Hindawi
Security and Communication Networks
Volume 2018, Article ID 4519548, 9 pages
https://doi.org/10.1155/2018/4519548

Research Article

Iris Template Protection Based on Local Ranking

Dongdong Zhao, Shu Fang, Jianwen Xiang, Jing Tian, and Shengwu Xiong

Hubei Key Laboratory of Transportation Internet of Things, School of Computer Science and Technology, Wuhan University of Technology, Wuhan, Hubei, China

Correspondence should be addressed to Jianwen Xiang; jwxiang@whut.edu.cn

Received 29 September 2017; Accepted 21 January 2018; Published 18 February 2018

Academic Editor: Kai Cao

Biometrics have been widely studied in recent years, and they are increasingly employed in real-world applications. Meanwhile, a number of potential threats to the privacy of biometric data arise. Iris template protection demands that the privacy of iris data should be protected when performing iris recognition. According to the international standard ISO/IEC 24745, iris template protection should satisfy the irreversibility, revocability, and unlinkability. However, existing works about iris template protection demonstrate that it is difficult to satisfy the three privacy requirements simultaneously while supporting effective iris recognition. In this paper, we propose an iris template protection method based on local ranking. Specifically, the iris data are first XORed (Exclusive OR operation) with an application-specific string; next, we divide the results into blocks and then partition the blocks into groups. The blocks in each group are ranked according to their decimal values, and original blocks are transformed to their rank values for storage. We also extend the basic method to support the shifting strategy and masking strategy, which are two important strategies for iris recognition. We demonstrate that the proposed method satisfies the irreversibility, revocability, and unlinkability. Experimental results on typical iris datasets (i.e., CASIA-IrisV3-Interval, CASIA-IrisV4-Lamp, UBIRIS-V1-S1, and MMU-V1) show that the proposed method could maintain the recognition performance while protecting the privacy of iris data.

1. Introduction

In recent years, an increasing number of real-world applications employ biometrics for identification and authentication. Compared with passwords, biometrics have some advantages; for example, people do not need to remember biometric data and biometrics are difficult to forge. However, biometrics also have some specific security/privacy issues. For example, because the main part of biometrics keeps stable during the life of a person, once the biometric data are disclosed, it is infeasible to revoke the biometric data and publish new data. According to the international standard ISO/IEC 24745 [1], biometric template protection should satisfy the irreversibility, revocability, and unlinkability. Irreversibility demands that it is difficult to recover the original biometric data from the template used for recognition; revocability demands that a new biometric template can be issued for recognition once a template is leaked; unlinkability demands that the biometric templates from different applications cannot be used for cross-matching; that is, attackers cannot determine whether the templates are from the same person. The difficulty in realizing biometric template protection is to achieve fuzzy recognition while protecting the privacy of biometric data, because biometric data usually vary in a small part due to some reasons like aging and device errors.

Iris biometric is one of the most important biometrics, and iris template protection has been widely studied in the past decade. Presently, many methods have been proposed for iris template protection. Existing iris template protection methods could be divided into two classes: iris biometric cryptosystem and cancelable iris biometric [2]. In iris biometric cryptosystem, keys are used to encrypt the iris data, and error-correcting codes are usually employed for fuzzy recognition. Iris biometric cryptosystem can be further divided into key-binding cryptosystem and key-generation cryptosystem depending on the way of generating keys. In the key-binding cryptosystem, keys are generated independently from the iris data. In the key-generation cryptosystem, keys are generated from or based on the iris data. Cancelable iris biometrics are mainly based on noninvertible transforms, which should maintain the similarity evaluation in the transformed domain. However, it is demonstrated that, in recent

years, many existing methods for iris template protection could not satisfy the irreversibility, revocability, and unlinkability simultaneously, while maintaining the recognition performance [2–4].

In this paper, we propose a method for iris template protection based on local ranking. Specifically, first, the original iris data are XORed with an application-specific string; second, the obtained result is divided into blocks; third, we partition the blocks into groups, and the blocks in each group are sorted according to their decimal values (we call this procedure as local ranking); Finally, the data in each block are replaced with the corresponding rank value. We further extend the proposed method to support two important strategies (shifting and masking) to enhance the recognition performance. We demonstrate that the proposed method satisfies the irreversibility, revocability, and unlinkability. Experimental results show that the proposed method could effectively maintain the recognition performance on typical iris datasets (i.e., CASIA-IrisV3-Interval [5], CASIA-IrisV4-Lamp [5], UBIRIS-V1-S1 [6], and MMU-V1 [7]) while preserving data privacy.

The rest of this paper is organized as follows. Section 2 introduces the related work, and Section 3 presents the proposed method. The security and efficiency of the proposed method are analyzed in Section 4. Experimental results are shown in Section 5. We conclude this work in Section 6.

2. Related Work

To support fuzzy iris recognition while protecting data privacy, existing methods mainly use the following techniques: fuzzy commitment [8], fuzzy vault [9], fuzzy extractor/fuzzy sketches [10, 11], biohashing [12–14], Bloom filter [15], and noninvertible transforms [16–19].

Specifically, Hao et al. used the fuzzy commitment to construct an iris biometric cryptosystem in [20]. To support fuzzy recognition, they used Hadamard and Reed-Solomon error-correcting codes in the fuzzy commitment, and, then, a biometric key is used to "encrypt" biometric data. However, it was demonstrated in [21] that data privacy could be leaked in the fuzzy commitment scheme. In [22], Kelkboom et al. demonstrated that the fuzzy commitment scheme could suffer from a decodability attack based cross-matching [23]. They also proposed an improved version of the fuzzy commitment scheme to prevent the cross-matching. In [24], Rathgeb and Uhl presented a statistical attack on the fuzzy commitment scheme, and they demonstrated that cryptographic keys could be retrieved easily and the privacy of iris data would be disclosed.

In [25], Lee et al. employed the fuzzy vault scheme to iris template protection, and they constructed an iris biometric cryptosystem. They applied a pattern clustering method to realize fuzzy iris recognition. However, it was demonstrated in [26–28] that the fuzzy vault scheme might disclose original iris data and is fragile to the cross-matching attack.

In [29], Álvarez et al. proposed an iris template protection scheme based on the fuzzy extractor. They used helper data to eliminate noises data and support fuzzy recognition. A random string is extracted from the iris data through the fuzzy extractor and it is used for recognition. Bringer et al. [30] attempted to extract optimal secure sketches to protect data privacy for a given iris database. However, Blanton and Aliasgari [31] pointed out that existing fuzzy extractor constructions suffer from security problems such as privacy leakage and cross-matching when multiple sketches of an iris are disclosed.

Biohashing was proposed for human authentication in [12], and there are several improved versions such as [13, 14]. In biohashing, a tokenised random number and biometric data are used as two factors to support effective recognition. The privacy of biometric data could be protected by iterated inner products and binary discretization. However, it was pointed out in [14, 32] that the recognition performance is poor when the tokenised random number is stolen. Moreover, it was shown in [33, 34] that an inverse operation and preimage attacks could be performed on biohashing.

Cancelable biometrics are mainly based on noninvertible transforms. Zuo et al. [16] proposed two noninvertible transforms for iris template protection. They used random shifting, XOR operation and salting to transform and protect iris data. In [17], Hämmerle-Uhl et al. applied two noninvertible transforms called block remapping and image warping in the image domain prior to iris feature extraction. Pillai et al. [18] used random protection and sparse representation to realize noninvertible transform. Ouda et al. [35] proposed a cancelable iris biometrics scheme which does not require any tokenised random number. Rathgeb et al. [15] proposed to use Bloom filters to eliminate local location relationship in iris data and realize the noninvertible transform. However, it was demonstrated in [36, 37] that the iris template protection scheme based on Bloom filters cannot satisfy the unlinkability. Afterward, a permutation strategy is embedded to the iris template protection scheme based on Bloom filters to prevent cross-matching and achieve the unlinkability in [38]. In [39], Lai et al. proposed a cancelable iris biometric based on the Indexing-First-One (IFO) hashing, which is inspired by the Min-hashing. They employed the P-order Hadamard product and modulo threshold function in IFO hashing to realize noninvertible transform.

Though a large number of methods for iris template protection have been proposed, many of them cannot satisfy the irreversibility, revocability, and unlinkability simultaneously while maintaining the recognition performance [2–4]. Therefore, we propose an iris template protection method based on local ranking, which satisfies the irreversibility, revocability, and unlinkability while maintaining the recognition performance.

3. The Proposed Method

In this section, the iris template protection method based on local ranking is presented. Moreover, the proposed method is extended to support the shifting and masking strategies.

3.1. Transformation. To protect the original iris data, we transform the data into templates by the proposed method as illustrated in Figure 1. Specifically, for any iris data x (denoted

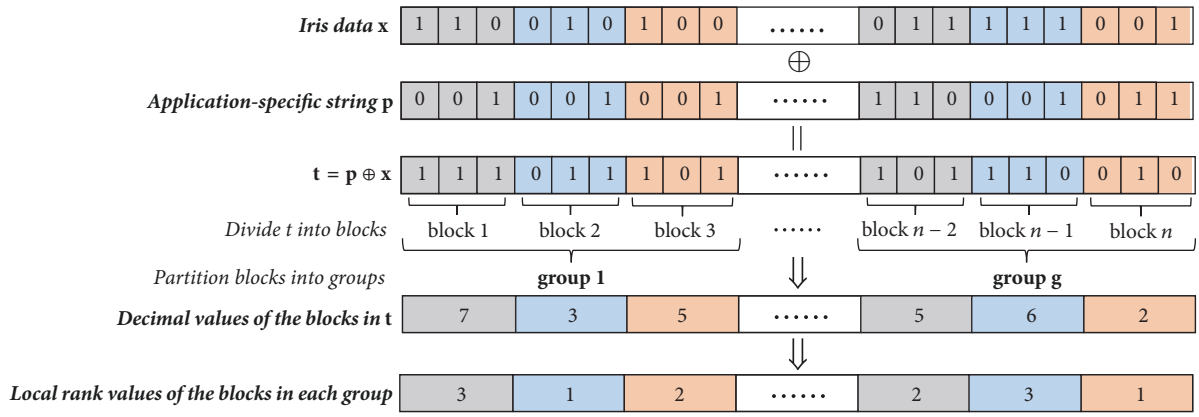


Figure 1: An illustration of the proposed method (block size and group size are 3).

as an m-bit string for simplicity) and an m-bit application-specific string p, the following process is conducted:

(1) Convert x to t: for $i = 1 \cdots m$:

$$t_i = x_i \oplus p_i, \tag{1}$$

where $\oplus$ is the Exclusive OR operation.

(2) Convert t to u by dividing t into n blocks: $u = u_1 \cdots u_n$, where each block has b bits; for example, $u_i = u_{i,1} \cdots u_{i,b}$ and $u_{i,j} = t_{(i-1)\times b+j}$ $(j = 1 \cdots b)$.

(3) Partition $u = u_1 \cdots u_n$ into g groups: $U = U_1 \cdots U_g$, where $U_i = \{u_{(i-1)\times d+1}, \ldots, u_{i\times d}\}$ for $i = 1 \cdots g$ where d is the group size and $n = g \times d$.

(4) For $i = 1 \cdots g$, sort the blocks $\{u_{(i-1)\times d+1}, \ldots, u_{i\times d}\}$ in U_i according to their decimal values $v_1, \ldots, v_d$. For $j = 1 \cdots d$:

$$v_j = \sum_{k=1}^{b} u_{(i-1)\times d+j,k} \times 2^{b-k}. \tag{2}$$

Obtain the rank values of $v_1, \ldots, v_d$ and denote them as $r_{(i-1)\times d+1}, \ldots, r_{i\times d}$ (corresponding to $u_{(i-1)\times d+1}, \ldots, u_{i\times d}$).

(5) Store $r_{(i-1)\times d+1}, \ldots, r_{i\times d}$ for $i = 1 \cdots g$ as the template, delete x, t, u, U, and v.

Note that when sorting $v_1, \ldots, v_d$, if two values v_i and v_j are the same, they will be compared according to their index values, that is, i and j. In the above method, the original iris data are protected because only the rank values are stored and the original iris data are deleted. We will demonstrate in Section 4 that it is difficult to infer the original iris data from the rank values.

In recognition, the distance/dissimilarity between any two templates $r = r_1 \cdots r_n$ and $r' = r'_1 \cdots r'_n$ (which are converted by the proposed method from two iris data x and x', resp.) can be calculated as follows:

$$\mathrm{Dis}\left(r, r'\right) = \sum_{i=1}^{n} \left|r_i - r'_i\right|. \tag{3}$$

3.2. Shifting. In traditional iris recognition system, shifting strategy is usually used for handling the noise caused by improper head rotation [40]. In this strategy, iris data are usually circularly shifted by certain bits, and the minimal distance is chosen for recognition. Suppose we want to conduct the shifting by $2 \times sn + 1$ times, and $w \times (-sn), \ldots, w \times (-1), 0, w \times 1, \ldots, w \times sn$ bits will be circularly shifted, respectively. We use $\mathrm{Dis}(x, x')$ to denote the function for calculating the distance between two iris data x and x' without using the shifting strategy and use $\mathrm{Dis}^{\mathrm{shift}}(x, x')$ to denote the distance when using the shifting strategy. Without considering data privacy, $\mathrm{Dis}^{\mathrm{shift}}(x, x')$ can be calculated as follows [40]:

$$\mathrm{Dis}^{\mathrm{shift}}\left(x, x'\right) = \min_{i=-sn}^{sn}\left(\sum_{j=1}^{m} \mathrm{Dis}\left(x^{\underline{i}}, x'\right)\right), \tag{4}$$

where $x^{\underline{i}}$ denotes the string obtained by circularly shifting x with $w \times i$ bits.

In some scenarios, the shifting strategy could be conducted at the user side (a user is a person who submits his iris data to an application server for authentication/recognition in order to use server resources). In such case, the shifting strategy can be simply carried out in the above way without any change. For example, some traditional iris systems (e.g., OSIRIS-V4.1 [41, 42]) employ application points set to enhance the recognition performance and reduce the computational/communication cost. The string length of iris data usually can be significantly reduced; for example, the iris data are reduced from 196608 bits to 1536 bits in OSIRIS-V4.1. If the iris data are only required to be shifted by a few times (i.e., sn is small, e.g., $sn < 50$), it is better to conduct the shifting strategy at the user side instead of the server side, because the communication cost will be lower if the user sends the shifted strings instead of the original long iris data and the computational cost at the server side is also lower. In the proposed method, the user will generate a template for each shifted string and send the sets of templates to the server. Suppose the templates are denoted as $r^{\underline{1}}, \ldots, r^{\underline{sn}}$ (where $r^{\underline{i}}$ is

the template generated by our method from $x^{\underline{i}}$); then, for a real-time template r' converted from x', we have

$$\mathrm{Dis}^{\mathrm{shift}}\left(r, r'\right) = \min_{i=-sn}^{sn}\left(\mathrm{Dis}\left(r^{\underline{i}}, r'\right)\right). \tag{5}$$

If the shifting strategy should be conducted at the server side (which provides authentication/recognition service and application resources to users) due to some reasons such that the user side has low computational ability and sn is large, then we should extend the proposed method to support the shifting strategy while protecting data privacy. In this case, the user only sends one template r which is generated from his original iris data x. To effectively support the shifting strategy, the proposed method would satisfy the following: w is a multiple of the block size b. Without loss of generality, we assume $w = b \times c$. For any two templates r and r', $\mathrm{Dis}^{\mathrm{shift}}(r, r')$ can also be calculated by (5), but $r^{\underline{i}}$ is obtained by circularly shifting r with $i \times c$ blocks at the server side.

3.3. Masking. The captured iris images often have some noises caused by foreseeable errors or device defects, and these noises could be marked by a masking code [40]. By the masking code, we could extract iris data without the noises for recognition. For two iris strings x and x', suppose their masking codes are mask$x$ and maskx', respectively, and the noise at each bit is marked as 0. Then, in traditional iris recognition systems, the similarity between x and x' when using the masking strategy can be calculated as follows [40]:

$$\mathrm{Dis}^{\mathrm{mask}}\left(x, x'\right) = \frac{m}{\mathrm{maskLen}} \times \mathrm{Dis}\left(y, y'\right), \tag{6}$$

where y, y' denote the bits of x, x' at which both mask$x$ and maskx' are 1, respectively. And, maskLen is the number of bits at which both mask$x$ and maskx' are 1, that is, $\mathrm{maskLen} = \sum_{i=1}^{m} \mathrm{mask}x_i \wedge \mathrm{mask}x'_i$.

In the proposed method, the iris data x (and x') is divided into blocks, and the final template r (and r') contains only the ranks of the blocks. To judge whether a rank could be used for recognition, we should also divide the masking code mask$x$ (and maskx') into blocks and calculate mask$r$ (and maskr') as follows:

$$\mathrm{mask}r_i = \begin{cases} 1 & \sum_{j=(i-1)\times b+1}^{i\times b} \mathrm{mask}x_j > 0 \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

The distance between r and r' when using the masking strategy can be calculated as follows:

$$\mathrm{Dis}^{\mathrm{mask}}\left(r, r'\right) = \frac{n}{\mathrm{maskLen}} \times \mathrm{Dis}\left(y, y'\right), \tag{8}$$

where $\mathrm{maskLen} = \sum_{i=1}^{n} \mathrm{mask}r_i \wedge \mathrm{mask}r'_i$, and y, y' denote the values of r, r' at the positions that mask$r$ and maskr' are 1. If $\mathrm{maskLen} = 0$, $\mathrm{Dis}^{\mathrm{mask}}(r, r')$ is forced to a large value which results in an unmatching.

If we want to use the shifting strategy together with the masking strategy, then the distance between r and r' can be calculated as follows:

$$\mathrm{Dis}^{\mathrm{shift+mask}} = \min_{i=-sn}^{sn}\left(\mathrm{Dis}^{\mathrm{mask}}\left(r^{\underline{i}}, r'\right)\right). \tag{9}$$

4. Security and Efficiency

We demonstrate that the proposed method satisfies the irreversibility, revocability, and unlinkability in this section. Note that all the security analyses are under a rigorous assumption that the attacker has known the application-specific string p. Moreover, we also analyze the efficiency of the proposed method.

4.1. Irreversibility. To satisfy the irreversibility, attackers should be unable to recover the original iris data x from the template r used for recognition. In the proposed method, the original iris data x are converted to a string of rank values. The concrete information at each bit of x could not be recovered from the rank values. Specifically, for any group $U_i = \{u_{(i-1)\times d+1}, \ldots, u_{i\times d}\}$, it has been converted to a group of decimal values $v_1, \ldots, v_d$, and, then, the group of decimal values are converted to a list of rank values $r_{(i-1)\times d+1}, \ldots, r_{i\times d}$. Without loss of generality, we assume $v_1, \ldots, v_d$ are sorted from the smallest to the largest. If the attacker can recover $v_1, \ldots, v_d$ from $r_{(i-1)\times d+1}, \ldots, r_{i\times d}$, then he can also recover the corresponding original iris data in x, and vice versa.

Given $r_{(i-1)\times d+1}, \ldots, r_{i\times d}$, suppose the number of possible $v_1, \ldots, v_d$ that can be mapped to $r_{(i-1)\times d+1}, \ldots, r_{i\times d}$ is denoted as $f(d, 2^b)$ (where b is the block size and 2^b is the number of available values for v_d); then we have

$$f\left(d, 2^b\right) = \sum_{j=1}^{2^b} f\left(d-1, j\right). \tag{10}$$

This formula is obtained by fixing the value of v_d as $0, \ldots, 2^b - 1$, resulting in $f(d-1, 1), \ldots, f(d-1, 2^b)$, respectively. The initial conditions are $f(1, 1) = 1, f(1, 2) = 2, \ldots, f(1, 2^b) = 2^b$ and $f(d, 1) = 1, f(d-1, 1) = 1, \ldots, f(1, 1) = 1$. After solving (10), we have

$$f\left(d, 2^b\right) = \binom{2^b + d - 1}{d}. \tag{11}$$

Given a template r, the number of possible iris data that can be mapped to r is

$$G = \left(f\left(d, 2^b\right)\right)^g = \binom{2^b + d - 1}{d}^{m/(b\times d)}. \tag{12}$$

In practice, d is usually set to an integer between 2 and 64, and b is usually set to an integer between 1 and 8. It is shown in Section 5.5 that the minimal value of G is larger than 2^{144} at the worst case in Table 4 (it contains the results for all common settings of parameters d and b), that is, $d = 64$ and $b = 1$. Moreover, it is also shown in Section 5.5 that we can adjust the irreversibility by b and d according to our security requirement. Therefore, we conclude that the proposed method satisfies the irreversibility.

4.2. Revocability. Once the iris template used for recognition is leaked, the iris template protection method should be able

to revoke the leaked template and reissue a new template for recognition. In the proposed method, the revocability can be easily realized by using a new application-specific string p. Specifically, the server, which provides the iris recognition service, can delete the leaked template and generate a new p for the corresponding user. Next, the server asks the user to resubmit a template (which is generated using the new p) for recognition. Note that the new application-specific string is only used for the users whose templates are leaked, and other users keep using the old application-specific string to avoid extra enrollments. For the user whose template is leaked, the old template cannot be used for recognition anymore because his application-specific string is updated and it is difficult to perform the cross-matching between the old template and the new template (guaranteed by the unlinkability). Therefore, we conclude that the proposed method satisfies the revocability.

4.3. Unlinkability. To satisfy the unlinkability, different templates from different applications/servers cannot be used for cross-matching; in other words, attackers cannot determine whether two templates from different applications correspond to the same user. We will analyze the unlinkability of the proposed method under a rigorous assumption that the two templates r, r' from different applications are from the same iris data x. The two applications use two different application-specific strings, that is, p and p'. Because p and p' are randomly generated, $t = x \oplus p$ and $t' = x \oplus p'$ can also be regarded as two random strings. Hence, the decimal values of t and t' are independent from each other, and finally the rank values r and r' are also independent from each other. It means that the distance (refer to (3), (5), (8), and (9)) between r and r' would not be smaller than the distances between two templates generated from different irises.

Furthermore, it is demonstrated in Section 5.6 that the distribution of the intraclass distances is quite similar to the distribution of the interclass distances when performing the cross-matching. It indicates that attackers cannot determine whether the cross-matching between r and r' is intraclass or interclass, and, thus, they cannot determine whether r and r' are from the same user. Therefore, we conclude that the proposed method satisfies the unlinkability.

4.4. Efficiency. According to Section 3.1, the computational complexity of step 1 is $O(m)$, where m is the string length of iris data. Step 2 divides t into blocks and step 3 partitions the blocks into groups, and, thus, the computational complexity is $O(m)$. Step 4 sorts the blocks in each group according to their decimal values. If the merge sorting algorithm is used, the computational complexity is $O(d \times \log(d) \times (m/d)) = O(m \times \log(d))$. The computational complexity of step 5 is $O(m)$. Overall, the computational complexity of the proposed method in Section 3.1 is $O(m \times \log(d))$. In practice, d is usually set to an integer less than 64, and it can be regarded as a constant; therefore, the computational complexity of the proposed method is $O(m)$. When using the shifting strategy, obviously, the computational complexity becomes $O(m \times sn)$. Masking strategy will not increase the computational complexity of the proposed method, and, in contrast, it usually decreases the string length of templates in recognition. Consequently, the computational complexity of the proposed method is the same to the original iris recognition system (without privacy protection), and we conclude that the proposed method is efficient.

5. Experimental Results and Discussion

In this section, we present the experimental results of the proposed method on the iris datasets CASIA-IrisV3-Interval [5], CASIA-IrisV4-Lamp [5], UBIRIS-V1-S1 [6], and MMU-V1 [7]. Moreover, we also show the results about the irreversibility and unlinkability of the proposed method.

5.1. Experiment Setup. In this paper, we mainly focus on the protection of iris data, and we employ a sophisticated iris processing system called OSIRIS-V4.1 [41, 42] for iris localization, normalization, and converting iris images to binary strings. After obtaining the binary strings of iris images, our method is used to convert the strings to templates. In the following experiments, the iris dataset CASIA-IrisV3-Interval is used as default, and, similar to [15], only the iris images from left eyes are used.

Specifically, all iris strings will be converted to templates, but only one template is chosen as the enrolled data of the valid user in each test. All templates will be compared with the chosen template. The comparison between the templates from the chosen user is intraclass matching, and the comparison between the templates from other users and the chosen template is interclass matching. Each iris will be regarded as the valid user in a test in turn, and an iris image of this user is randomly chosen for enrollment. Application-specific strings are randomly generated binary strings with the same length to the iris strings. Each test will be conducted 30 times by default, and, after processing all irises, we obtain the Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR), and Equal Error Rate (EER), which are three widely used metrics for evaluating the recognition performance.

5.2. Using Shifting and Masking Strategies. In this experiment, we investigate the effectiveness of the shifting and masking strategies on the recognition performance of the proposed method, and we use the CASIA-IrisV3-Interval dataset. OSIRIS-V4.1 should employ a set of application points after using the shifting strategy, and it converts the original binary iris string from 196608 bits to 1536 bits. Similar to [15], sn is set to 8 and w is set to 384. According to Section 3.2, it is better to conduct the shifting strategy at the user side, and the shifted templates are generated and then sent to the server. The server will calculate the distance between templates. The masking strategy will be performed at the server side on the templates. Other parameters are set as $b = 2$, $d = 8$, $g = m/(b \times d) = 96$.

As shown in Table 1, the GAR of the proposed basic method (without using the shifting or masking strategy) is 87.51%, 84.20%, and 80.84% for FAR = 1%, 0.1%, and 0.01%, respectively, and the EER is 8.43%. After using the shifting strategy, the GAR is enhanced to 98.58%, 97.84%, and 96.85% for FAR = 1%, 0.1%, and 0.01%, respectively, and the EER is enhanced to 1.36%. It indicates that the shifting strategy is effective to the proposed method. Moreover, by using the

Table 1: The influence of the shifting and masking strategies on the recognition performance of the proposed method.

Methods	GAR(%)			EER(%)
	FAR = 1%	FAR = 0.1%	FAR = 0.01%	
Basic method	87.51	84.20	80.84	8.43
Basic method + shift	98.58	97.84	96.85	1.36
Basic method + shift + mask	*98.64*	*98.07*	*97.00*	*1.32*

Table 2: The GAR (when FAR = 0.01%) of the proposed method using different b and d.

b	d					
	2	**4**	**8**	**16**	**32**	**64**
1	93.18	97.05	97.81	97.93	**98.07**	**98.11**
2	88.60	95.50	97.00	97.50	97.56	97.62
4	66.34	87.46	93.03	94.48	95.35	95.54
8	39.80	64.13	76.76	82.05	85.33	86.53

Table 3: The GAR (%) (when FAR = 0.01%) and EER (%) of the proposed method (with $b = 1, d = 64$) and OSIRIS-V4.1 on different datasets.

Dataset	OSIRIS-V4.1	Proposed method
CASIA-IrisV3-Interval	**98.24/1.01**	98.11/1.06
CASIA-IrisV4-Lamp	**79.95/4.90**	79.07/5.0
UBIRIS-V1-S1	67.27/**13.06**	**67.63**/13.44
MMU-V1	75.42/5.64	**76.17/5.50**

shifting strategy together with the masking strategy, the GAR is further enhanced to 98.64%, 98.07%, and 97.00% for FAR = 1%, 0.1%, and 0.01%, respectively, and the EER is enhanced to 1.32%. Therefore, the shifting and masking strategies are effectively supported by the proposed method.

5.3. Varying Group Size and Block Size. In this experiment, we investigate the influence of the group size d and the block size b on the recognition performance of the proposed method, and we use the CASIA-IrisV3-Interval dataset. The shifting and masking strategies are always used in this experiment, and parameter settings are the same as those in Section 5.2. The block size b is set to 1, 2, 4, and 8, respectively, and the group size d is set to 2, 4, 8, 16, 32, and 64, respectively. Without loss of generality, we present the GAR value at FAR = 0.01% to evaluate the performance of the proposed method.

As shown in Table 2, the recognition performance of the proposed method increases with the increase of d. The reason might be that the rank values obtained under a larger d are more correlative to the actual decimal values of the original iris data, and they contain more useful information for recognition. It is also shown in Table 2 that the recognition performance of the proposed method decreases with the increase of b. A larger b will be induced to a lower correlation between the rank values and the decimal values of original iris data, and, thus, less useful information is contained in the template and it leads to a lower recognition performance. It is also shown in Section 5.5 that larger b often results in higher irreversibility as more useful information about the original iris data is lost.

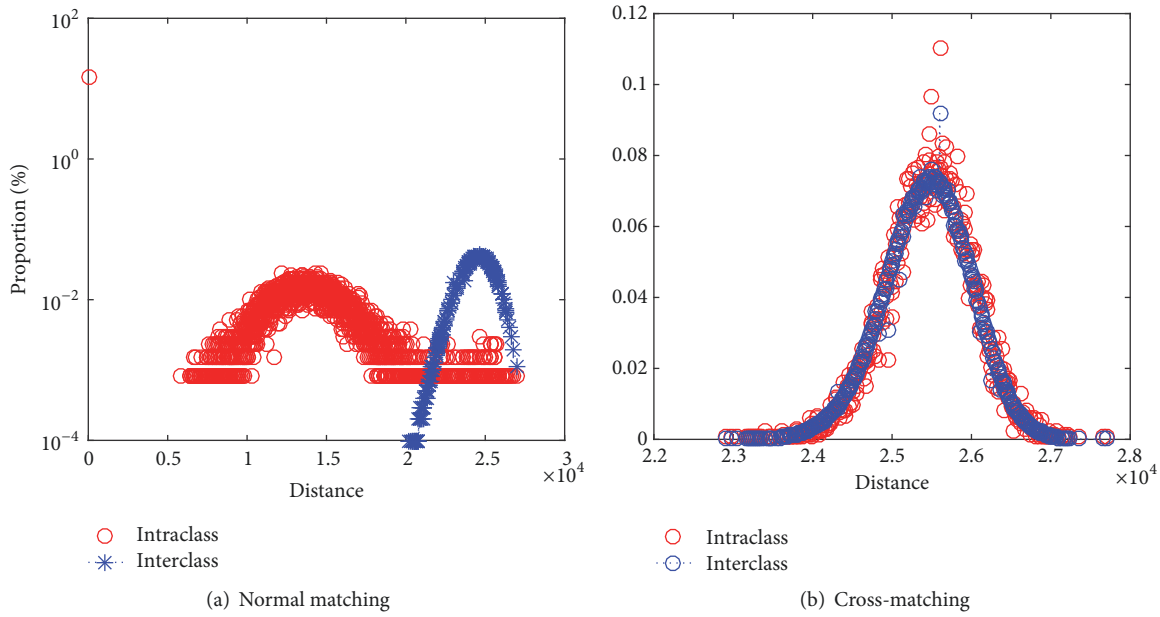
5.4. Using Different Datasets. In this part, we choose other three iris datasets to further check the effectiveness of our method, that is, CASIA-IrisV4-Lamp [5], UBIRIS-V1-Session 1 [6], and MMU-V1 [7]. The CASIA-IrisV4-Lamp dataset contains 16212 iris images from 411 subjects, and the images are captured under nonlinear deformation due to variations of visible illumination. We only use the iris data of left eyes in CASIA-IrisV4-Lamp. The UBIRIS-V1-Session 1 dataset contains 1214 iris images from 241 persons, and the images suffer from several noise factors under less constrained image acquisition environments. So it would be difficult for iris recognition system to achieve a high performance. The MMU-V1 dataset contains 450 images from 46 persons, and we use the iris data of both left eyes and right eyes due to its small size. In this experiment, b is set to 1 and d is set to 64, and both shifting (with $sn = 8$ and $w = 384$) and masking strategies are used.

As shown in Table 3, we compare the results of the proposed method with OSIRIS-V4.1 (the original iris recognition system without privacy protection). Note that OSIRIS-V4.1 fails to handle a few of iris images in CASIA-IrisV4-Lamp, UBIRIS-V1-Session 1, and MMU-V1 due to their poor quality, but this does not affect the comparison. After using our method in OSIRIS-V4.1, the GAR value on the CASIA-IrisV4-Lamp dataset is slightly decreased from 79.95% to 79.07%, and the EER value is slightly increased from 4.9% to 5.0%. On the UBIRIS-V1-Session 1 dataset, the GAR value obtained by using our method is 67.63%, and it is slightly better than that of OSIRIS-V4.1 (i.e., 67.27%). However, the EER value of our method is slightly worse than the EER value of OSIRIS-V4.1. On the MMU-V1 dataset, our method achieves better GAR and EER than OSIRIS-V4.1. Overall, the results of our method are quite close to those of OSIRIS-V4.1, and the recognition performance is maintained while providing privacy protection. These results demonstrate the effectiveness of our method.

5.5. Irreversibility. As analyzed in Section 4.1, G in (12) can be used to evaluate the irreversibility of the proposed method. Because G is too large to compute in programming, $\log_2 G$ is used instead of G. We present the values of $\log_2 G$ under the parameter settings $b = 1, 2, 4, 8$ and $d = 2, 4, 8, 16, 32, 64$ in Table 4. It is shown that the values of $\log_2 G$ increase with the increase of b. $\log_2 G$ also appears to quickly decrease with the increase of d. $\log_2 G$ has the best value at $d = 2$ and $b = 8$. In practice, we can adjust the value of G by b and d and control the irreversibility of the proposed method. For

Table 4: The values of $\log_2 G$ under different b and d.

b	d					
	2	**4**	**8**	**16**	**32**	**64**
1	1217.25	891.62	608.63	392.40	242.13	144.54
2	1275.62	984.82	707.17	476.18	304.23	186.57
4	1360.79	1144.35	907.36	675.91	473.41	313.56
8	**1440.54**	1317.54	1172.57	1012.95	846.14	679.58



(a) Normal matching (b) Cross-matching

Figure 2: The intraclass and interclass distribution of distances when $b = 1$ and $d = 64$.

all of the parameter settings in Table 4, the proposed method satisfies the irreversibility because the smallest G is larger than 2^{144}, and attackers cannot recover the original iris data from more than 2^{144} alternatives.

5.6. Unlinkability. In this part, we investigate the unlinkability of the proposed method on the CASIA-IrisV3-Interval dataset in the experiment. Specifically, first, we compare the distribution of the distances from intraclass matching with the distribution of distances from interclass matching in one application. Next, we compare the distribution of the distances from intraclass cross-matching with the distribution of distances from interclass cross-matching over two applications. In the second case, in each test, we select one iris string as the valid user in the 1st application, and the iris string is converted to a template r using a randomly selected application-specific string p by the proposed method. In the 2nd application, all iris strings are converted to templates $r'_1 \cdots r'_N$ using another randomly selected application-specific string p' by the proposed method. Next, r is compared with $r'_1 \cdots r'_N$, respectively, and the distances are recorded. The comparison between r and the templates in $r'_1 \cdots r'_N$ which are from the same iris as r is called intraclass cross-matching. The comparison between r and the templates in $r'_1 \cdots r'_N$ which are from different irises to r is called interclass cross-matching. Note that each iris will be selected as the valid user of the 1st application in a test in turn, and we will randomly select one image from the iris for enrollment (to be the valid user). In this experiment, the shifting and masking strategies are always used, and sn is set to 8. The experiment is conducted 100 times, and we count the times of matching that results in the same distance value. The results for $b = 1$ and $d = 64$ (this parameter setting achieves the best recognition performance in Table 2) are shown in Figure 2, and the y-axis represents the proportion of times of matching that results in each distance value. Similar phenomenon is found for other parameter settings, so we do not present their results here.

As shown in Figure 2(a), when performing normal matching in one application (i.e., the first case), the distribution for intraclass matching is quite different from the distribution for interclass matching. The points for intraclass matching mainly locate at the space Distance $< 2.2 \times 10^4$, and the points for interclass matching mainly locate at the space Distance $> 2.0 \times 10^4$. The distribution for intraclass matching overlaps with the distribution for interclass matching in a very small space, and this enables the proposed method to support effective iris recognition. Figure 2(b) shows the distributions for cross-matching. The distribution for intraclass cross-matching overlaps with the distribution for interclass cross-matching in a large space. When attackers perform a

cross-matching, they could not determine whether this matching is intraclass or interclass according to the matching result (i.e., the distance), and, thus, they could not determine whether the two templates are from the same user. Therefore, the proposed method satisfies the unlinkability. Figures 2(a) and 2(b) also demonstrate that the unlinkability is mainly achieved by using different application-specific strings.

6. Conclusion

In this paper, we propose a method for iris template protection. By the proposed method, original iris data are replaced with a string of local rank values. We extend the proposed method to support two important strategies (i.e., shifting and masking) to handle noises. Moreover, we demonstrate that the proposed method satisfies the irreversibility, revocability, and unlinkability. Furthermore, we show that the proposed method is as efficient (in the form of computational complexity) as the iris recognition system without privacy protection. Experimental results show that the proposed method could effectively maintain the recognition performance on several typical iris datasets while protecting data privacy.

In future work, we attempt to extend the proposed method to support some other widely used strategies in iris recognition. We will also improve the proposed method to support template protection for other biometrics.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China (Grant no. 61672398), the Key Natural Science Foundation of Hubei Province of China (Grant no. 2017CFA012), the Applied Fundamental Research of Wuhan (Grant no. 20160101010004), and the Fundamental Research Funds for the Central Universities of China (Grant no. 173110002).

References

[1] *Information Technology-Security Techniques-Biometric Information Protection. ISO/IEC JTC1 SC27 IS 24745*, 2011, http://www.iso.org/iso/catalogue_detail?csnumber=52946.

[2] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, article no. 3, pp. 1–25, 2011.

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

[4] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov, and J. Yearwood, "Protection of Privacy in Biometric Data," *IEEE Access*, vol. 4, pp. 880–892, 2016.

[5] *CASIA-IrisV3 and CASIA-IrisV4, Institute of Automation (IA, Chinese Academy of Sciences (CAS)*, 2017, http://biometrics.idealtest.org/.

[6] H. Proenca and L. A. Alexandre, "UBIRIS: A Noisy Iris Image Database," in *Proceedings of the 13th International Conference on Image Analysis and Processing - ICIAP 2005*, vol. LNCS 3617, pp. 970–977, Springer, Cagliari, Italy, 2005.

[7] "MMU Iris Image Database," http://pesona.mmu.edu.my/~ccteo/.

[8] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 1999 6th ACM Conference on Computer and Communications Security (ACM CCS)*, pp. 28–36, November 1999.

[9] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography. An International Journal*, vol. 38, no. 2, pp. 237–257, 2006.

[10] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 523–540, Springer, Berlin.

[11] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor, "Optimal iris fuzzy sketches," in *Proceedings of the 1st IEEE International Conference on Biometrics: Theory, Applications, and Systems, BTAS '07*, pp. 1–6, USA, September 2007.

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

[13] A. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognition*, vol. 40, no. 3, pp. 1057–1065, 2007.

[14] A. B. J. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on BioHash," *Pattern Recognition*, vol. 41, no. 6, pp. 2034–2044, 2008.

[15] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *Proceedings of the 6th IAPR International Conference on Biometrics, ICB 2013*, pp. 1–8, Spain, June 2013.

[16] J. Zuo, N. K. Ratha, and J. H. Connell, "Cancelable iris biometric," in *Proceedings of the 2008 19th International Conference on Pattern Recognition (ICPR)*, pp. 1–4, Tampa, FL, USA, December 2008.

[17] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *Proceedings of the the 12th International Conference on Information Security (ISC)*, pp. 135–142, Springer.

[18] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 9, pp. 1877–1893, 2011.

[19] D. Zhao, W. Luo, R. Liu, and L. Yue, "Negative iris recognition," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 112–125, 2015.

[20] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

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

[22] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis, "Preventing the decodability attack based cross-matching in a fuzzy commitment scheme," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 107–121, 2011.

[23] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches," in *Proceedings of the 30th IEEE Symposium on Security and Privacy*, pp. 188–203, May 2009.

[24] C. Rathgeb and A. Uhl, "Statistical attack against iris-biometric fuzzy commitment schemes," in *Proceedings of the 2011 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, CVPRW 2011*, USA, June 2011.

[25] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim, "Biometric key binding: Fuzzy vault based on iris images," in *Proceedings of the International Conference on Biometrics (ICB 2007)*, pp. 800–808, Springer, Berlin, Germany.

[26] E.-C. Chang, R. Shen, and F. W. Teo, "Finding the original point set hidden among chaff," in *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, ASIACCS '06*, pp. 182–188, Taiwan, March 2007.

[27] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Proceedings of the 2007 Biometrics Symposium, BSYM*, pp. 1–6, USA, September 2007.

[28] H. T. Poon and A. Miri, "A collusion attack on the fuzzy vault scheme," *International Journal of Information Security*, vol. 1, pp. 27–34, 2009.

[29] F. H. Álvarez, H. E. Luis, and S.-A. Carmen, "Biometric fuzzy extractor scheme for iris templates," in *Proceedings of the 2009 World Congress in Computer Science, Computer Engineering*, pp. 563–569, 2009.

[30] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor, "Theoretical and practical boundaries of binary secure sketches," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 673–683, 2008.

[31] M. Blanton and M. Aliasgari, "Analysis of reusability of secure sketches and fuzzy extractors," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1433–1445, 2013.

[32] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of BioHashing and its variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359–1368, 2006.

[33] Y. Lee, Y. Chung, and K. Moon, "Inverse operation and preimage attack on biohashing," in *Proceedings of the 2009 IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications, CIB 2009*, pp. 92–97, USA, April 2009.

[34] P. Lacharme, E. Cherrier, and C. Rosenberger, "Preimage attack on biohashing," in *In 2013 International Conference on Security and Cryptography (SECRYPT)*, pp. 1–8, July 2013.

[35] O. Ouda, N. Tsumura, and T. Nakaguchi, "Tokenless cancelable biometrics scheme for protecting iriscodes," in *Proceedings of the 2010 20th International Conference on Pattern Recognition, ICPR 2010*, pp. 882–885, Turkey, August 2010.

[36] J. Hermans, B. Mennink, and R. Peeters, "When a bloom filter is a doom filter: security assessment of a novel iris biometric template protection system," in *Proceedings of the In 2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp. 1–6, 2014.

[37] J. Bringer, C. Morel, and C. Rathgeb, "Security analysis of Bloom filter-based iris biometric template protection," in *Proceedings of the 8th IAPR International Conference on Biometrics, ICB 2015*, pp. 527–534, Thailand, May 2015.

[38] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, and J. Fierrez, "Unlinkable and irreversible biometric template protection based on bloom filters," *Information Sciences*, vol. 370/371, pp. 18–32, 2016.

[39] Y.-L. Lai, Z. Jin, A. B. Jin Teoh et al., "Cancellable iris template generation based on Indexing-First-One hashing," *Pattern Recognition*, vol. 64, pp. 105–117, 2017.

[40] L. Masek, *Recognition of human iris patterns for biometric identification [Master, thesis]*, University of Western Australia, 2003.

[41] E. Krichen, A. Mellakh, P. V. Anh, S. Salicetti, and B. Dorizzi, "A biometric reference system for iris," *OSIRIS Version*, vol. 4.1, 2013.

[42] N. Othman, B. Dorizzi, and S. Garcia-Salicetti, "OSIRIS: An open source iris recognition software," *Pattern Recognition Letters*, vol. 82, pp. 124–131, 2016.