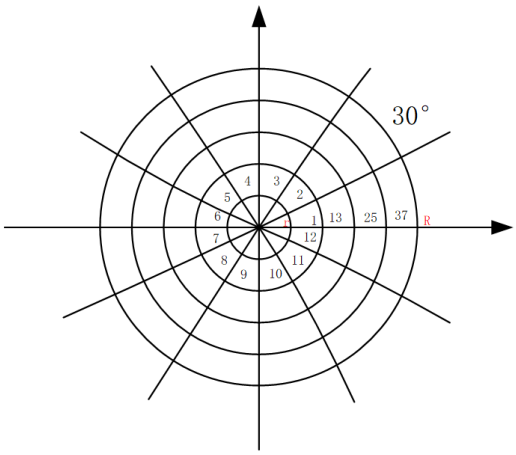


FIGURE 3. The idea of sector division. Here, $r = 10, R = 50, n = 4$, and $\theta = 30°$, thus the valid region of a fingerprint will be divided into 48 sub-sectors indicated with Arabic numeral.

D. SECTOR MINUTIAE CODING

Generally, after the sector division, the fingerprint minutiae are distributed in those sectors randomly. In Fig. 5, we take two samples from a standard fingerprint database (FVC2004). We can see that the differences between each sector are mainly reflected on numbers of minutiae, types of minutiae and also the corresponding angle information. Therefore, one of the key steps is to characterize the minutiae

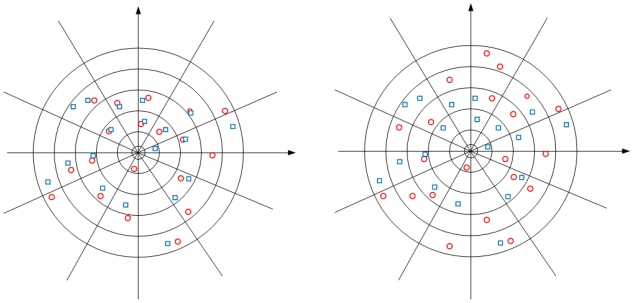


FIGURE 4. Distributions of fingerprint minutiae. The one on the left indicates the minutiae come from the same one but collected at a different time (represented by red squares and blue squares, respectively). The one on the right indicates the minutiae come from different fingerprints.

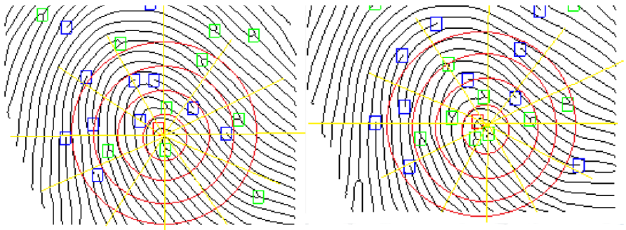


FIGURE 5. Sector Minutiae Distributions of FVC2004 DB1 73-6 (left) and of FVC2004 DB1 73-7 (right). The squares of different colors indicate minutiae of different types.

information with designed bit strings, i.e. codewords, which, as a sequence, will result in a reasonable *codeword* with each fingerprint images. In other words, here we need to introduce an encoding procedure to accomplish this task.

We know, generally, a fingerprint image can be partitioned into M sectors, in which $M = n \times (360/\theta)$, where n is the number of rings, and $a = 360/\theta$ is just the number of sectors in each ring. It is easy to see that a fingerprint image can be mapped to a bit string with length N, where $N = k \times M$.

In fact, each fingerprint sector can be represented by a feature vector with length k to reflect the minutiae information, which can be obtained by the following steps: judgment on valid regions of a fingerprint, statistics of minutiae quantity for a given region, statistics of minutiae types and sector direction calculation. Here, we introduce two strategies to represent the minutiae information. One is long sector coding with the length of information bits $k = 13$, and the other is the so-called short sector coding with $k = 9$.

The long sector coding strategy exploits the direction information associated with the minutiae to improve the precision of fingerprint minutiae [30]. Here we allocate four bits to denote the direction information which can be obtained as follows. First, we need to quantify the original direction information mentioned in the last subsection. Given the original direction $\theta(i)$, the quantified direction can be obtained with Eq. (5).

$$\theta^q(i) = \lfloor \theta(i,j)/\sigma \rfloor \tag{5}$$

Here, $\theta^q(i)$ is the direction after the quantization, σ is set to be 30° in this paper implying the direction information reduced to six directions only[1]. Then, we compute the direction value θ_{S_i} of each sub-sector with Eq. (6).

TABLE 1. The coding of sub-sector directions with the idea of Gray codes.

Direction Values	0	1	2	3	4	5
Direction Representations	0111	0101	0100	1100	1101	1111

$$\theta_{S_i} = \lfloor \frac{1}{N_{S_i}} \sum_{(i,j)\in S_i} \theta^q(i,j) \rfloor \tag{6}$$

Here, N_{S_i} is the number of pixel block in the i^{th} sub-sector and S_i denotes the i^{th} sub-sector image region. θ_{S_i} is just the average of direction values of the i^{th} sub-sector after round down operation. In table.1, based on the idea of Gray codes, we illustrate the representation of selected direction values.

The primary criterion of a fingerprint identification system is the similarity between relative locations, types, and the angle information of fingerprint minutiae. The fingerprint codes exploit this valid information and encode them as a fixed-length codeword with appropriate data form which can be encrypted later.

The only difference between the long and short fingerprint coding strategies is that the short sector coding is composed of only three parts: valid regions tags, number of minutiae in given region and minutiae types. However, in the long sector coding strategy, we also consider the sub-sector directions with an additional four bits besides the information contained in short strategy.

In Fig. 6, we illustrate the strategy of long sector coding. For simple, in this paper, we take the short sector coding as an example to explain our strategy in detail. Fig. 7 depicts the scheme of short sector coding which includes flag digits (two bits), number of minutiae (three bits) and minutiae types (four bits).

- Flag digits: two bits, which is used to indicate the validity of the concerning sub-sector. If there is no fingerprint information in a given sub-sector due to the considered region is small, we take 00 to indicate this case implying this region is invalid. Otherwise, we take 11 to indicate a valid region.
- The number of minutiae: three bits, straight forward, we take 000 to indicate that there are no minutiae in the considered sub-sector. Similarly, 001, 011, 111 indicate the number of minutiae is 1, 2 and 3 or more, respectively.
- Types of minutiae: Four bits, we use 0000 denotes no information contained. 0001 denotes the minutiae is composed of one endpoint, 1000 one branch point. Similarly, 0101, 1001 and 1010 denote two endpoints, one endpoint, and one branch point, two branch points, respectively. The case that there are more than two minutiae in the concerned sector is denoted as 1111.

In Table 2, we show the rules to represent the minutiae information of each sub-sector in detail.

[1]In fact, σ can be set to be any angle depending on the required degree of accuracy.

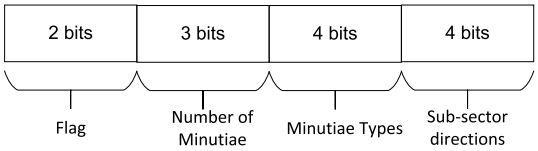


FIGURE 6. The structure of sector minutiae coding with long strategy.

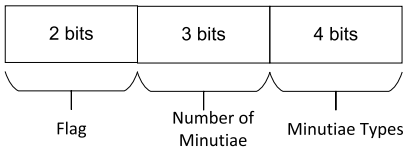


FIGURE 7. The structure of sector minutiae coding with short strategy.

TABLE 2. The structure of sector coding of fingerprint minutiae. The flag is composed of two bits which are used to signify the concerning region being valid (represented as 11) or not (represented as 00). Note that in the invalid region, there is no valid information considered. The block of minutiae consists of three bits, where 000 indicates no minutiae contained, 001 one minutia in the concerned region, 011 and 111 indicate two or more minutiae, respectively. The block of minutiae types consists of four bits, where 0000 denotes no information contained. 0001 denotes the minutiae is composed of one endpoint, 1000 one branch point. Similarly, 0101, 1001 and 1010 denote the three different minutiae types respectively as shown in this table. Note, we use 1111 to denote the case that there are more than two minutiae in the concerned sub-sector.

Region Attribute	Flag Digits	number of minutiae		types of minutiae	
invalid region	00	000		0000	
valid region	11	0	000	0000	
		1	001	one endpoint	0001
				one branch point	1000
		2	011	two endpoints	0101
				one endpoint and one branch point	1001
				two branch points	1010
		3	111	1111	

To show the idea of sector coding more clearly, we consider the fingerprint labeled $DB1:1-1$ in the standard fingerprint database FVC2004 [31]. If we set $n=3, \theta=\pi/6$, then we can get 36 valid sectors. With the coding algorithm mentioned above, the minutiae are transformed into 36 vectors as shown in Tab. 3.

TABLE 3. Fingerprint codewords obtained by using sector minutiae coding .

110011000	110010001	110000000	110011000	110000000	110011000
110000000	110000000	110000000	110000000	110000000	110000000
110000000	110000000	110000000	110111001	110000000	110000000
110011000	110000000	110000000	110000000	110000000	110000000
110011000	110000000	110010001	110000000	110000000	110010001
110000000	110010001	110000000	110000000	110000000	110000000

It is easy to check the rationality of sector coding. For example, if there is a valid sector contains one branch point, it will be encoded as 110011000. The hamming distance between this codeword and 110111001 is 2, where the latter denotes the case that there are two minutiae consisting one branch point and one endpoint in the concerned sub-sector. A similar relation exists between 110011000 and 110111010, where the latter implies there are two branch points in the valid sector. As the hamming distance between them is 4, it is harder for 110011000 to be transformed to 110110101 which indicates there are two endpoints in the valid sector. Likewise, the hamming distance between 110011000 and 111111111 is 5, thus it is reasonable to know that it is, even more, harder for a valid sector with one branch point is corrupted to be a valid sector with more than two minutiae.

III. A FUZZY COMMITMENT SCHEME BASED ON FINGERPRINT SECTOR MINUTIAE CODING

Fuzzy commitment algorithm that applied to the encryption stage of biometric identification is derived from the idea of a bit commitment scheme. The idea of the traditional fuzzy commitment scheme is illustrated in Fig. 8 [25]. Let $H:\{0,1\}^m \rightarrow \{0,1\}^l$ be a one-way Hash function and define $F(C,X)=(H(C),X-C)$, where C is a codeword in error-correcting code space and $X-C=\varepsilon$. The two stages of fuzzy commitment can be viewed as commitment and de-commitment. In the stage of commitment, we first choose a codeword C randomly as the initial key, then we use the biometric sequence of a registrar X to encrypt the key C. After computing $(\xi,\varepsilon)=F(C,X)=(H(C),X-C)$, we store (ξ,ε) in a database or a cloud platform.

In the stage of de-commitment, when the input biometric sequence of an authenticator X' is received, we obtain C' by the relation that $C'=X'-\varepsilon=C+(X'-X)$. Then the error-correcting technology in, the corresponding decoding algorithm is called to accomplish the error-correcting task. We name the output of decoder as C'', i.e. $C''=Decoder(C')$. Now one can compare the value of ξ and $H(C'')$. If $H(C'')=\xi$ holds, this authentication is approved, failed. Given the error-correcting capability of the concerning code is t, i.e. up to t errors can be corrected by the error-correcting code, the authentication will succeed while the hamming distance between biometric sequence X' and X is less than or equal to t.

Just as shown in Fig. 8, in traditional fuzzy commitment scheme, the helper data are constructed as a codeword from a selected error-correcting code (C), used to encode a chosen secret, masked with the biometric sequence (X) that has been observed during enrollment. Note, here $X=C+\varepsilon$ and ε are assumed to be public. In the biometrics secrecy system, C as the secret key in the template is hidden by using a Hash function. Therefore the secret of the biometrics systems highly depends on the size of the codeword space of the error-correcting code.

It is obvious, in traditional biometrics secrecy system based on fuzzy commitment, we can obtain C' with the biometric

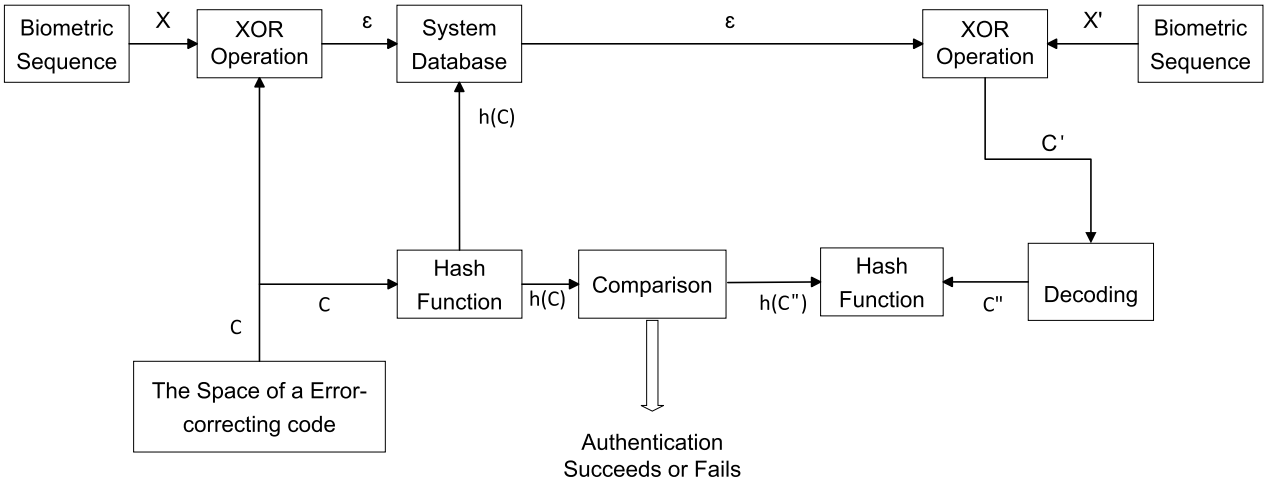


FIGURE 8. The scheme of the traditional fuzzy commitment when used for identity authentication based on fingerprint recognition.

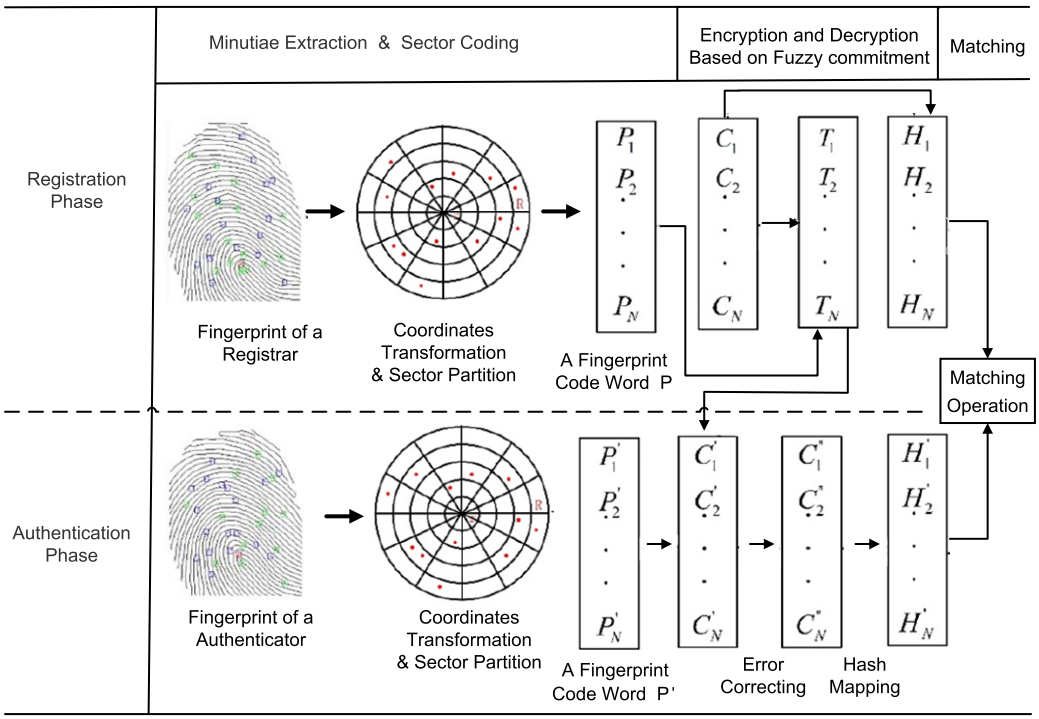


FIGURE 9. An identity authentication scheme based on a fuzzy commitment by using our fingerprint sector minutiae coding approach.

sequence (X') and ε. However, during the authentication process, the decoded output C'' obtained by the error-correcting decoding procedure should be exactly the same as the original C, due to the features of Hash function.

Of course, this requirement guarantees the secret of the concerning system, however, in some sense, reduce the robustness of the biometrics authentication system. In this paper, we improve the traditional biometrics secrecy system based on a fuzzy commitment by using the sector coding discussed in the last section. With the idea of sector division, we offer a flexible way to realize the fingerprint recognition between the complexity and security by designing error-correcting codes with different parameters. Our scheme also provides a good balance between the genuine accept rate (GAR) and the false acceptance rate (FAR) with customized sector coding strategies. The basic idea of the protocol can be shown in Fig. 9, which composes two key phases: registration and authentication.

A. REGISTRATION PHASE

In the registration phase, we need to map the fingerprint code P to a secret template, which can be accomplished as follows.

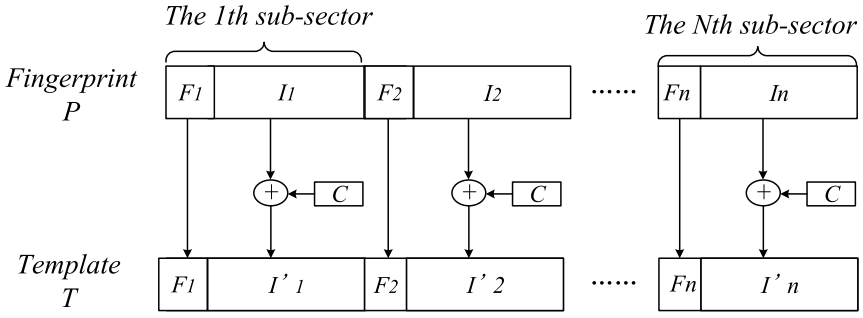


FIGURE 10. The mapping from fingerprint codes to the corresponding templates to be stored in a database or a cloud platform.

Take the fingerprint $P = \{p_1, p_2, \ldots, p_{N-1}, p_N\}$, where p_i $(1 \leq i \leq N)$ indicates the fingerprint code of the i^{th} sector composing the flag bits (F_i) and information bits (I_i). Then we select a codeword from the error-correcting codeword space randomly and apply the XOR operation on I_i and C_i to obtain the updated information bits I_i', i.e. $I_i' = I_i + C_i$.

When the short sector coding is applied for the fingerprint coding, we choose the BCH code (15, 7, 2) with code length being 15 and distance 2. Note that, in order to implement the XOR operation, we need to append zeros to the end of the information bits of the concerning fingerprint code such that the length of the information bits and the codeword are same. Similarly, When the long sector coding strategy is applied, the BCH code (15, 5, 3) with distance 3 is chosen. Of course, the appending operation is also required here. By this way, the template can be obtained, where $T = \{T_1, T_2, \ldots, T_{N-1}, T_N\}$ and $T_i = F_i, I_i'$. The idea of this phase can be illustrated with Fig. 10.

After the fingerprint map, one key step is to encrypt each codeword C_i with Hash function, and the resultant key is denoted as H where $H = \{H_1, H_2, \ldots, H_{N-1}, H_N\}$. The key H and fingerprint template T are all data should be held in the database (or cloud platform) to be used to identify the validity of the authentication.

Based on this scheme, there are different error-correcting codes can be chosen for different modes of sector minutiae coding. The parameters requirements for different security of biometric identification systems can be realized by the dynamic adjustment of error-correcting digits. The security of the biometrics information of users can be guaranteed by the random selection of codewords since it is impossible to recover the original fingerprint minutiae from just fingerprint template T.

B. AUTHENTICATION PHASE

In the authentication phase, the fingerprint code P' is generated from the fingerprint images with feature extraction and sector coding. Then the corresponding template T is drawn from the database and the *XOR* operation is performed on T and P' yielding the sequence C'. It is easy to see that, C' can be viewed as the original codeword C with noise. Thus, take C' as the input of a decoder for BCH codes, the output C'' should be exactly same as C if the fingerprint image is legal and the error caused by the noise can be corrected by the corresponding BCH code. Next, the Hash value of C'' will be calculated and the result is denoted as H' where $H' = \{H_1', H_2', \ldots, H_{N-1}', H_N'\}$. Now, we can compute the matching score of s of this authentication by Eq. (7) as follows,

$$s = \frac{N_\epsilon}{N - \alpha - \beta + \gamma} \times 100. \tag{7}$$

Here, N indicates the total number of sectors, α and β the number of invalid sectors of the register and the authenticator, respectively. γ denotes the number of common invalid sectors of the register and the authenticator. N_ϵ indicates the number of sectors that the corresponding keys of the register and of authenticator are identical. The authentication is successful if the matching score s is larger than a threshold λ and fail if s below λ.

IV. DISCUSSION

The procedure of the scheme shows that the error-correcting codes with different parameters can be designed according to practical requirements. The security of the fingerprint information is guaranteed by the mapping methods of codeword space which realized by using a Hash function here. In some sense, the security of this system can almost reach the same level as the one with the same length of *key*, given the codeword space is not exposed. For the case that the codeword space is exposed, the security of this scheme totally depends on the size of the codeword space of the concerning error-correcting code. In our scheme, the value of Hash mapping are truncated with one fixed length, say 40 bits. Thus the length of the key is $40 \times N$, where N is just the number of sectors.

Given $N = 60$, for example, the length of the binary key is 2400. Once the information about the concerning error-correcting codes is leaked out, the security of this identity authentication system depends on the size of codeword space. Suppose the error correcting code in use is $BCH(31, 21, 4)$, a key with length 21×60 can be obtained. Clearly, the larger the codeword space, the higher the security performance of the system and vice versa. For simple but without losing any generality, in this paper, we consider the *BCH* code

TABLE 4. The GAR of the proposed fingerprint recognition scheme with $r = 8, R = 123, n = 5, \gamma = 30^o$.

Thresholds λ	70	75	80	85	90	95	100
Short coding strategy	93.8	92.5	91.7	90.8	89.7	88.5	86
Long coding strategy	91.6	90.7	89.9	89.0	88.1	87.4	85.3

TABLE 5. The FAR of the proposed fingerprint recognition scheme with $r = 8, R = 123, n = 5, \gamma = 30^o$.

Thresholds λ	70	75	80	85	90	95	100
Short coding strategy	0.75	0.63	0.45	0.31	0.12	0.05	0.03
Long coding strategy	0.57	0.48	0.37	0.20	0.08	0.01	0.01

with length 15, say the code $BCH(15, 7, 2)$ whose codeword space size is 2^7. It is evident that it will take 128^{60} attempts to break through the system with methods of brute force. We want to point out that the security can be improved easily with an advanced error-correcting code adopted. Of course, along with the adoption of the advanced error-correcting code, a new sector minutiae coding strategy is required, which also can be easily designed based on our proposed coding approach.

Typically, we can use the genuine accept rate (*GAR*) and false acceptance rate (*FAR*) to evaluate the fingerprint recognition system. In this paper, we test our system by using fingerprints from the online database DB1-A of FVC2004. There are 100 fingerprints in DB1-A, thus we can obtain 800 fingerprint images if each fingerprint is captured 8 times. Suppose each fingerprint image is divided into 60 sectors with the parameter value as $r = 8, R = 123, n = 5$ and $\gamma = 30^o$. We compute the *GAR* and *FAR* of the proposed fingerprint recognition system under two cases: short fingerprint coding and long fingerprint coding. In Tab. 4 and 5, we show the numerical results under different thresholds.

The lengths of sector minutiae coding are 540 and 780 when the short encoding scheme and long encoding scheme are adopted, respectively. According to the methods mentioned at (III-A), the FAR and GAR are obtained under different thresholds denoted as λs. In Tab. 4 and 5, we display the performances of GAR and FAR by using our scheme with the values of λ being 70, 75, 80, 85, 90 and 95 respectively.

It is easy to see the higher the threshold, the more similarity between the registered fingerprint and the authenticated fingerprint are required. Thus, FAR should be relatively low just as shown in Tab. 5. On the other hand, the lower threshold means less similarity between the registered fingerprint and the authenticated fingerprint could be accepted. Therefore, both the GAR and FAR would be relatively high.

It is also interesting to consider and compare the two coding strategies discussed in this paper. For example, given the threshold λ being 70, when the short coding strategy mentioned in this paper is in use, the GAR and FAR are 93.8% and 0.75%, respectively. While, if long coding strategy is exploited, the GAR and FAR are turn out to be 91.6% and 0.57%, respectively. It obviously that, the short coding strategy yields a better GAR when compared with the long coding strategy. On the other hand, a better FAR would be obtained when using a long coding strategy. We can check this result again by considering the case that λ being 95. It is evident that the GAR and FAR are 88.5% and 0.05%, respectively, when the short coding strategy is in use. While the GAR and FAR will be reduced to 87.4% and 0.01%, respectively if one chooses the long coding strategy.

V. CONCLUSION

Consider the scenarios of cloud-assisted IoT, we develop an identity authentication by using fingerprint recognition system based on a fuzzy commitment scheme. In this way, the idea of fuzzy commitment is successfully applied in the fingerprint recognition system to alleviate the information leakage problem. The error-correcting codes used in the fingerprint recognition system play a crucial role in the security of the system as which highly depends on the size of the codeword space of the concerning code. Our scheme provides a flexible way to realize fingerprint recognition between complexity and security by designing different error-correcting codes. Moreover, one also can adjust the threshold (λ) according to various application scenarios to achieve a balance between GAR and FAR.

The flexibility of the proposed scheme is accomplished by introducing a sector coding strategy based on the minutiae information of fingerprint into a fuzzy commitment scheme. We also want to point out that, for simplicity, we take *BCH* codes $[15, 7, 2]$ and $[15, 5, 3]$ during the numerical simulations. In fact, an advanced error-correcting code may be required in practices due to the security issue. Along with the adoption of advanced error-correcting codes, the sector minutiae coding strategy may be required to improve, and a more advanced coding strategy should be designed. However, the sector minutiae coding strategy proposed in this paper can easily be expanded and improved based on a similar idea.

As a future work, we notice that artificial intelligence has attracted lots of attention in recent years and the deep learning has been introduced in the identity authentication scheme based on fingerprint recognition [17], [19]. It is interesting to consider the applications of the neural network in the sector coding, by which one may design a more advanced coding strategy to satisfy the requirements come from the advanced error-correcting codes that required in a practice identity authentication scheme. We think the deep learning-based sector coding may play a crucial role in addressing the security and privacy problems for cloud-assisted IoT.

ACKNOWLEDGMENT

We thank Prof. Q. Jiang for the valuable suggestions on the early version of our manuscript and thank Dr. Y. Liu for the constructive comments on the security analysis of the proposed protocol.

REFERENCES

[1] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and A. C. Shehzad, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Elect. Eng.*, vol. 63, pp. 182–195, Oct. 2017.

[2] K.-H. Yeh, "A secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments," *IEEE Syst. J.*, vol. 12, no. 2, pp. 2027–2038, Jun. 2018.

[3] H. Xiong, Q. Mei, and Y. Zhao, "Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments," *IEEE Syst. J.*, to be published. doi: 10.1109/JSYST.2018.2890126.

[4] C. M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for Internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019. doi: 10.1109/ACCESS.2019.2891105.

[5] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. S. Shen, "Providing task allocation and secure deduplication for mobile crowdsensing via fog computing," *IEEE Trans. Dependable Secure Comput.*, to be published. doi: 10.1109/TDSC.2018.2791432.

[6] D. Wu, J. Yan, H. Wang, D. Wu, and R. Wang, "Social attribute aware incentive mechanism for device-to-device video distribution," *IEEE Trans. Multimedia*, vol. 19, no. 8, pp. 1908–1920, Aug. 2017.

[7] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, "User centric three-factor authentication protocol for cloud-assisted wearable devices," *Int. J. Commun. Syst.*, vol. 32, no. 6, p. e3900, Apr. 2019. doi: 10.1002/dac.3900.

[8] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 76, pp. 37–48, Dec. 2016.

[9] H. Xiong, H. Zhang, and J. Sun, "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing," *IEEE Syst. J.*, to be published. doi: 10.1109/JSYST.2018.2865221.

[10] S. Rane, Y. Wang, S. Drape, and P. Ishwar, "Secure biometrics: Concepts, authentication architectures, and challenges," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 51–64, Sep. 2013.

[11] P. S. Sudhish, A. K. Jain, and K. Cao, "Adaptive fusion of biometric and biographic information for identity de-duplication," *Pattern Recognit. Lett.*, vol. 84, pp. 199–207, Dec. 2016.

[12] A. K. Jain and K. Nandakumar, "Biometric authentication: System security and user privacy," *Computer*, vol. 45, no. 11, pp. 87–92, Nov. 2012.

[13] T. Ignatenko and F. M. J. Willems, "Information leakage in fuzzy commitment schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 337–348, Jun. 2010.

[14] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, and J. Tian, "An effective biometric cryptosystem combining fingerprints with error correction codes," *Expert Syst. Appl.*, vol. 39, no. 7, pp. 6562–6574, Jun. 2012.

[15] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognit. Lett.*, vol. 79, pp. 80–105, Aug. 2016.

[16] S. Barman, D. Samanta, and S. Chattopadhyay, "Fingerprint-based cryptobiometric system for network security," *EURASIP J. Inf. Secur.*, vol. 1, no. 3, 2015. doi: 10.1186/s13635-015-0020-1.

[17] K. Cao and A. K. Jain, "Learning fingerprint reconstruction: From minutiae to image," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 104–117, Jan. 2015.

[18] A. K. Jain, S. S. Arora, K. Cao, L. Best-Rowden, and A. Bhatnagar, "FingeFingerprint recognition of young children," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1501–1514, Jul. 2017. doi: 10.1109/TIFS.2016.2639346.

[19] T. Chugh, K. Cao, and K. Anil Jain, "Fingerprint spoof buster: Use of minutiae-centered patches," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2190–2202, Sep. 2018. doi: 10.1109/TIFS.2018.2812193.

[20] K. Cao and A. K. Jain, "Automated latent fingerprint recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 4, pp. 788–800, Apr. 2018. doi: 10.1109/TPAMI.2018.2818162.

[21] T. Chugh, K. Cao, J. Zhou, E. Tabassi, and A. K. Jain, "Latent fingerprint value prediction: Crowd-based learning," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 20–34, Jan. 2018. doi: 10.1109/TIFS.2017.2721099.

[22] B. Tams, P. Mihăilescu, and A. Munk, "Security considerations in minutiae-based fuzzy vaults," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 985–998, May 2015.

[23] W. Yang, J. Hu, and S. Wang, "A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 7, pp. 1179–1192, Jul. 2014.

[24] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 88–100, Sep. 2015.

[25] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur.*, pp. 28–36, Nov. 1999.

[26] W.-B. Zhong, X.-B. Ning, and C.-J. Wei, "A fingerprint matching algorithm based on relative topological relationship among minutiae," in *Proc. Int. Conf. Neural Netw. Signal Process. (ICNNSP)*, Jun. 2008, pp. 225–228.

[27] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, Nov. 2004.

[28] H. Hasan and S. Abdul-Kareem, "Fingerprint image enhancement and recognition algorithms: A survey," *Neural Comput. Appl.*, vol. 23, no. 6, pp. 1605–1610, Nov. 2013.

[29] J. Zhou, F. Chen, and J. Gu, "A novel algorithm for detecting singular points from fingerprint images," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 7, pp. 1239–1250, Jul. 2009.

[30] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 8, pp. 777–789, Aug. 1998.

[31] *The Fingerprints Used Here are From the Standard Database FVC 2004*. Accessed: 2004. [Online]. Available: http://bias.csr.unibo.it/fvc2004/download.asp

SHA SHI received the B.E. degree in telecommunication engineering and the M.S. degree in application mathematics from XiDian University, in 2003 and 2007, respectively. She received the Ph.D. degree in computer science and technology from the Beijing University of Posts and Telecommunications, in 2012.

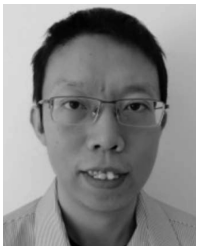
From 2008 to 2009, she was an Engineer with the 52th Institute of China Electronics Technology Group Corporation, Hang Zhou, Zhejiang, China. From 2012 to 2013, she was a Research Consultant with Siemens Corporate Technology. Since 2013, she has been a Lectureship with the Biomedical Engineering Department, School of Life Science and Technology, Xidian University. Her research interests include information security, biometric encryption, and the Internet of Things.

JIA CUI received the M.S. degree in information system from Nanyang Technological University, Singapore, in 2008. Since 2009, she has been an Engineer with the National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing, China. Her research interest includes information security, big data, the Internet of Things, and artificial intelligence.

XIN-LI ZHANG received the B.S. degree in life and medical science from Xinxiang Medical University, in 2004, where he is currently pursuing the master's degree. From 2004 to 2015, he was a Doctor with the Second People Hospital of Xinxiang, Henan, China. From 2015 to 2019, he was a Doctor with AIER EYE Hospital, Henan. His research interest includes biomedical engineering, bioinformatics based on eyes, and iris-based identity authentication.

YANG LIU received the B.S. degree in electronics and the applications of computer from Jilin University, in 2000, the M.S. degree in computer science and technology from the Beijing University of Posts and Telecommunications, in 2006, and the Ph.D. degree in information security from the Institute of information engineering, CAS, in 2018.

He is currently a Senior Engineer with the National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing, China. His research interest includes information security, big data, the Internet of Things, and artificial intelligence.



JING-LIANG GAO was born in Shandong, China, in 1983. He received the B.E. degree in electrical and information engineering, the M.S. degree, and the Ph.D. degree in information and communication engineering from Xidian University, China, in 2006, 2011, and 2015, respectively.

From 2015 to 2018, he was a Postdoctoral Researcher with the State Key Laboratory of Integrated Services Networks, Xi'an, China. Since 2018, he has been an Assistance Professor with the School of Telecommunication Engineering, Xidian University, Xi'an. His research interests include information theory, the Internet of Things, and artificial intelligence.

YUN-JIANG WANG received the B.E. degree in computer science and technology, the M.S. degree in optical engineering, and the Ph.D. degree in telecommunication and information system from Xidian University, China, in 2003, 2006, and 2010, respectively.

Since 2010, he was an Assistant Professor with the State Key Laboratory of Integrated Services Network (ISN), Xidian University, and been an Associate Professor, in 2012. His research interests include information theory, the Internet of Things, artificial intelligence, and quantum computing.