IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 20, 2019, accepted August 25, 2019, date of publication August 28, 2019, date of current version September 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2938019

One-Factor Cancellable Palmprint Recognition Scheme Based on OIOM and Minimum Signature Hash

XIYU WANG AND HENGJIAN LI
School of Information Science and Engineering, University of Jinan, Jinan 250022, China
Corresponding author: Hengjian Li (hengjianli@gmail.com)

This work was supported by the Shandong Provincial Government Scholarship (2019).

ABSTRACT The traditional Cancellable biometrics scheme needs another key or token to generate the revocable template, which usually suffers from the token-stolen problem. To solve this problem, a one-factor cancellable palmprint biometric recognition scheme based on Orthogonal Index of Maximum (OIOM) hash and Minimum Signature Hash (MSH) is proposed to generate pseudonymous identifier. Firstly, to improve the efficiency and effectiveness, a parallel structure is designed to obtain Orthogonal Gaussian random projection(GRP)matrices, which is employed to generate the OIOM hash code. Secondly, a random binary string is XOR the binary OIOM hash code to construct the helper data and it is stored in the database. Meanwhile, this string is hashed by MSH to get the final pseudonymous identifier. Lastly, during matching stage, based on helper data and a palmprint images, another pseudonymous identifier is generated to recognition. This implies that, just one factor, a palmprint of user, is needed in the matching stage, and therefore the privacy of user is preserved. To evaluate the proposed scheme, PolyU database and touchless TJU database are used in experiments. The noninvertible, renewability, unlinkability and several security attacks of the proposed scheme are analyzed. The experiment results and analysis show that the proposed scheme has strong security on the basis of maintaining palmprint recognition performance.

INDEX TERMS Biometric recognition, cancellable palmprint feature, orthogonal index of maximum, minimum signature hash.

I. INTRODUCTION

In today's information society, biometric technology is becoming more and more popular. This has led to the emergence of a large number of biological templates. Although compared with traditional identification methods such as keys, passwords and ID cards, biometric recognition technology is more secure and convenient [1]. But if a large number of unprotected biometric templates are stored, various security issues and personal privacy issues will arise when these templates are attacked by opponents [2]. For example, when a biometric template is stolen by an opponent, he can pretend that you are doing some illegal activities. Furthermore, because every biometric feature of everyone is limited, once stolen, it will not be updated. Consequently, the protection of biometric templates is an urgent and crucial issue [3].

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

Palmprint, as one of the most important biological feature, is widely used for its advantages of convenient image acquisition and low cost of equipment. Compared with face, fingerprint and iris, palmprint has many characteristics and rich useful information, such as large area, wrinkles, main lines, rich texture and obvious orientation, which can be used to extract features and identify [4]. Although palmprint recognition has some of the advantages mentioned above, there are also security problems common to other biological features, that is, privacy disclosure [5]. Palmprint features do not change over time, and also contain some personal privacy issues. In light of these challenges and the concerns presented by the previous work, the privacy protection of palmprint must be considered in the process of palmprint recognition [6]. It is of great significance to study and create more robust and secure cancellable biometric recognition systems.

Biometric encryption is generally classified into two types: biometric cryptography and revocable authentication [7].

The fuzzy vault scheme [8] and the fuzzy Commitment scheme [9] belong to biometric cryptography. However, fuzzy vault schemes suffered from the drawback that majority of the data was stored in the open environment and lack of reusability [10]. The generation of cancellable biometric template is an important way to protect biometric templates [11]. Locality-sensitive hashing(LSH) is an algorithmic technique that hashes similar input items into the same ''buckets'' with high probability. Recently, LSH hash functions, such as projection random, winner take all hashing [12] and IFO [13], are used to protect the biometric feature for its privacy-preserving nearest neighbor property. Based on projection random and winner take all hashing method, Teoh propos the IOM scheme is used to protect the real value fingerprint feature [14]. IFO is employed to protect the binary template, such as iris coding. Cancellable biometric is to generate a noninvertible identifier from the original biometric information through a specific conversion function using the parameters given by the user. Cancellable biometric recognition technology also ensures its recognition performance and high matching accuracy. However, it is challenging to design an all-round cancelable biometric scheme as it should satisfy the following properties semultaneously. According to the evaluation criteria of template protection, a standard cancelable biometric template should satisfy the following four points, namely noninvertible, renewability, unlinkability and accuracy performance [15].

(1) Noninvertible: Noninvertible refers to the fact that the original biometric template can not be recovered from the cancelable biometric template even if the specific parameters of the conversion function used by the user are known.

(2) Renewability: Renewability refers to the ability to generate multiple uncorrelated cancelable biometric templates from the original biometric templates with different parameters given by users.

(3) Unlinkability: Unlinkability is a strict irrelevance of multiple cancelable biometric templates generated from the same biometric template, which does not produce cross-cutting phenomenon.

(4) Performance: Despite performance degradation is inevitable due to information loss in the one-way transform. The performance degradation of the scheme of the scheme should be insignificant.

Like as the traditional cryptography, anonymous biometric authentication model is also very important in biometric recognition [16]. In the current work, a one-factor cancellable palmprint biometric recognition scheme is proposed to generate pseudonymous identifier. For palmprint recognition, zhang applied to the orientation information and constructed a joint histogram on each block to form the feature vectors of a palmprint [17]. We use another filter and more orientation information to obtain the information fully. Firstly, based on the Logistic-Tent-Sine composite chaotic system [18], to improve the efficiency and effectiveness, a aparallel structure is designed to generate Orthogonal Gaussian random projection(GRP)matrices. The Schmidt orthogonalization scheme is employed in the GRP and palmprint feature to obtain the OIOM hash code, which is represented in binary form. A random binary string is XOR the binary OIOM hash code to construct the helper data for authentication. The random binary string is hashed by MSH to get the final pseudonymous identifier. Lastly, during matching, based on helper data and another palmprint images another pseudonymous identifier is generated to match. The proposed scheme is salted by the XOR encryption/decryption that adopted from fuzzy commitment (an instance of biometric cryptosystem) to generate cancellable biometrics templates. Specifically, XOR operates on the transformation key that enables one factor property.

In the authentication process, the user only needs to provide his/her palmprint features to generate a query pseudonymous identifier, which matches the corresponding pseudonymous identifier stored in the registration stage, and does not directly involve the protected palmprint template in the database. And this scheme only needs one factor to complete palmprint recognition, which is more practical than the other two factors.Based on LSH hashing methods, this scheme has strong security on the basis of maintaining palmprint recognition rate. The experiment is carried out on the PolyU palmprint database [19] and TJU toucheless palmprint database [20]. The noninvertible, renewability, unlinkability and several security attacks of the proposed scheme are analyzed. The experiment results and analysis show that the proposed scheme has strong security on the basis of maintaining palmprint recognition rate.

The main contributions of this paper can be summarized as follows:

(1) The Gaussian random projection matrices is very vital in the IOM local sensitive hashing. A parallel structure is designed to improve the speed of generating Gaussian random projection matrices. Then, Schmidt orthogonalization scheme is employed to improve the performance of IOM. Therefore, the novel scheme is named as OIOM.

(2) Minimum hash signature, which is local sensitive hashing, compresses a larger data into a smaller signature without affecting Jaccard similarity between data. We are the first to apply the MSH technique on palmprint template protection and to enhance the accuracy of authentication. Also, the external factor may be long and this solves the long password memory problem when it is applied to protect the feature.

(3) Despite the use of user-specific external factor (e.g. key/token) satisfies revocability and unlinkability requirements, failure in managing external factor can lead to several problems as mentioned. We introduce a one factor palmprint authentication mechanism to address key management. The key to the irreversibility and diversity of our approach lies in the introduction of 'proxy' identifiers instead of the converted palmprint identifiers, i.e. pseudonymous identifier. Pseudonymous identifier is similar to cancellable palmprint recognition template in cancellable palmprint feature recognition system. In our scheme, we use a random binary string as a pseudonymous

identifier. Pseudonymous identifier is independent of palmprint feature templates and is required only during registration. Therefore, pseudonymous identifier can be uniquely allocated according to different users or applications, and can be revoked and replaced when needed.

(4) In a conventional way, the biometric protection scheme is used in the verification scheme. In our paper, the scheme can be used in identification scheme as the pseudonymous identifier can be represented as a user.

The rest of this paper is organized as follows. Section II introduces the related work for different biometric protection schemes and the palmprint feature extraction methods, especially the local texture descriptor-based approaches. The basic knowledge of CompCode histogram feature of palmprint and Jaccard distance is introduced in Section III. In Section IV, a one-factor cancellable palmprint biometric recognition scheme based on OIOM hash and MSH is proposed. The experimental results are given and their analysis is described in section V. Section VI analyses the security of the proposed method. Finally, section VI summarizes this paper.

II. RELATED WORK

Biometric encryption is generally classified into two types: biometric cryptography and revocable authentication. There is a large volume of literature in the area of biometric security and privacy and we will primarily focus on methods which are related to face template security. Methods that use fuzzy commitment or fuzzy vault schemes have been explored in the past [8], [9]. Fuzzy vault algorithm is a classical practical algorithm in key binding strategy. The algorithm can link the fuzziness of biological features with the accuracy of key algorithm. However, lack of reusability [10] and cross-match attack [21] is the main problems in the fuzzy vault. Cancellable biometrics offers a solution for preserving user privacy and a biometric template protection scheme [2]. Combined with cancelable biometric and modified fuzzy commitment, Feng proposed a hybrid face template protection scheme [22]. Despite the popularity of cancelable two-factor biometric recognition schemes, it also has many drawbacks. Because the scheme needs to input user-specific parameters, which is equivalent to a key, and the key needs to be stored, it will bring inconvenience to users. And user-specific parameters will be stolen. When the key is stolen, the opponent can enter the system instead of the real user. In addition, exposing user-specific parameters may cause an intrusion into the transformation template. Therefore, it is necessary to design a one-factor cancelable biometric recognition scheme which can effectively avoid the drawbacks of two-factor biometric recognition [23].

In the LSH, collision probability for similar objects is high enough and collision probability for dissimilar objects is low [24]. The randomized data structure provide the possibility of the security. Inspired by these characteristics, many biometric protection scheme algorithms have been proposed in the field of cancellable biometric recognition [25]–[27]. However, the security problems must be considered and the bloom filter-based has been cracked as reported in [28]. During design the biometric protection scheme, biometric feature type is one vital factor, such as binary code, real number vector. Difference cancellable template schemes are suitable for different feature types. The IFO and Bloom scheme are used to protect the binary code [13], [22]. However, these schemes usually exist misalignment during the match stage. The random distance between binary vectors is preserved after transformation and Partial Hadamard transform that is used to generate cancellable binary biometric representations [29]. However, this scheme need to fit the specific fingerprint feature. For the real number vector, researchers have developed the following techniques. Jin *et al.* [14] first used the random projection to map the real number vector into the compressed space and the index of the projection maximum values is computed to generate the discrete index hash codes. Qiu used the random compassion to generate cancellable palmprint template [5]. However, when the token is the same, the performance will decreased. Another solution is that the quantization scheme is employed to translate the real number vector into integer vector [30].

The deep neural network is also employed in the biometric protection. To address the advent of similarity-based attacks (SA), Deep Secure Quantization (DSQ) based on neural network implementations is used to protect iris feature [31]. Deen Dayal Mohan presented a significant bit based representation for creating secure face templates with negligible degradation in the performance [32]. Compared with single biometrics system, multi-biometrics system which integrates multiple biometrics can improve the accuracy and security of recognition. Yang *et al.* [33] formed the final template protection scheme by fusing fingerprints and finger veins with cancellable templates. But this method can not effectively resist all kinds of attacks. The electrocardiogram (ECG) signals have the potential to be used in daily activities such as access control and patient handling as well as in wearable electronics applications. Recently, the cancellable biometric techniques based on ECG has attracted the researcher's attention [34]. Combined with EEG and Fingerprint multimodal biometric, Mohamed Hammad propose a secure multimodal biometric system using fusion strategy at different level to improve the performance and to resist spoof attacks [35], [36].

For palmprint biometric recognition system, the code based approaches suffer from the misalignment problem and it must be solved the rotation and translation error [37]. The palmprint biometric protection scheme must account for local variations in rotation and translation, therefore, coding-cased approaches are not well suitable for cancellable schemes. Recently, methods based on local texture descriptors have been proposed and have promising performance. Generally, local texture descriptors designed for general-purpose applications are applied for palmprint recognition. Histograms of Oriented Gradients (HOG) [38], Local Directional Patterns (LDP) [39] are the general-purpose texture descriptors for palmprint images. Zhang introduces the Collaborative

Representation Competitive Code (CR-CompCode) for palmprint recognition, a combination of a coding-based method and a local texture descriptor [14]. The Local Line Directional Patterns (LLDP) descriptor encoding multiple orientations for each pixel [40]. Rida et al. proposed a hybrid palmprint recognition method by first building incoherent sample dictionary based on 2DPCA and extracting discriminative features using 2DLDA [41]. For machine learning methods, Lunke Fei proposed novel and discriminative direction binary features from direction-based convolution difference for palmprint recognition [42]. A. Genovese et al., proposed an innovative CNN that uses a novel method of applying Gabor filters in a CNN. The palmnet has a recognition accuracy greater than that of the current methods in the literature

Cancellable biometrics offers a solution for preserving user privacy and a biometric template protection scheme. However, this traditional scheme needs not another key or token to generate the revocable character, which usually suffers from the token-stolen problem. To address the above challenges, a one-factor cancellable palmprint biometric recognition scheme based on Orthogonal Index of Maximum hash and Minimum Signature Hash is proposed. The specific process of this scheme is as follows. Firstly, the compcode feature of palmprint the region of interest is extracted. Several GRP matrices are generated and Schmidt orthogonalized [13]. The position information of the maximum value is obtained by projecting the compcode feature as OIOM hash coding. The binary conversion of OIOM hash coding is also carried out. Then the user-specific binary code is XOR the OIOM binary hash code to generate the binary string in the authentication stage. Finally, the last pseudonymous identifier is obtained by minimum signature hash transformation of binary strings. And this scheme only needs one factor to complete palmprint recognition, which is more practical than the other two factors.

III. PRELIMENAR

In this section, we describe the palmprint feature extraction. Then, A typical Locality Sensitive Hashing (LSH), index-of-max hashing is introduced.

A. COMPCODE MAPPING FEATURE

Methods based on local texture descriptors generally involve encoding the intensity value of each pixel, computing the histograms of the encoded representation (blockwise histograms) for each local region of the image. The Ref. [17] is the typical of this instance.

During the feature extraction, different directions of Gabor filter are used to surround the palmprint image, and the filter index in the dominant direction is the local area palmprint feature. It maps the palmprint images from grayscale space to direction feature space. Gabor transform can simulate the visual cortex cells of mammals, and has strong robustness to the changes of illumination and contrast of images. However, anisotropic filter, a variation version of the Gabor, was proposed to improve the accuracy of palmprint feature recognition [43]. The anisotropic filter is Gabor-like filter bank, and it is very suitable for exaction the orientation line feature. The Gabor-like filter bank formula is as follows:

$$G_R(u, v) = \left(4u^2 - 2\right) \exp\left(-\left(u^2 + v^2\right)\right) \tag{1}$$

where (u,v) is the plane coordinate and can be obtained by the following formula.

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 1/\alpha & 0 \\ 0 & 1/\beta \end{pmatrix} \times \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \times \begin{pmatrix} x - x_0 \\ y - y_0 \end{pmatrix} \tag{2}$$

where (x_0, y_0) is the center of the filter, the rotation θ, to locally orient the filter along palm lines and α and β are to adapt the line orientation. The ROI of palmprint image is filtered by the anisotropic filter banks to get the filtered image. Then the maximum index of filter banks is obtained to form the local orientation feature. The formula is as follows:

$$CompCode(x, y) = \arg\min_j \left(I(x, y) * G_R\left(u, v, \theta_j\right)\right) \tag{3}$$

where $I(x, y)$ represents the point with abscissa x and ordinate y in the palmprint image; $*$ represents convolution operation; $\theta_j = j\pi/J, j = \{0, 1, \cdots, J-1\}$, J represents the number of directions to obtain palmprint image, $J = 8$; G_R represents Gabor filter. The CompCodes-based algorithm are sensitive to a small amount of matching deviation between the training image and the test image.

In addition, features based on global statistics, such as histograms, are robust to deviations. Then by concatenating these blockwise histograms to obtain a one-dimensional feature vector representing the corresponding biometric template, and using different distance measures (e.g., the Euclidean or chi-squared distance) to compare the resulting templates. The specific implementation steps are illustrated in Fig.1.

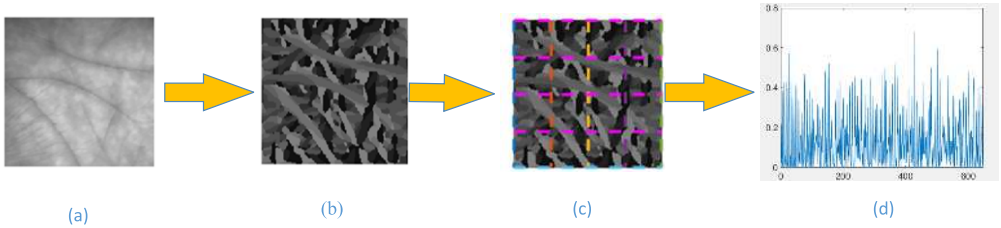

FIGURE 1. Histogram of feature vector extraction (a)region of interest for a plamprint (b) the orientation feature (c) the feature are divided into non overlap blocks(d)the normalized histogram of whole palmprint.

B. INDEX OF MAX

LSH divides the original data set into multiple sub-collections through the hash function mapping transformation operation, and the data in each sub-set is adjacent and the number of elements in the sub-set is small. The problem of finding neighbors within a very large set translates into the problem of finding neighbors within a small set, and obviously the amount of computation has dropped a lot. Based on random projection and LSH, Index of Max(IOM) hashing was proposed to generate a cancelable biometric template [14]. IOM converts a real biometric vector into a discrete index hash code under the random parameters generated outside. The GRP-based IOM hashing is a hashing transformation of biological features using Gaussian random projection(GRP) matrix. In this method, palmprint vectors are embedded in m-dimensional Gaussian random subspace, and the index of projection features with maximum values is obtained.

The GRP-based IOM hashing consists of the following steps [14]:

(1) The fingerprint feature vector $F \in R^d$ is given in a real vale form. The d is the dimension and m representes number of GRP vectors for q times $\{w_j^i \in R^d | i = 1, \ldots, q, j = 1, \ldots, m\} \sim N(0, I_d)$ is generated, so the GRP matrix $W^i = [w_1^i, \ldots, w_m^i]$ can be formed. Then it is multiplied by the real fingerprint feature F (x, y).

(2) The position t of the maximum value obtained is calculated and recorded.

(3) Repeat the above two steps q times and the $t_{GRP} = \{t_i \in [1, m] | i = 1, \ldots, q\}$ is the final IOM hash codes based on GRP.

IV. METHODOLOGY

In this section, an overview of the proposed one factor cancelable scheme is first illustrated, followed by the detail of the scheme. The proposed scheme consists of the following three parts: (1)The generation of orthogonal GRP and Generation the OIOM hashing code; (2)Generation random string and the pseudonymous identifier; (3)Jacard metric for matching of the templates/query instances. Fig.2 presents the flowchart

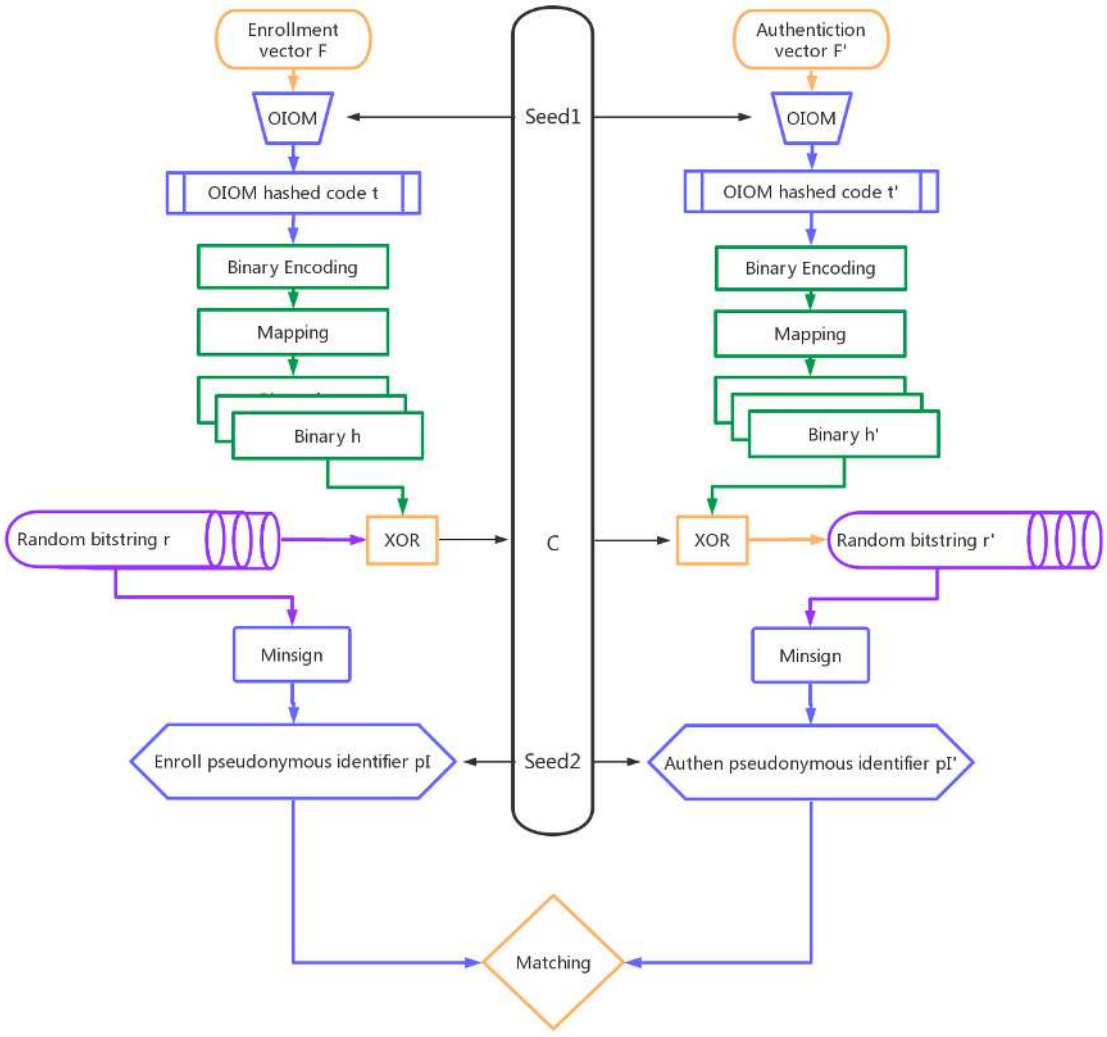

FIGURE 2. Overview of the proposed one-factor cancellable palmprint feature scheme.

TABLE 1. Nomenclature.

Notation(s)	Description
F	Palmprint vector $F \in R^d$
W	Gaussian random matrice
Z	Orthogonalized Gaussian projection matrice
m	Number of Gaussian random projection vector
q	Number of Gaussian random matrice
t	OIOM hashed code
h	Binary OIOM hashed code
c	Generated encryption template
pI	Pseudonymous identifier

of the proposed scheme. Table 1 tabulates the notations used in this section.

As illustrated in the Fig.2 for authentication, the system first generate a pseudonymous identifier according to the user's palmprint provided. Then the pseudonymous identifier is matched to other pseudonymous identifiers in the database. In the part 1, the histogram feature vector F of the user's palmprint is transformed to the cancelable OIOM hash code $t \in \{1, m\}^q$ with seed 1. Then the hash code t is embed into binarized template h, $h \in \{0, 1\}^d$. In the part 2, a random bit-string r, $r \in \{0, 1\}^d$ is generated from a random bits generator, which is also not user-specific seed dependence. Then the XOR operation is performed with r and binary-coded OIOM hash code h, $h \in \{0, 1\}^d$, yield the encrypted template C. In addition, r carries out hash coding with seed 2 based on minimum signature and returns pseudonymous identifier, $pI \in \{0, 1\}^d$. In the part 3, the query pseudonymous identifier pI′ is generated, $pI' \in \{0, 1\}^d$. The Jaccard distance is used to retrieve and match pI′.

A. GENERATION THE OIOM HASHING CODE

1) THE PARALLEL STRUCTURE FOR ORTHOGONAL GRP MATRIX IMPLEMENTATION

In the IOM-based cancelable biometric protection scheme, the security and performance mainly depend on the random projection generation mechanism and its statistical character. Generally speaking, the GRP matrix used in OIOM hash transform must satisfy strong randomness and irreversibility. Compared with the traditional one-dimensional chaotic system, composite chaotic system has higher randomness and security for its larger Lyapunov exponent. LTSS is one of the typical composite chaotic system [18]. The formula of LTSS is as follows:

$$x_{n+1} = \begin{cases} \left(\left(rx_n\left(1-x_n\right)+rx_n/2\right) \bmod 1 \right. \\ \left. +(4-r)\sin\left(\pi x_n\right)/2\right) \bmod 1, & if: x_n < 0.5 \\ \left(\left(rx_n\left(1-x_n\right)+r\left(1-x_n\right)/2\right) \bmod 1 \right. \\ \left. +(4-r)\sin\left(\pi x_n\right)/2\right) \bmod 1, & if: x_n \geq 0.5 \end{cases} \tag{4}$$

As shown in Fig.3, LTSS composite chaotic system is composed of logistic, tent and sine chaotic maps through two additive combinations to ensure the chaotic degree of the composite chaotic system, and the chaotic sequence is always between 0-1 by two residual functions.

Firstly, assuming that the value of the n-th input of the system is x_n, x_n is input into one-dimensional logistic chaotic map, one-dimensional tent map and one-dimensional sine map. The mapping values of logistic chaotic and tent chaotic are combined by adder, and redundancy operation is carried out to ensure that the combined mapping values are between 0 and 1. The mapping value of sine chaotic and the mapped value after processing are combined and redundant for the second time. Finally, the mapping values of the whole LTSS chaotic system are obtained. By repeating the above operations, we can get more random sequences than the traditional one-dimensional chaotic sequences.

Base on the LTSS and Schmidt orthogonalized algorithm, we proposed the parallel structure for orthogonal GRP matrix implementation, as illustrated in the Fig.4. There are two main core parts of the whole model. One is the design of mapping function and the other is the key value filtering.

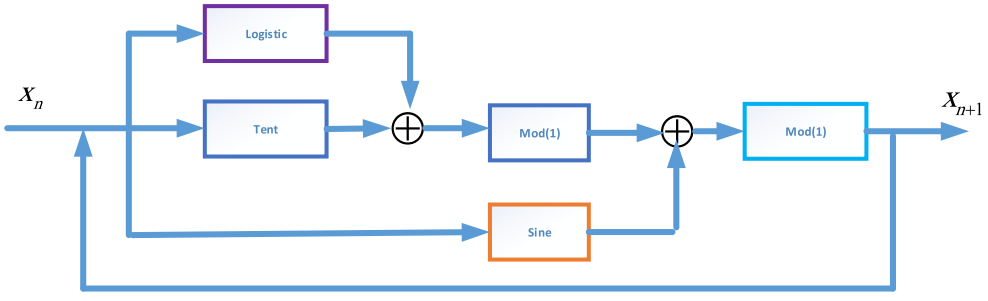

FIGURE 3. LTSS Composite Chaotic Model [18].

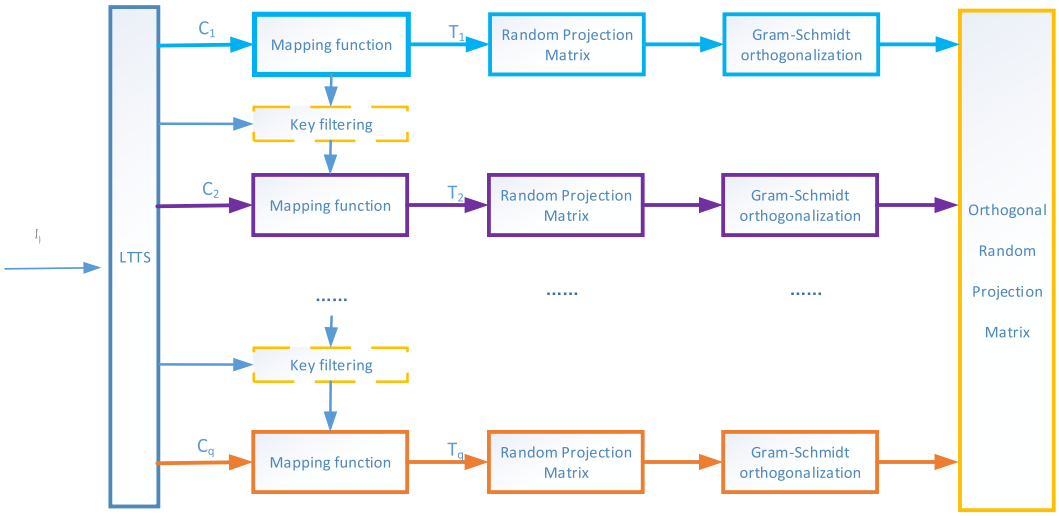

FIGURE 4. Generation model of orthogonal GRP matrix in parallel structure.

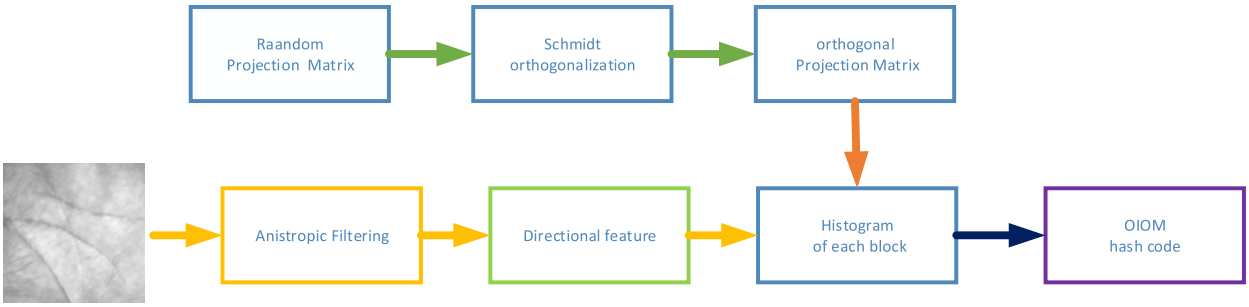

FIGURE 5. The illustration of generation OIOM hash code for palmprint protection.

The parameter $C = [C_1, \ldots, C_n]$ in represent some chaotic values in the Fig.4. The projection random parameters $T = [T_1, \ldots, T_n]$ are randomly selected for the GRP matrix. The parameter n refers to the index of random projection matrices. The key filtering is the function of choosing the matrix randomly to improve the security. The random projection matrices are then orthogonalized by the Schmidt scheme to improve the correlation of different column of matrices.

2) OIOM HASHING CODE

In the IOM hashing process, the projection matrix of GRP-based IOM is non-orthogonal and has correlation. Therefore, the extracted hashing codes are correlated and there is certain information redundancy among different hashing codes. In the OIOM hashing code, the OIOM is obtained by the orthogonal GRP matrix via the Schmidt orthogonalization. Orthogonal GRP matrix has strict independence. It can extract hashing code with more information and improve recognition the IOM hashing performance. As the IOM, the OIOM also meets the requirement of cancelable biometric protection scheme.

The main steps of generation OIOM hash code for palmprint protection is shown in the Fig.5. Firstly, ROI of the original palmprint image is input and filtered by anisotropic filter to obtain palmprint histogram feature. The generated GRP matrix is Schmidt orthogonalized to obtain the orthogonal GRP matrix. The feature is multiplied by the orthogonal GRP matrix, and the position of the maximum projection value is recorded. Orthogonal GRP embeds CompCode feature eigenvectors of palmprint into m-dimensional Gaussian random subspace and uses maximum projection feature index. Repeat this process with q-independent Gaussian random matrix and generate a set of q-OIOM hashing codes. Finally, we get the cancellable palmprint OIOM hashing code. OIOM hashing algorithm based on orthogonal GRP matrix is given in Algorithm 1.

Fig.6 give an example of OIOM hash code. From the Fig.6, we can see that the distribution of hash code is uniform. And different random projections generate different OIOM hash codes.

To compare with the performance with IOM, Fig.6 illustrates the performance between IOM and OIOM. The experimental results is based on PolyU database [19]. includes 600 gray-scale images collected from 100 hands with 6 samples. From the Fig.7, we can see that the performance of OIOM is better than that of IOM. And The cancelable performance is a little worse than the original performance.

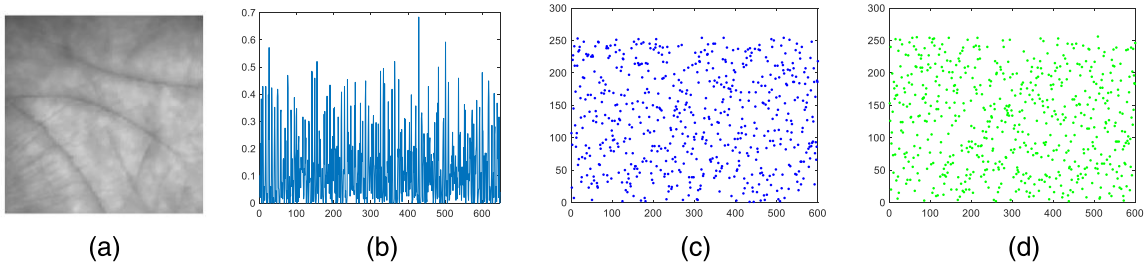

FIGURE 6. (a)Region of interest (b) histogram feature (c) and (d)OIOM hash with different Random Projection The region of interest is 128∗128. the histogram feature is 648. q = 600 and max index M = 256.

Algorithm 1 Orthogonal Index of Maximum Hash

Input: Feature vector, $F \in R^d$ number of Gaussian random matrices q and the number of Gaussian random projection vector m.

Output: Hashed code $t_{GRP} = \{t_i \in [1, \mathrm{M}] | i = 1, \ldots, q\}$.

Step 1: Generate q Gaussian random matrices.

$$W^i = [w_1^i, \ldots, w_m^i] i = 1, \ldots, q.$$

Step 2: Gaussian projection matrix is Schmidt orthogonalized.

$$Z^i = [Z_1^i, \ldots, Z_m^i] i = 1, \ldots, q.$$

Step 3: Initialize i^{th} hashed code $t_i = 0$.

Step 4: Perform random projection and record the maximum index in the projected feature vector.

For $k = 1 : q$

$\bar{F}^k = Z^k F$

Find $F_j^k = \max(\bar{F}^k), j = 1, \ldots, M$

Then $t_i = j$(**j refers the index of** $\bar{F}^k$)

End for

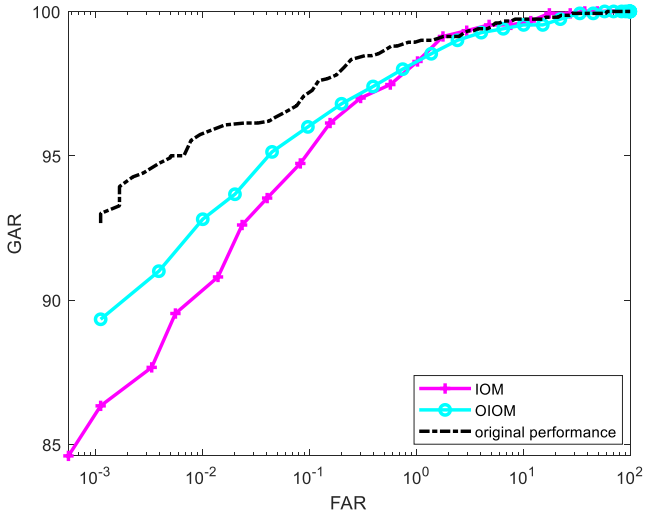

FIGURE 7. ROC curve of different approaches. It is noted that the Jacard metric is employed in IOM and OIOM while the original feature blockwise histogram is evaluated by the 'euclidean' metric.

The OIOM are summarized as followings. OIOM is local sensitive hashing, which can be used to generate cancellable biometric templates. In the OIOM scheme, the random projection is orthogonal, which can improve the recognition rate while maintaining the security of IOM. Also, OIOM hash has the following advantages: (1) OIOM hash can better hide real palmprint features, and use location information to represent cancelable palmprint features (2) OIOM hashing is essentially a location-based hashing method, which depends on the relative order of palmprint features and is independent of the size of palmprint features. (3) In GRP-based OIOM, OIOM obtains the orthogonal GRP matrix by Schmidt orthogonalization of GRP. Because the orthogonal matrix has strict irrelevance, more palmprint information can be extracted and better recognition results can be obtained. OIOM provides a solid foundation for the one-factor palmprint recognition scheme proposed and can get better palmprint verification performance. Finally, the OIOM hash code is converted into binary code, and each feature code is represented by the binary number of corresponding hash code.

B. GENERATION RANDOM STRING AND THE PSEUDONYMOUS IDENTIFIER

1) MINIMUM HASH SIGNATURE

MinHash (or the min-wise independent permutations locality sensitive hashing scheme) is a technique for quickly estimating how similar two sets are [44]. After random row scrambling, the probability that the minimum hash value of the two sets is equal the Jaccard similarity of the two sets. In short, the minHash is that the rows of a matrix are randomly scrambled, and the minHash value of a column is equal to the number of rows where the first value of the column is "1". It was used in the search engine to detect duplicate web pages in the large-scale clustering problems [24], [45]. Based on the number of permutation seeds, different index vectors are generated after Minhashing. Because of the randomness and similarity preservation in MinHash, it has been employed to protect the iris template [13].

The minimum hash is a simplify version of minHash. After getting the signature matrix above, we can use the similarity

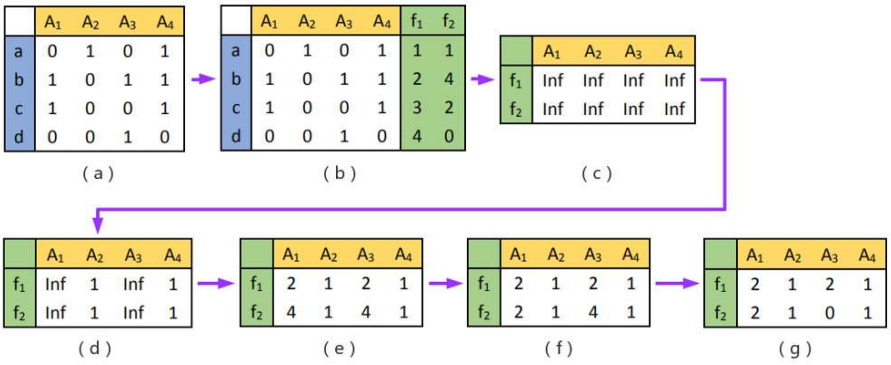

FIGURE 8. Minimum Signature Hash transform (a) the feature matrix, (b) the hash function value of the feature matrix, (c) the initial signature matrix, (d) (e) (f) is the signature matrix updated by each round, respectively (g) the final minimum signature matrix.

between columns in the signature matrix to calculate Jaccard similarity between sets. MSH is implemented as follows:

1) Traversing all the row vectors of the characteristic matrix, we calculate the values of the two hash functions listed at 1 where the row vectors are located. That is to calculate the values of the hash functions $f_1^{(r)}$ and $f_2^{(r)}$ at that point.

2) We compare the two values of the column in the original minimum hash signature matrix. If the corresponding two values of the column in the original minimum hash signature matrix are smaller than those of the newly generated two hash functions, the minimum hash signature matrix will not be updated; if the corresponding two values of the column in the original minimum hash signature matrix are larger than those of the newly generated two hash functions, the column in the minimum hash signature matrix will be updated to the newly generated hash values with smaller values.

3) If all the row vectors are iterated through, the update of the minimum hash signature matrix stops. And pseudonymous identifier (pI) is obtained.

Several hash functions are generated randomly to generate signature matrix $sig(i, c)$. The initial values of signature matrix $sig(i, c)$ are infinite. Where i represents the generated i hash function and c represents the c column of the initial eigenvalue matrix.

Therefore, the initial size of the generated signature matrix $sig(i, c)$ is $2 \times n$, where the size of n is determined by the number of columns of the characteristic matrix. Let's assume that the hash function we used in the experiment is expressed in f. The two hash functions used are:

$$f_1(r) = (r + 1) \bmod 5 \tag{5}$$

$$f_2(r) = (3 \times r + 1) \bmod 5 \tag{6}$$

An example of generation the final minimum signature matrix is illustrated in the Fig.8, in which the round number is 5. As we can see from Fig.8, the initial feature matrix is Fig.8 (a). Initialize the signature matrix with an initial value of Inf. Because only two hash functions are used in this example, the size of the signature matrix is 2×4. The initial signature matrix is the Fig.8 (c). Inthe first row, the values of columns 2 and 4 are 1. Then we calculate $f_1 = 1, f_2 = 1$. The signature matrix is updated to the Fig.8 (d). In the second row, the values of columns 1 and 3 are 1. Then we calculate $f_1 = 2$, $f_2 = 4$. The signature matrix is updated to the Fig.8 (e). In the third row, the values of columns 1 and 4 are 1. Then we calculate $f_1 = 3, f_2 = 2$. The signature matrix is updated to the Fig.8 (f). In the fourth row, the values of columns 3 is 1. Then we calculate $f_1 = 4, f_2 = 0$. The signature matrix is updated to Fig.8 (g). Finally, the signature matrix is obtained by iterating through all the row vectors.

The random string is usually represented as a specific user in practice. The privacy is enhanced if the random string is processed by MSH. Compared with the password in two-factor scheme, the random string may have a long string. The traditional Hash function, such as MD5 and SHA-1, is a widely used cryptographic hash function that produces a fixed length bit hash value. Also, the MSH can map the random string into a fixed length. As cryptographic hash function is used to protect the user's password, the random string can be protect by the MSH.

2) GENERATION THE PSEUDONYMOUS IDENTIFIER

OIOM hash converts real-valued palmprint feature vectors into discrete index hash codes. The main generation pseudonymous identifiers steps of the algorithm are given in Algorithm 2.

In the registration process, firstly, the histogram feature vector F of the user's palmprint is transformed to the cancelable OIOM hash code $t \in \{1, m\}^q$ with seed 1. It is noted that the seed 1 is provided by the recognition system while it is given by author in the traditional two-factor biometric protection scheme. Then the hash code t is embed into binarized template h, $h \in \{0, 1\}^d$. A random bitstring r, $r \in \{0, 1\}^d$ is generated from a random bits generator, which is also not user-specific seed dependence. Then the XOR operation is performed with r and binary-coded OIOM hash code h, $h \in \{0, 1\}^d$, yield the encrypted template c, $c = h \oplus r \in \{0, 1\}^d$. In addition, r carries out hash coding with seed 2 based

Algorithm 2 Pseudonymous Identifier Generation Scheme

Input: blockwise CompCode histogram vector $F \in R^d$.
Output: Pseudonymous identifiers.

Step 1: **We obtain OIOM hash codes t by OIOM hash mapping of CompCode features of palmprint based on seed 1. The palmprint feature t obtained from OIOM mapping is converted to binary OIOM hash coding h.**

Step 2: **The user-specific binary number r is XOR with the obtained binary OIOM hash code h to get C.**

Step 3: **The user-specific binary number r is transformed by hash transform based on minimum signature, and the pseudonymous identifier pI is obtained on the basis of seed 2.**

Step 4: **In the authentication stage, the palmprint OIOM hash feature h′ is obtained in the same way as in the registration stage, and then the binary coding r′ is obtained by XOR with the C obtained in the registration stage. We obtain pseudonymous identifier pI′, using minimum signature hash transform based on seed 2.**

on minimum signature and returns pseudonymous identifier, $pI \in \{0, 1\}^d$. The encrypted template c and pI are stored in the database.

In the authentication process, the user show the palmprint to be queried, and OIOM hash coding is carried out on it with seed 1 to get $t' \in \{1, m\}^q$. It converts binary to $h' \in \{0, 1\}^d$. The reverse conversion of c and r′ is $r' = h' \oplus C$. Then the hash coding of r′ based on minimum signature is carried out with seed 2. Lastly, the query pseudonymous identifier pI′ is generated, $pI' \in \{0, 1\}^d$.

During the registration and recognition stage, only one factor, a user palmprint biometric is needed when using the system. Therefore, this scheme is a one-factor recognition scheme. This is simply but efficient scheme. What is more, it is very security. This scheme does not directly use palmprint feature template or conversion template to identify and authenticate, but uses a hash random string independent of palmprint feature as a pseudonymous identifier to identify and authenticate. Therefore, the use of pseudonymous identifier for palmprint recognition and authentication has the advantages of uniqueness, revocability and diversity. In different application scenarios, updating the projection matrix and a random string, a novel cancellable palmprint features based on OIOM is generated. Therefore, the original pseudonymous identifier can be revoked in other applications. If a template is compromised, we can easily cancel it and reissue a new one by the projection matrix and a random string.

By utilizing multiple different hash functions, i.e. non-invertible hash functions, different palmprint feature matrices will be generated. The palmprint features generated by this method can satisfy the irreversibility, diversity and revocability, which is conducive to improving the security of recognition. Note that our proposed scheme is different from the pure two-factor OIOM hash scheme, because our proposed scheme uses OIOM hash and minimum signature hash. Therefore, the security, revocability and diversity of the system have been optimized.

C. JACCARD DISTANCE FOR MATCHING AND CLASSIFICATION

Originally, Jaccard distance is used to evaluate the similarity in LSH functions [24]. Here, the Jacard metric which is usually employed to evaluate the similarity between pseudonymous identifiers in the given. The greater the Jaccard value, the lower the similarity between the two pseudonymous identifier, indicating the lower the similarity between registered and tested palmprints. Given two pseudonymous identifier, they are denoted by A and B. Among them, A represents the pseudonymous identifier pI obtained at the registration stage and B represents the pseudonymous identifier pI′ obtained at the testing stage. A and B are the two testing sets, Jaccard coefficient is defined as the ratio of the intersection size of A and B to the union size of A and B. The formula is as follows:

$$J(A, B) = \frac{|A \cap B|}{|A \cup B|} = \frac{|A \cap B|}{|A| + |B| - |A \cap B|} \tag{7}$$

When A and B are empty sets, J (A, B) is 1.

The index related to Jaccard coefficient is called Jaccard distance. The formula is defined as follows:

$$d_j(A, B) = 1 - J(A, B) = \frac{|A \cup B| - |A \cap B|}{|A \cup B|} = \frac{A \Delta B}{|A \cup B|} \tag{8}$$

where $A \Delta B = |A \cup B| - |A \cap B|$.

$$J(A, B) \in [0, 1] \tag{9}$$

In the identification, the minimum Jaccard distance is believed to the recognition result. In the verification process, Jaccard distance is calculated and compared with the set decision threshold value. When the Jaccard distance is smaller than the set decision threshold value, the two sets are supposed to the same class. This decision threshold can be adjusted in real applications. When the decision threshold is too low, it will increase the false acceptance rate. When the decision threshold is too high, it will increase the false rejection rate. We need to set an optimal decision threshold according to the specific situation, to a certain extent, to make the false rate lower.

V. EXPERIMENTAL RESULTS

This section presents the two popular palmprint databases considered in our proposed scheme, including the PolyU 2D contact-based palmprint database [19] and the TJU Contactless Palmprint Dataset [20], introduces the evaluation procedure and the error metrics used to compare the recognition accuracy. It is should be noted that PolyU

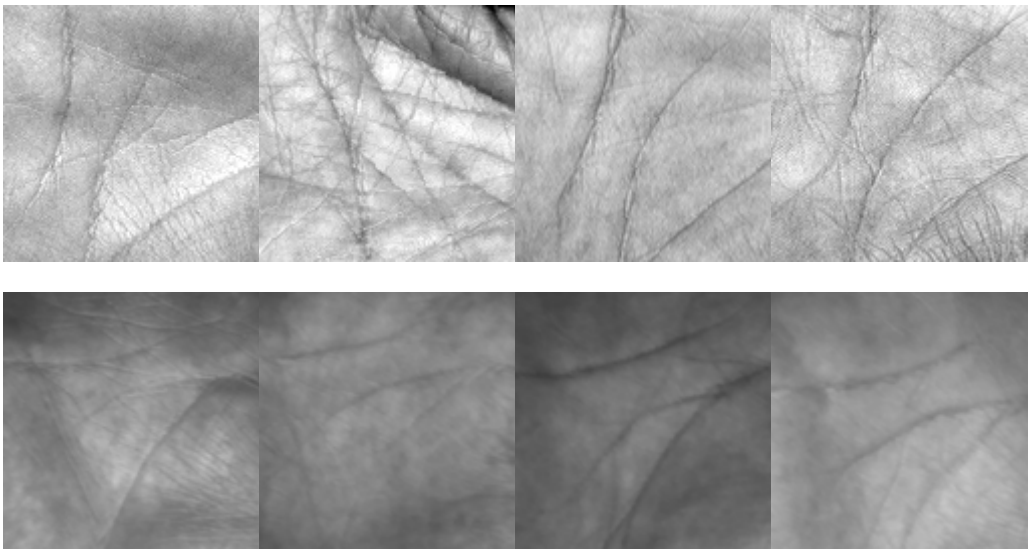

FIGURE 9. Some typical palmprint region of interest images from the two databases. The up and down rows show the samples selected from the PolyU and TJU database respectively.

release two databases, one contains 600samples used in section IV and here we use another touched databases containg 7752 samples. Palmprint recognition includes palmprint identification and palmprint verification. Palmprint identification is a one-against-many matching process to determine the class label of a query palmprint image. Palmprint verification is a one-to-one palmprint matching procedure. During the authentication process, the false acceptance rate (FAR), the false rejection rate (FRR), the Equal error rate (EER) and the receiver operating characteristic (ROC) curve are calculated to estimate the performance of the performance.

In the experimental setting, there are two hash functions in the MSH. The two functions has the following form.

$$g_{m\_i} = circshift\left(g_{m\_1}, i\right) \tag{10}$$

where $g_{1\_1} = [3, 5, 4, 8, 6, 2, 1, 7]$, $g_{2\_1} = [5, 2, 4, 3, 7, 1, 8, 6]$, $m = \{1, 2\}$, $i = \{2, 3, 4, 5, 6, 7, 8\}$. The function ( ) represents it circularly shifts the elements in vector g_{m_1} by i positions. The initial real values in the LTSS chaotic system is between 0 and 1. The ROI size of palmprint is 128×128. The each block size is 16×16. And the orientation of anisotropic filters is uniform and the number is 8. Therefor the size of histogram is 512. Correspondingly, the size of random projection is set 512×256. The round of MSH is 600, then the length of OIOM hash code is obtained to 600. The PolyU 2D and TJU palmprint databases are employed to show the effectiveness of the proposed method on palmprint identification, and the subset of TJU databases are used to test the proposed method for palmprint verification for comparison with the state-of-the-art algorithms. In the following, we show the detailed experiments and the results on each database. Fig.9 shows some typical palmprint region of interest images from PolyU and TJU database respectively.

A. PALMPRINT DATABASES EMPLOYED

(1) Polyu 2D Palmprint database: The PolyU palmprint database contains7,752palmprint images collected from 386 palms of 193 individuals. The PolyU database images are captured using a contact-based methodology. The images were captured in two sessions with an interval of around 2 months. An individual was asked to provide about 10 samples for both the left and right palms. The total numbers of images captured in the first session and the second session are 3889 and 3863, respectively. Actually, a palm in the PolyU database might have about 11 to 27 samples. The ROI images with the sizes of 128×128 pixels have also been included in the database.

(2) The TJU Contactless Palmprint database: The palmprint dataset images were collected from 300 volunteers, including 192 males and 108 females. Among them, 235 subjects were 20∼30 years old and the others were 30∼50 years old. We collected samples in two separate sessions. In each session, the subject was asked to provide 10 images for each palm. Therefore, 40 images from 2 palms were collected from each subject. In total, the database contains 12,000 images captured from 600 different palms. The average time interval between the first and the second sessions was about 61 days. The maximum and minimum time intervals were 106 days and 21 days, respectively.

B. EXPERIMENTS ON THE POLYU 2D PALMPRINT DATABASE

In the following identification experiments, for the PolyU database, 3 and 4 palmprint images per hand were randomly selected to form the training set, and the others were used for testing. To verify the identification performance, the following CR_CompCode [17], HOL [38], LLDP [40],

TABLE 2. The rank-1 identification accuracy (%)on PolyU databas.

Train set	CR_ComCode [17]	HOL [38]	LLDP [40]	E-SRC [41]	IOM [14]	The proposed
3	99.70	99.33	99.08	99.77	99.85	99.88
4	99.83	99.38	99.25	99.78	99.95	99.95

TABLE 3. Rank-1 performance on TUJ full database(%).

Train bumber	CR_Com Code[17]	HOL [38]	LLDP [40.	E-SRC [41]	DDBPD [42]	IOM [14]	Original Feature	The proposed
Identification rate	98.48	95.28	98.50	96.45	97.8333/98.7333	97.65	99.22	98.07

and Ensemble-SRC (E-SRC) [41] state-of-the-art algorithms were chosen for comparison. In our experiments, The Chi-square metric was employed to evaluate the similarity. For the sake of a fair comparison, the local block sizes of all the related methods are set as 16×16 pixels, unless otherwise presented. In the IOM and the proposed scheme, the Jacard distance was used to the matching scores. The methods are repeated 10 times and the mean rank-1 identification accuracies are as the final performance for comparison. The rank-one identification accuracies are reported in Tab.2 based on different number of training samples.

From Tab.2, we can see that the performance of our proposed scheme is little better than most of the state-of-art the algorithm. When train set is 3, the recognition accuracy of the proposed scheme reaches 99.88%. When train set is 4, the recognition accuracy of the proposed scheme reaches 99.95%. Compared with other schemes, the recognition accuracy is improved. What is more important, our scheme has the cancelability and security property. Compared with the original IOM performance, the performance of the proposed is a little higher for the different train numbers which are 3 and 4 respectively. In a word, they are provided the good performance.

C. EXPERIMENTS ON THE TJU DATABASE

To compared with other algorithms and palmnet [37], the experiments are divided into two parts. One is the whole TJU palmprint database, which contains 12,000 images captured from 600 different palms. The others is part of TJU palmprint database, which only contains 5182 images are considered in our experiments [37]. Since the valleys between the fingers are not entirely visible in all images and the preprocessing algorithm palmnet con not extract the valley points. A small fraction of images are discarded. More detail can be found in [37].

1) THE WHOLE TJU PALMPRINT DATABASE

In this section, we use the TJU database to evaluate the performance of the proposed method on palmprint identification. The samples captured in the first session are chosen to form the training set and the samples of the second session are chosen to form the testing set. Thus, both the gallery and probe sets contain 6,000 palmprint samples. We follow the evaluation protocol in [17].In order to evaluate the proposed method better, it is compared with many popular methods, LLDP [40], HOL [38] and DDBPD [42]. In addition, the recently published holistic feature-based methods including the CR_Compcode [17] and E-SRC [41] are also executed. HOL and LLDP have different implementations. Therefore, the detail implementations can be found for comparison in [37].

In the matching stage, it is should be noted that the Jaccard metric distance is employed in our proposed scheme. And the Chi-square distance to compute the similarity of two features in the other algorithms [42]. Table 3 gives the identification accuracies of these methods on the TJU database. It shows that recognition accuracy of the base algorithm can achieve the best performance. As can be seen from the table, the recognition accuracy of our scheme is 98.07%. Compared with the accuracy of the original algorithm, the proposed scheme is reduced by about 1%. This is caused by the loss of information in the anonymous identifier obtained in the biometric recognition and protection scheme. However, in terms of security, our proposed scheme is much better than the original algorithm.

2) THE SUBSET OF TJU DATABASE

The training and testing subsets contain about 50% of the samples selected randomly in the database. As stated in [37], the samples in the two subsets are disjoint. Therefore, a training phase is not required for the methods in the literature. A similar evaluation procedure is similar to the palmnet used. The whole stage including feature extraction, cancelable palmprint OIOM hash codes, pseudonymous identifier generation and matching steps are performed on the testing subset are repeated 5 times. And the averaged results are the final performance. In these cases, we randomly split the database using the same 2-fold cross validation procedure, and evaluated the Rank-1 accuracy based on the resulting feature vectors.

We compare the recognition accuracies of the proposed one-factor scheme against those of the most recently reported

TABLE 4. Rank-1 performance on subset of TJU database.

Ref	CR_ComCode [17]	HOL [38]	LLDP [40]	Palmnet [37]	IOM [14]	Original	The proposed
Identification rate	98.71	99.64	99.75	99.83	99.71	99.71	99.71

TABLE 5. EER performance(%).

Ref	CR_ComCode [17]	HOL [38]	LLDP [40]	Palmnet [37]	IOM [14]	Original	The proposed
Identification rate	0.47	0.41	0.54	0.16	0.41	0.22	0.32

algorithms in the literature. The base line of the proposed scheme is block-wise texture-descriptor histogram, therefore, we consider the similar algorithms, CR-CompCode [17], LLDP [40], HOL [38] for comparisons. Recently, the CNN-based machine learning method is very popular, Palmnet [37] is one of the algorithms and is considered. We configure the methods using the parameters provided by their authors, when available. And we select the Gabor-based version since it is the more accurate version in the vast majority of cases. Table 4 lists the recognition accuracies of the proposed method and those of the other considered methods in the literature for the identification mode, expressed in terms of the Rank-1 classification accuracy. As shown, the proposed one-factor scheme achieves the best accuracies among the considered methods. As shown in the Table 4, the identification performance of our proposed scheme is 99.71%, which is better than most other schemes. Although it performs slightly worse than LLDP and Palmnet solution, it outperforms them in terms of security. Therefore, the proposed single factor scheme achieves the best results in the method considered.

Table 5 lists the recognition accuracies of the proposed one factor and those of the other methods in the literature for the verification mode, expressed in terms of the EER. Table 5 shows that the EER performance of our proposed scheme is 0.32%, which is higher than most of the algorithms. The Fig.10 shows the ROC curves for all considered palmnet, IOM and the proposed scheme. The curves illustrate the superior accuracies of the proposed scheme on all considered algorithms and for the majority of the FAR and GAR values. Although the EER performance of the proposed scheme is slightly worse than that of Palmnet and the original scheme, it is far better than other schemes in terms of security and overall performance.

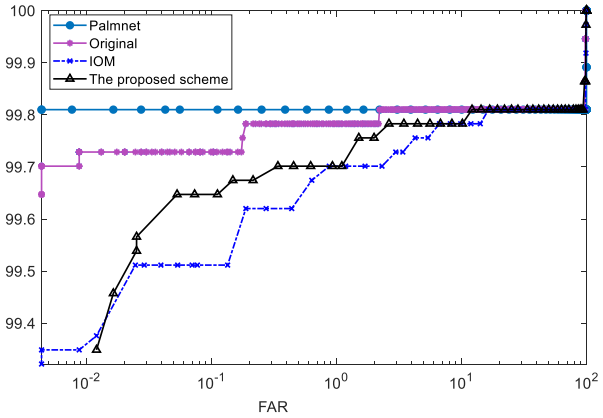

FIGURE 10. ROC curves for the different algorithms, including palmnet, IOM and the original.

D. COMPUTATION EFFICIENCY

Our all experiments were carried out on a PC computer with Intel(R) Core(TM) i5-3570 CPU @ 3.40GHz (4 CPUs). MATLAB R2018b is used in Windows 10.0 operating system. To evaluate the complexity of the proposed algorithm, we calculated the computational time of each stage. The whole stage can be divided into the following The proposed scheme consists of the following three parts: (1) The generation of orthogonal GRP and Generation the OIOM hashing code (2) Generation random string and the pseudonymous identifier (3) Jacard metric for matching of the templates/query instances. In the case of $k = 256$, $q = 600$, the processing time of each stage in this scheme is illustrate in Table 6. The total of processing time of query an instance less than 0.1 second. It should be noted that if the orthogonal GRP is implemented in a parallel way, the time is reduced to six hundredths. This shows that the proposed scheme meets the real-time requirements.

TABLE 6. Average time taken (sec) in each stage.

Stage	PolyU database	TJU database
Part 1	0.0517	0.0630
Part 3	0.0085	0.0096
Part 3	0.0036	0.0042
Total time	0.0638	0.0766

E. DISCUSSION

Most biometric template protection scheme focuses on the fingerprint. The palmprint trait is also very important.

Compared with the state-of-the art performance, the original performance is not less than other schemes. However, our scheme shows that the slight degradation of the original performance.

The main highlights of our proposed systems are summarized below:

- The feature used in the proposed algorithm is alignment-free, which is very suitable for further processing. Also, this is not strictly required for the user when the palmprint image is captured.
- Specifically, we use OIOM hash method and MSH method as the key factors to protect the original palmprint feature template. The palmprint CompCode features are indexed by Orthogonal Index of Maximum hash, and the maximum position information is used to replace the original palmprint feature information, which protects the palmprint features.

According to the advantages of the proposed system, it is very suitable for real applications. However, there are some disadvantages of the proposed system:

- Compared with the recently years, the 256-length compact binary codes learned from CNN for a image [46], the length of cancellable palmprint template is two long, that is 600 in integer values. One value needs 8 bits, if the template is represented in binary way, its length is 4800.

VI. SECURITY AND PRIVACY ANALYSIS

In the above section, we mainly discuss the performance of the proposed one-factor palmprint protection scheme, then we will analyze the noninvertible, unlinkability and renewability. Privacy analysis refers to the feasibility of a one-factor biometric protection scheme to assist various attacks to recover the original biometric one. Then, the security attack analysis is also given. Unlike privacy attack, security attack means the illegitimate access should be forbidden, with feasible attack complexity to the biometric systems via the fake features (including spoof biometric trait) or the elaborated examples that close to the genuine biometric template. For the biometric protection security analysis concerned, Brute force attack, false accept attack, birthday attack, ciphertext-only attack only attack and known-plaintext attack is also given.

A. PRIVACY ANALYSIS

1) NONINVERTIBLE

Noninvertible refers to the computational complexity of recovering palmprint vectors from one-factor cancellable palmprint feature recognition. We assume that the adversary successfully retrieves the pseudonymous identifier and seed 2. The final part of the scheme is to classify pseudonymous identifiers by matching, without the original palmprint features and their transformation forms participating in the matching process. Therefore, there is no clue for the adversary to guess the palmprint feature vector directly from the stolen pseudonymous identifier. In addition, it is difficult to recover palmprint vectors from parameters, because there is no direct relationship between parameters and palmprint vectors.

If given C and h are known, the opponent can recover r according to $C = h \otimes r$. However, r cannot be recovered without h being stored. Assuming that the opponent guesses h, it will take 2^d times, $d = 4200$, or 2^{4200} times, so it is very difficult for r to be recovered.

If given C and r is public, the opponent can attempt to recover h from $C = h \otimes r$. On the other hand, since both C and r are computed with the same h, the attacker attempts to restore h from the perspective of correlation analysis. For example, given h and three different r, three C can be obtained from the following formula.

$$\begin{aligned} C_1 &= r_1 \oplus h \\ C_2 &= r_2 \oplus h \\ C_3 &= r_3 \oplus h \end{aligned}$$

Because r and h are not stored, opponents can only guess r based on C. Therefore, the attacker can cross-XOR Cs in the following way.

$$\begin{aligned} C_1 \oplus C_2 &= (r_1 \oplus h) \oplus (r_2 \oplus h) = r_1 \oplus r_2 \\ C_2 \oplus C_3 &= (r_2 \oplus h) \oplus (r_3 \oplus h) = r_2 \oplus r_3 \\ C_3 \oplus C_1 &= (r_3 \oplus h) \oplus (r_1 \oplus h) = r_3 \oplus r_1 \end{aligned}$$

We guess that a r_i needs 2^d times, $d = 4800$, or 2^{4200} times. So it is very hard for us to get h according to the correlation between r_i and r_{i+1}

Even if we get h, it is difficult to recover the original palmprint eigenvector F, because OIOM hash is noninvertible. Firstly we assume that the opponent successfully retrieves hash codes and seed 1. Hash codes and parameters (such as m, q) are known. For discrete index OIOM based on GRP, there is no clue for opponents to guess palmprint feature vectors directly from h. In addition, it is very hard to recover palmprint vectors from markers such as projection matrices, because there is no direct relationship between markers and palmprint vectors.

2) UNLINKABILITY

Unlinkability is very important in the biometric protection scheme. In order to verify the unlinkability requirement of this scheme, we make experiments on the PolyU and TJU database. As in [14], pseudo-genuine, which is generated by different pseudonymous identifiers of the same hand via different seeds. This match is similar to a true pseudonymous identifier match. Correspondingly, the matching score between two pseudonymous identifiers generated by from the hand different seeds in each template is called pseudo-genuine score. In the same manner, the pseudo-imposter score is computed between two pseudonymous identifiers generated from different hands using different seeds or projection matrices.Fig.11 shows the distribution of pseudo-imposter replacement scores and pseudo-genuine scores. From the figure, the distribution of pseudo-imposter scores overlaps with that of pseudo-genuine scores. This means that the pseudonymous identifiers generated from the

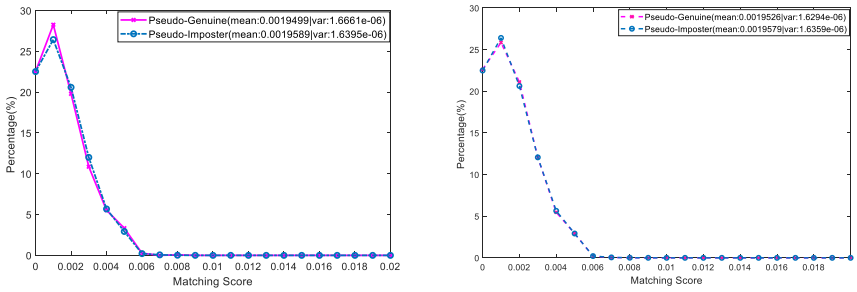

FIGURE 11. Pseudonymous Genuine & Pseudonymous Imposter distributions for unlinkability analysis. Overlapped distributions indicates indistinctiom of hashed codes that generated from the same user or from the others. (a) PolyU database. (b) TJU database.

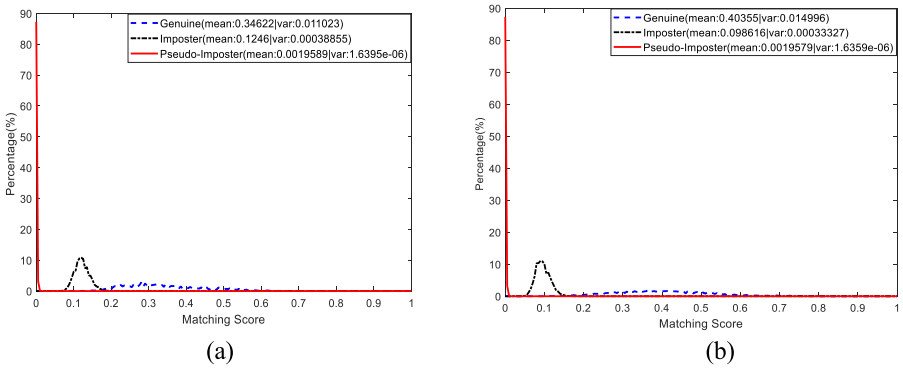

FIGURE 12. The genuine, imposter, and pseudonymous imposter distributions for renewability analysis. A large degree of overlapping of pseudonymous imposter and imposter distributions illustrates that hashed codes generated using different random vectors leads to significant distinction. (a) PolyU database. (b) TJU database.

same user or other users are sufficiently undistinguishable. On the contrary, if the two scores are far apart, it is easy for attackers to distinguish whether pseudonymous identifier is generated by the same user. The difficulty of distinguishing pseudonymous identifiers means the performance of unlinkability. Therefore, the scheme satisfies the requirement of unlinkability from the above analysis.

3) RENEWABILITY

Renewability means that if a palmprint pseudonymous identifier is stolen, the new pseudonymous identifier can be generated according to the original feature and parameters. The following analysis and experiments show that the one-factor scheme can satisfy this point. Firstly, in OIOM hash transform, we use orthogonal GRP matrix for feature projection. A new OIOM hash feature can be obtained by changing the parameter of the generation orthogonal GRP matrix. Secondly, when generating pseudonymous identifier, we perform a minimum signature hash transform for random binary strings to obtain pseudonymous identifier. Therefore, new pseudonymous identifiers can be generated by changing the number of hash functions and their formulas. In the experiment, two hash functions are used to obtain the initial minimum signature matrix of 10×480, so the final pseudonymous identifier of 10×480 is obtained. The dimension of pseudonymous identifier is changed by changing the dimension of minimum signature matrix. It is assumed that the minimum signature matrix used is $m \times n$-dimensional and the pseudonymous identifier obtained is $m \times n$-dimensional. Based on the above three aspects, no matter which aspect is changed, new pseudonymous identifier can be obtained. Therefore, the scheme meets the requirement of renewability.To verify the renewability of the proposed one-factor scheme, we make experiments on PolyU and TJU database and the distribution graphs of genuine, imposter and pseudo-imposter are given in the Fig.12. As shown in Fig.12, we can see that mean score of pseudo-imposter is lower than the distribution of imposter. This is because that in the pseudo-imposter match, both the seeds and hands for generation pseudonymous identifiers are different. However, during the imposter match, only the palmprint from the hands is different and all the seeds are the same during generation the cancelable OIOM codes. Therefore, the pseudonymous identifiers generation from the pseudo-imposter match have more discriminative ability and have lower matching scores. This also means that the pseudonymous identifier generated by the same palmprint database are different even under the same conditions. Therefore, the renewability of this scheme is obvious and verified.

B. SECURITY ATTACKS ANALYSIS

1) BRUTE FORCE ATTACK(BFA)

BFA is a kind of security attack, which attempts to obtain illegal access using randomly generated identifiers. In this scheme, the difficulty of brute force attack can be measured

by the guessing complexity of pseudonymous identifier pI. Because each entry of the pseudonymous identifier is independent and contains values between 1 and m. Therefore, the guessing complexity of pseudonymous identifier with length q is $2^{q\log_2^k}$. When the optimum parameter is $q = 600$ and $k = 256$ the guessing complexity is 2^{4800}. This complexity is far beyond the computing power of existing computer devices, so the proposed scheme effectively avoids brute force attack.

2) FALSE ACCEPT ATTACK(FAA)

FAA is an attack on palmprint OIOM hash database. It is different from BFA in that the number of illegal access attempts required by FAA is much less than that required by BFA. Because BFA is blind guesses about the whole code. And the FAA takes advantage of the far end of the biometric recognition system. It can simply use the artificial template generator to start the attack without destroying any database. Therefore, it is easier to attack the system than BFA. Its attack condition is that access can be granted as long as the matching score successfully reaches the predefined threshold T.

We get parameters from the experiment, $q = 600, k = 256$. When FAR = FRR, the threshold T is 0.32. The minimum number of successful accesses to matched entries is $T \times q = 192$. k represents 256 possible index values, and it is equivalent to $2^8 = 2^{\log_2^k}$ guessing for an entry. Therefore, the complexity of FAA can be estimated from $(2^{\log_2^k})^{T\times q} = 2^{1536}$.

Compared with 2^{4800} in BFA, attack complexity is reduced to 2^{1536}. However, this reduction is still beneficial to attack complexity. We can increase the attack difficulty by adding T and q, but we prefer to increase T because increasing q requires more storage space. Therefore, the complexity of FAA reaches the level of computational infeasibility.

3) BIRTHDAY ATTACK(BA)

Birthday attack is an attack based on mathematical knowledge behind the birthday problem in probability theory. In this scheme, birthday attack refers to the situation where the opponent obtains a large amount of hash code from the damaged database. For a single entry hash codes ($q = 1$), it is found that the expected test for the first collision is $R(\lambda) = \sqrt{\frac{\pi}{2}\lambda}$, where λ is the maximum entry value of OIOM hash code, i.e. $\lambda = m$. Suppose two hash codes collide, i.e. $h_i(X)$, $h_i(Y)$, where $i = 1, \ldots, q$ and $h(X), h(Y) \in [1, \lambda]$. The anticipated test of finding the collisions for T_q element is $(\frac{\lambda\pi}{2})^{\frac{T_q}{2}}$.

Compared with the traditional FAA, the complexity of BFA is greatly reduced. In addition, the attack difficulty is closely related to the size of the selected parameters. However, we can increase complexity by increasing q or decreasing T without affecting the accuracy performance. In short, we need to select the appropriate parameters to ensure the accuracy performance while achieving the maximum level of security.

4) CIPHER-TEXT ONLY ATTACK (COA)

COA is a kind of attack in symmetric key cryptosystem. Its attack method is that the attacker tries to recover plain text through cipher text. In our proposed scheme, the cipher text corresponds to C stored in the system, while the plain text corresponds to the random string r in the system. Therefore, the focus of this attack is whether the opponent can learn r from C if C is exposed. Since r in this scheme is a random string with length q, $C = h \oplus r$ is an equivalent uniform random string. Therefore, adversary cannot learn r from a separate C.

5) KNOWN-PLAINTEXT ATTACK (KPA)

KPA is a kind of security attack, which assumes that opponents can access plain text and cipher text at the same time. So this way can reveal more secret information. In this scheme, KPA is equivalent to learning from C and r, because $C = h \oplus r$. However, r in our scheme is not stored in the system and it is not feasible to apply enumeration method. Therefore, this scheme effectively prevents KPA.

VII. CONCLUSION

The proposed scheme that is one-factor palmprint recognition based on OIOM and Minimum Signature Hash in this paper meets the four design criteria of biometric template protection. This scheme is a one-factor cancelable palmprint feature recognition scheme, which is safer and more practical than the original two-factor cancelable biometric recognition scheme. Firstly, the palmprint features are transformed by OIOM hash transform, which adds the first layer of protection to the template. In the OIOM hash change, we use LTSS system to generate orthogonal GRP matrix, which enhances the randomness of projection matrix and the noninvertible of the scheme. Then the minimum signature hash transform is applied to the user-specific binary number, which adds a second layer of protection to the template. These two layers of protection can ensure that the converted template is irreversible, while maintaining a better accuracy performance. This scheme separates the matched identifier from the biometric template, so that the matched identifier has good updating and unlinkability. After several aspects of security analysis, the proposed scheme not only keeps the accuracy, but also improves the security in many aspects.Proposed one-factor scheme.

REFERENCES

[1] A. K. Jain, "Technology: Biometric recognition," *Nature*, vol. 449, pp. 38–49, Sep. 2007.
[2] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.
[3] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, Jun. 2004.
[4] D. Zhang, W.-K. Kong, J. You, and M. Wong, "Online palmprint identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 9, pp. 1041–1050, Sep. 2003.
[5] J. Qiu, H. J. Li, and C. Zhao, "Cancelable palmprint templates based on random measurement and noise data for security and privacy-preserving authentication," *Comput. Secur.*, vol. 82, pp. 1–14, May 2019.

[6] L. Leng, A. Beng, and J. Teoh, "Alignment-free row-co-occurrence cancelable palmprint Fuzzy Vault," *Pattern Recognit.*, vol. 48, no. 7, pp. 2290–2303, Jul. 2015.
[7] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 1, p. 3, Dec. 2011.
[8] A. Juels, and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. ACM Conf. Comput. Commun. Secur.*, Nov. 1999, pp. 28–36.
[9] A. Juels and M. Sudan, "A fuzzy vault scheme," *Des., Codes Cryptogr.*, vol. 38, pp. 237–257, Feb. 2006.
[10] M. Blanton and M. Aliasgari, "Analysis of reusability of secure sketches and fuzzy extractors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1433–1445, Sep. 2013.
[11] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, Apr. 2001.
[12] J. Yagnik, D. Strelow, D. A. Ross, and R.-S. Lin, "The power of comparative reasoning," in *Proc. IEEE Int. Conf. Comput. Vis.*, Nov. 2011, pp. 2431–2438.
[13] Y.-L. Lai, A. Jin, and A. B. J. Teoh, "Cancellable iris template generation based on indexing-first-one hashing," *Pattern Recognit.*, vol. 64, pp. 105–117, Apr. 2017.
[14] Z. Jin, J. Y. Hwang, Y.-L. Lai, A. B. J. Teoh, and S. Kim, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 393–407, Feb. 2018.
[15] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1406–1420, Jun. 2018.
[16] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in *Proc. CVPR Worshop*, Jun. 2007, pp. 1–7.
[17] L. Zhang, L. Li, A. Yang, Y. Shen, and M. Yang, "Towards contactless palmprint recognition: A novel device, a new benchmark, and a collaborative representation based identification approach," *Pattern Recognit.*, vol. 69, pp. 199–212, Sep. 2017.
[18] C. Yu, H. Li, and X. Wang, "A SVD based image compression, encryption and identity authentication algorithm in cloud," *IET Image Process.*, pp. 1–10, Aug. 2019. doi: 10.1049/iet-ipr.2018.5912.
[19] *PolyU Palmprint Database*. Accessed: 2014. [Online]. Available: http://www.comp.polyu.edu.hk/~biometrics/
[20] Tongji University. (2017). *Tongji Contactless Palmprint Dataset*. [Online]. Available: https://cslinzhang.github.io/ContactlessPalm/
[21] B. Tams, P. Mih ilescu, and A. Munk, "Security considerations in minutiae-based fuzzy vaults," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 985–998, May 2015.
[22] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 103–117, Mar. 2010.
[23] J. Kim and A. B. J. Teoh, "One-factor cancellable biometrics based on indexing-first-order hashing for fingerprint authentication," in *Proc. 24th Int. Conf. Pattern Recognit. (ICPR)*, Beijing, China, Aug. 2018, pp. 3108–3113.
[24] M. S. Charikar, "Similarity estimation techniques from rounding algorithms," in *Proc. 34th Annu. ACM Symp. Theory Comput.*, May 2002, pp. 380–388.
[25] G. Li, B. Yang, C. Busch, and C. Rathgeb, "Towards generating protected fingerprint templates based on Bloom filters," in *Proc. Int. Workshop Biometrics Forensics (IWBF)*, Mar. 2015, pp. 1–6.
[26] M. J. Lee, Z. Jin, and A. B. J. Teoh, "One-factor cancellable scheme for fingerprint template protection: Extended feature vector (EFV) hashing," in *Proc. IEEE Int. Workshop Inf. Forensics Security (WIFS)*, Hong Kong, Dec. 2018, pp. 1–7.
[27] J. Bringer, C. Morel, and C. Rathgeb, "Security analysis of Bloom filter-based iris biometric template protection," in *Proc. Int. Conf. Biometrics (ICB)*, May 2015, pp. 527–534.
[28] X. Dong, Z. Jin, and A. B. J. Teoh, "A genetic algorithm enabled similarity-based attack on cancellable biometrics," 2019. *arXiv:1905.03021*. [Online]. Available: https://arxiv.org/abs/1905.03021
[29] S. Wang, G. Deng, and J. Hu, "A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognit.*, vol. 61, pp. 447–458, Jan. 2017.
[30] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.
[31] Y. Chen, Y. Wo, C. Wu, G. Han, and R. Xie, "Deep secure quantization: On secure biometric hashing against similarity-based attacks," *Signal Process.*, vol. 154, pp. 314–323, Jan. 2019.
[32] D. D. Mohan, N. Sankaran, S. Tulyakov, S. Setlur, and V. Govindaraju, "Significant feature based representation for template protection," in *Proc. ICCV*, Jun. 2019. [Online]. Available: http://openaccess.thecvf.com/content_CVPRW_2019/papers/Biometrics/Mohan_Signi_cant_Feature_Based_Representation_for_Template_Protection_CVPRW_2019_paper.pdf
[33] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, Jun. 2018.
[34] M. Hammad, G. Luo, and K. Wang, "Cancelable biometric authentication system based on ECG," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 1857–1887, Jan. 2019.
[35] M. Hammad, Y. Liu, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, vol. 7, pp. 26527–26542, 2019.
[36] M. Hammada and K. Wang, "Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network," *Comput. Secur.*, vol. 81, pp. 107–122, Mar. 2019.
[37] A. Genovese, V. Piuri, F. Scotti, and K. N. Plataniotis, "PalmNet: Gabor-PCA convolutional networks for touchless palmprint recognition," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3160–3174, Dec. 2019.
[38] W. Jia, R.-X. Hu, Y.-K. Lei, Y. Zhao, and J. Gui, "Histogram of oriented lines for palmprint recognition," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 3, pp. 385–395, Mar. 2014.
[39] L. Fei, J. Wen, K. Yan, Z. Zhong, and Z. Zhang, "Local multiple directional pattern of palmprint image," in *Proc. 23rd Int. Conf. Pattern Recognit. (ICPR)*, Dec. 2016, pp. 3013–3018.
[40] Y.-T. Luo, L.-Y. Zhao, B. Zhang, W. Jia, F. Xue, J.-T. Lu, Y.-H. Zhu, and B.-Q. Xu, "Local line directional pattern for palmprint recognition," *Pattern Recognit.*, vol. 50, pp. 26–44, Feb. 2016.
[41] I. Rida, S. Al-Maadeed, A. Bouridane, S. Bakshi, and A. Mahmood, "Palmprint identification using an ensemble of sparse representations," *IEEE Access*, vol. 6, pp. 3241–3248, 2018.
[42] L. Fei, B. Zhang, Y. Xu, Z. Guo, J. Wen, and W. Jia, "Learning discriminant direction binary palmprint descriptor," *IEEE Trans. Image Process.*, vol. 28, no. 8, pp. 3808–3820, Aug. 2019.
[43] H. Li, J. Zhang, and L. Wang, "Robust palmprint identification based on directional representations and compressed sensing," *Multimedia Tools Appl.*, vol. 70, no. 3, pp. 2331–2345, Jun. 2014.
[44] A. Z. Broder, M. Charikar, M. Mitzenmacher, and A. M. Frieze, "Min-wise independent permutations," *J. Comput. Syst. Sci.*, vol. 60, no. 3, pp. 630–659, Jun. 2000.
[45] O. Chum, J. Philbin, and A. Zisserman, "Near duplicate image detection: Min-hash and TF-IDF weighting," in *Proc. BMVC*, Sep. 2008, pp. 812–815.
[46] V. E. Liong, J. Lu, P. Moulin, J. Zhou, and G. Wang, "Deep hashing for compact binary codes learning," in *Proc. CVPR*, Jun. 2015, pp. 2475–2483.

XIYU WANG received the bachelor's degree from the University of Jinan, in 2017, where she is currently pursuing the master's degree with the Shandong Provincial Key Laboratory of Network-Based Intelligent Computing. Her research interests include biometric privacy protection, image processing, and signal processing.

HENGJIAN LI received the B.S. and Ph.D. degrees from Southwest Jiaotong University, Chengdou, China, in 2004 and 2010, respectively. He is currently an Associate Professor with the School of Information Science and Engineering, University of Jinan, China. He has published over 30 articles and holds more than ten patents. His research interests include image processing and pattern recognition, biometrics protection, and cloud security.