An Efficient Privacy-Preserving Palmprint Authentication Scheme Based on ElGamal

Yong Ding[1], Huiyong Wang[2(✉)], Zhiqiang Gao[2], Yujue Wang[1], Kefeng Fan[3], and Shijie Tang[4]

[1] Guangxi Key Laboratory of Cryptography and Information Security, School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, People's Republic of China
[2] School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin 541004, People's Republic of China
why608@163.com
[3] China Electronics Standardization Institute, Beijing 100007, People's Republic of China
[4] School of Electronic Engineering and Automation, Guilin University of Electronic Technology, Guilin 541004, People's Republic of China

Abstract. Biometric credentials have become a popular means of authentication. However, since biometrics are unique and stable, one data breach might cause the user lose some of his biometrics permanently. And the stolen biometrics may be used for identity fraud, posing a permanent risk to the user. There have been many studies addressing this problem, in which the protection of biometric templates is a basic consideration. However, most existing solutions have inefficient security or efficiency. In this paper, we use the ElGamal scheme which shows good performance in applications to construct an efficient, privacy-preserving palmprint authentication scheme. We first construct a palmprint recognition scheme based on palm lines and feature points with good performance. Then, we use the RP (random projection) method to effectively reduce the extracted palmprint features, which greatly reduces the volume of data to be stored. Finally, we design a confidential comparison process based on the ElGamal scheme to perform efficient comparisons of palmprint features while ensuring provable security. Subsequent theoretical analysis/proof and a series of experiments prove the significance and validity of our work.

Keywords: Biometric · Palmprint · ElGamal · Random projection

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2019
Published by Springer Nature Switzerland AG 2019. All Rights Reserved
J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 246–267, 2019.
https://doi.org/10.1007/978-3-030-21373-2_19

1 Introduction

1.1 Biometric Authentication and Some Security Concerns

Traditionally, identification methods can be classified into two categories: token-based (e.g., using a physical key, an ID card, and a passport), and knowledge-based (e.g., using a password). However, these approaches both have some limitations. In token-based approaches, the token can be easily stolen or lost. In knowledge-based approaches, the knowledge can be guessed or forgotten. Compared with traditional approaches, biometrics (fingerprint, palmprint, face, iris, voice, etc.) are more accurate, portable and user friendly. As a result, biometrics have emerged as a powerful means for authentication [1] in recent years.

Biometrics are also known as biometric authentication, referring to the process of extracting the characteristics of an individual's physiological characteristics or personal behavior by using automatic technology, and comparing these characteristics with the existing templates stored in the database, so as to verify an individual's identity [2].

Nevertheless, biometrics has also accumulated many security and privacy concerns, for they are susceptible to many threats. On the one hand, human biometrics are unique and stable, which means that in case of information theft, it is impossible to withdraw the stolen biometrics and re-register them. However, it is very difficult to protect some biometrics from being maliciously collected, such as face, gait, sound, and the picture might be enough for an identity fraud or individual profiling and tracking. On the other hand, if biometrics are transmitted and stored in plain text, it is easy to cause large-scale data leakage when subjected to external and internal attacks. For example, Aadhaar, the world's largest biological (iris) identification database project launched in India in 2009, has produced a large amount of evidence of personal information abuse [3].

Thus, how to build a privacy-preserving biometric authentication system (BAS) which can effectively mitigate the aforementioned privacy and security risks has become an important issue.

A typical biometric authentication system (Fig. 1) is an access control system equipped with biometric acquisition devices. It can be classified into two categories according to the purpose of the tasks [4]: verification and identification. The task of a verification system is to determine whether the individual to be authenticated is a legitimate user. Such systems are often used as an access mechanism for certain systems, such as unlocking mobile phones with fingerprints. They usually require a one-to-one comparison of the user's biometric feature with a particular record (a stored feature template) in the database. The task of identification is to use biometrics to find an individual's identity without knowing any of his personal information. Usually, the user data is compared with a plurality of records in the database, and the workload is larger than verification. Most identification systems are used in passive ways, such as screening a mass of people to locate certain suspects in public environments. The above two tasks both include two stages: registration and authentication. During the registration phase, the user (active or passive) enters a certain biometric feature

along with his identity using an acquisition sensor, then the biometric feature is transformed (or encrypted) into a template and stored to the database. In the authentication phase, a verification system calls the acquisition device to re-acquire a fresh biometric feature of the client, then finds the record by the proposed identity in the database (if it exists), and compare the fresh template and the stored template to decide whether they belong to a same person. In contrast, an identification system compares the fresh template and nonspecific multiple templates to check if a template belonging to the client is stored in the database, so as to find his identity.

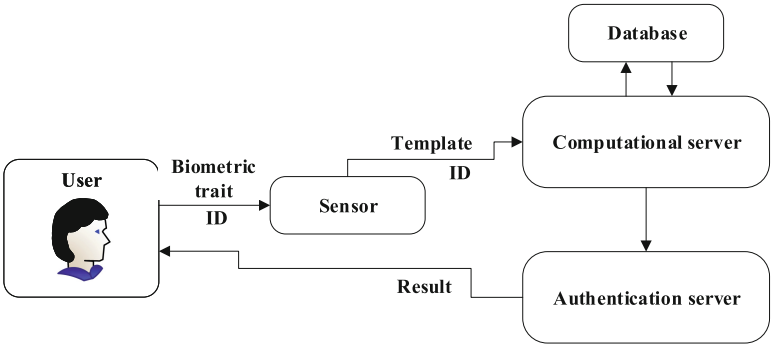

Fig. 1. The authentication phase in a BAS with a distributed architecture.

Generally, it is believed that unauthorized access to biometric templates is the greatest threat to biometrics security [5]. As a result, many template protection schemes were proposed, which can be classified into two categories [7]: transformation based schemes and crypto-based schemes. Transformation based methods use invertible or non-invertible functions to transform biometrics into unreadable templates, so that no information about the original biometric feature should be leaked in case of a theft. Meanwhile, crypto-based schemes turn to cryptography techniques to protect biometrics from leaking.

In the family of biometrics, palmprint is a promising member, for human palms have Larger region and provide more information than other biometrics, such as fingers, iris and retina. As a result, palm features can be extracted even from a low resolution image, and easier to achieve a high accuracy in authentication [6].

1.2 Related Work

A biometric template method should have the following properties [8]:

Diversity: The templates for the same biometric trait stored in multiple databases should be diverse enough, so that none data can be comprised under cross matching attacks.

Revocability: A stolen biometric should be revoked and replaced.

Security: A leaked template should not reveal inform about the original biometrics.

Performance. The performance of an authentication system should be degraded heavily due to any template protection methods.

It is not easy to build a template protection scheme which satisfies the above conditions, and the standard encryption schemes like RSA, AES, etc. cannot be used to encrypt the templates [7].

The following schemes are representative of transformation-based template protection schemes

Biohashing or biometric salting was proposed by Teoh et al. [9] and Ngo et al. [10] as an invertible transformation technique, and were applied to several biometrics like fingerprints [11,12], iris [13,14], and palmprints [15].

In 2005, Sutcu et al. [16] proposed a non-invertible method based on cryptographic hash functions. In 2006 and 2007, Ratha et al. [17,18] used three non-invertible transformations to generate secure fingerprint templates. And in 2008, Zuo et al. [19] proposed several ways to construct cancellable iris biometrics.

In crypto-based template protection methods, the following schemes are representative.

In 1999, Juels and Wattenberg [20] introduced the concept of fuzzy commitment. In 2007, Teoh and Kim [21] proposed a finger template protection based on fuzzy commitment. And in 2006, Hao et al. [22] proposed the first fuzzy commitment scheme for iris. In 2006, Van Der Veen et al. [23] applied the fuzzy commitment technique to face authentication.

In 2002, Juels and Sudan [24] introduced the concept of fuzzy vault, and in 2003, Clancy et al. [25] proposed and implemented the first fingerprint vault. In 2004, Uludag and jain [26] proposed the first finger-print based fuzzy vault. Lee et al. [27] and Wu et al. [28] proposed two fuzzy vault method for iris in 2007 and 2008.

In recent years, homomorphic encryption (HE) has shown great potential in constructing privacy-preserving biometric authentication systems. Homomorphic encryption (HE) allows us to compute arbitrary functions confidentially, which is in line with the need of privacy protection in cloud computing.

In 2014, Luo [29] uses the RSA algorithm to construct a blind authentication scheme, and built a palmprint authentication system on that basis. The system uses a three-layer architecture, which includes a client, a remote server and a trustworthy third party, which turned to be the critical defect of the architecture.

In 2015, Qu [30] summarized the application of homomorphic encryption in biometric authentication, and designed a palmprint authentication scheme based on HE. This scheme includes four stages: registration, authentication, update and cancellation. Yet this paper didn't give any specific experimental data, and no dimension reduction technique is used, leading to comparatively low efficiency.

In 2016 Erkin [31] used the mobile phone to acquire the palmprint images and build an authentication system. The resulting error recognition rate is 15.2%.

In 2017, Wang [32] proposed an effective privacy-preserving palmprint authentication scheme, which reduced the palmprint feature vector size from $128 * 128$ to $100 * 1$, and reached a correct recognition rate of 95%. But their scheme is susceptible to selective ciphertext attacks.

1.3 Our Contribution

Our contribution mainly includes the following aspects:

(1) We propose a palmprint verification scheme based on the extraction of palm ridge lines and achieves good performance.
(2) We use the RP method [34] to reduce the dimension of the feature vectors, and find the optimal balance between dimension reduction and performance.
(3) We propose a projection that maps binary vectors to prime vectors, which strengths the robustness of the encryption algorithm against chosen ciphertext attacks.

2 Image Processing and Feature Acquisition

2.1 Extracting ROI from Palmprint

The procedure consists of seven steps: (1) Select the palmprint image. (2) Smooth the original image.(3) Use a threshold to convert the smoothed image to a binary image. (4) Trace the boundary of the binary image. (5) Find the key points. (6) Build a palmprint coordinate system. (7) Crop a subimage with fixed size from the center of the image as ROI. The flow chart of the algorithm is shown in Fig. 2.

The details of each step are described in the following:

(1) Select the palmprint image I. The palmprint image can be captured by a CCD camera, a mobile phone or a Webcam. The most ideal palmprint image we select looks like Fig. 2(a), which satisfies that $\angle 1 < \angle 2$, $\angle 1 < \angle 4$, $\angle 3 < \angle 2$, $\angle 3 < \angle 4$. Namely, the angle between the index finger and the middle finger, the angle between the ring finger and the little finger are both smaller. Other angles between fingers are greater. This is because we will detect the valley points between the index–middle fingers and the ring–little fingers as key-points. We will explain the specific reasons at step (5). In this paper we take the palmprint image from PolyU databases (provided by Hong Kong Polytech University).
(2) Smooth the original image. We use a Low-pass filter to smooth the original image. The purpose is to make the image more smooth and convenient for binarization.

$$I_{SmoothMap} = I * A$$

(where A is the low-pass filter).

(3) Binarize the image. Use a threshold α to convert the original gray image into a binary map.

$$I_{binarymap} = \begin{cases} 1, I_{SmoothMap} > \alpha \\ 0, I_{SmoothMap} \leq \alpha \end{cases}.$$

(4) Trace the boundary of the palmprint. Use the boundary tracking operator to obtain the boundary of palmprint

$$I_{bounbary} = I_{binarymap} * B$$

where B is the boundary tracking operator.

(5) Detect the key points of the palmprint.
The area-method. We find that the image has the following characteristics: As shown in the Fig. 2(b), let the area of the circle be S, and when the center of the circle is at the A, B, F, the area of the intersection of the circle and the palm is approximately $1/2S$. When the center is at C, D, E, the intersection of the circle and the palm is approximately $3/4S$. If the input of the palmprint is an ideal image, and the appropriate radius is chosen so that the center of the circle moves along the edge of the palm to compute the area where the circle intersects with the palm. When the area reaches its maximum, the center of the circle is the first key point and then the neighborhood of the key point is removed and the second key point will be detected using the same way.
The arc-method. As shown in the Fig. 2(b), let the circumference of the circle be L, and when the center of the circle is at the A, B, F, the arc of the intersection of the circle and the palm is approximately $1/2L$. When the center is at C, D, E, the intersection of the circle and the palm is approximately $3/4L$. If the palmprint is ideal, when the appropriate radius is chosen so that the center of the circle moves along the edge of the palm to compute the area where the circle intersects with the palm, and the area reaches maximum, the center of the circle is the first key point and then the neighborhood of the key point is removed and the second key point will be detected using the same way.

(6) Create the Cartesian coordinate system. By the above steps, the key points C and E(the valley point between the index finger and the middle finger and the valley point between the ring finger and little finger) have been found. Then connect CE, and make a line parallel to line CE on the right side which intersect with each other at two points C_1E_1 with the boundary of palms, the midpoint of E_1C_1 is the origin of the coordinates, the direction of E_1C_1 is the y-axis, and the direction perpendicular to E_1C_1 is the x-axis (Fig. 2(c)). Those operations are based on the following reasons: Due to individual differences, sometimes CE might be too long or too short and may lead to an inappropriate ROI and E_1C_1. The length of E_1C_1 is approximate to the length of the palm. The shape of the same palm is not always same at different time, the distance of the two key points is not equal at

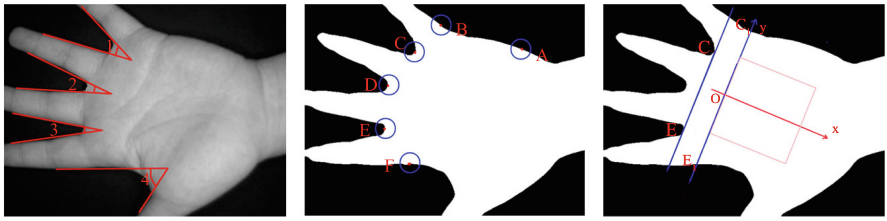

Fig. 2. Our ideal palmprint image.

different time. We select the width of palmprint as reference, since the width of the palm will not change.

(7) Extract ROI. With reference to the length of E_1C_1, a square area $\left([0, +\frac{d}{2}] \times [-\frac{d}{4}, +\frac{d}{4}]\right)$ whose length is equal to half of E_1C_1 is extracted as the ROI (Fig. 2(c)).

2.2 Extracting Features from ROI

The features of the palmprint are based on image features, digital features, texture features and main features. We use the image features and the texture features as the palmprint features.

(1) Extract the image feature of the palmprint. Firstly, we calculate the average gray value of the image and choose a threshold, then binarize the image. if the value of the image is greater than the threshold, set it to 1, otherwise set it to 0.

(2) Extract image texture feature. First, we calculate the sum of the horizontal and vertical gradients of each point, and obtain an image of a gradient value. Then we calculate the average gray value of the image and take it as a threshold. Finally we binarize the image. If the value of the image is greater than the threshold, let it be 1, otherwise 0.

(3) Extract the image feature based on LBP. The Local Binary Patterns method (LBP) is proposed by Ojala [33] and used for the description of texture features. The original operator of LBP is defined as follows: firstly, a window unit is set for each pixel in the image, and then the pixel is taken as the threshold of the pixel, and the remaining 8 pixels in the window are binarized. Then the weighted sum is used to get the LBP value of the point. The calculation of the LBP value for each pixel is shown as: $LBP = \sum_{i=0}^{7} B(g_i - g_c)2^i$, where g_c is the gray value of the center pixel and g_i is the gray value of a neighboring pixel, the two valued function is defined as follows:

$$B(x) = \begin{cases} 1, x > 0 \\ 0, x \leq 0 \end{cases}.$$

2.3 Dimension Reduction

We use the random projection (Rp) [34] method to reduce the dimension of the feature vector. Firstly we construct a matrix of $U = ml^2$, where m is the dimension to be descended, and l^2 is the dimension of the characteristic matrix. The concrete steps are as follows:

(1) Generate a random projection matrix: A random projection matrix U of ml^2 dimension is generated as follows:

$$U_{i,j} = \begin{cases} 1, p = 1/6 \\ 0, p = 1/6. \\ -1, p = 1/6 \end{cases}$$

(2) Reduction. The original feature matrix A is reduced by multiplying U to get the m dimension vector α.

$$\alpha = UA$$

(3) Binaryzation. The vector α is binarized and resulting vector β is obtained.

$$\beta_{(i,1)} = \begin{cases} 1, \alpha_{(i,1)} > 0 \\ 0, \alpha_{(i,1)} \leq 0 \end{cases}.$$

(4) The vector β is the target feature vector.

3 Confidential Comparison

3.1 The ElGamal Encryption Scheme

The security of the ElGamal encryption scheme [35] is based on hardness of solving the discrete logarithm problem on a cyclic group. It goes as follows.

Select a large prime number p, where $g(g < p)$ is the generator of cyclic group Z_p^*. Select a random number $x \in Z_p^*$, and calculate $y = g^x \ mod \ p$. Take array (y, g, p) as a public key and x as a private key.

Encryption: select a random number r, where r and $p-1$ are mutual prime, then compute ciphertext as:

$$E(m) = (a, b) = (g^r \ mod \ p, my^r \ mod \ p)$$

Decryption: compute:

$$m = b(a^x)^{-1} \ mod \ p = my^r((g^r)^x)^{-1} \ mod \ p = m(g^x)^r(g^{rx})^{-1} \ mod \ p$$

Since a random number is introduced to the encryption process, the encryption result of ElGamal is randomised, which enables the algorithm to resist selective ciphertext attacks (CPA). Besides, ElGamal is multiplicatively homomorphic.

3.2 Hamming Distance

Hamming distance [36] are often used to evaluate the similarity between two n-bit binary strings. Set $X, Y \in \{0,1\}^n$, the Hamming distance $H(X,Y)$ between X, Y is defined as:

$$H(X,Y) = \sum_{i=1}^{n}(x_i \oplus y_i)$$

In order to use Hamming distance to calculate the similarity between two eigenvectors, Wong et al. [37] proposed the definition of fraction Hamming distance, which was defined as:

$$H_F(X,Y) = \frac{1}{n}\sum_{i=1}^{n}(x_i \oplus y_i)$$

3.3 Our Scheme

We now describe the process of the matching phase. Note that the registration phase includes the former two steps of the matching phase.

The first step is to project the binary feature vectors to prime vectors. We assume the original binary feature vector is $x = (x_1, x_2, \ldots, x_n)$. Since the ElGamal encryption scheme can not encrypt 0 and 1, we propose the following projection to transform the binary feature vector into a prime vector:

$$x_i{}' = \begin{cases} a_i, x_i = 0 \\ pb_i, x_i = 1 \end{cases}.$$

where $x' = (x'_1, x'_2, \ldots, x'_n)$ and p is a prime number, a_i and b_i are non-zero random integers but not any multiple of p.

Obviously, this projection enables the proposed scheme to resist CPA attacks, for the mapping result varies in each trial.

The second step is to encrypt the prime vector by the ElGamal scheme. We calculate:

$$E(x') = (E(x'_1), E(x'_2), \ldots, E(x'_n))$$

and

$$E(y') = (E(y'_1), E(y'_2), \ldots, E(y'_n))$$

where $y = (y_1, y_2, \ldots, y_n)$ is a newly extracted feature vector for authentication. In registration, $E(x')$ will be stored to the database as the template.

The third step is the confidential comparison: For a newly extracted feature (fresh) vector $y = (y_1, y_2, \ldots, y_n)$ and its projection $y' = (y'_1, y'_2, \ldots, y'_n)$, calculate the bitwise product of the two vectors:

$$c = (c_1, c_2, \ldots, c_n) = (E(x'_1)E(y'_1),\ E(x'_2)E(y'_2),\ \ldots,\ E(x'_n)E(y'_n))$$

The fourth step is to calculate the Hamming distance: Decrypt ciphertext $c = (c_1, c_2, \ldots, c_n)$ with the private key sk and get $c' = (c'_1, c'_2, \ldots, c'_n)$.

$$d_i = \begin{cases} 1, c'_i \ mod\ p \equiv 0 \\ 0, c'_i \ mod\ p \not\equiv 0 \end{cases}.$$

$$d_i{}' = \begin{cases} 1, c_i' \ mod \ p^2 \equiv 0 \\ 0, c_i' \ mod \ p^2 \not\equiv 0 \end{cases}.$$

Then the fractional Hamming distance of x and y is

$$H_F(X,Y) = \frac{1}{n}\sum_{i=1}^{n}(d_i \oplus d_i')$$

The fourth step is to compare the fractional hamming distance with the preset threshold τ. If $H_F > \tau$, x and y are from a same individual; Otherwise, authentication fails.

4 Experiments

The proposed scheme is implemented with MATLAB 2013b on a desktop PC powered by a Intel(R) Xeon(R) CPU E5-2670 (2.60 GHz), and 8 GB random access memory.

4.1 Extrating ROI

We use the PolyU Palmprint Database provided by Hong Kong Polytech University, which contains 600 palmprint images of 100 person (each person has 6 palmprint images). The resolution of each image is 75dpi, and the size of each image is 384×284 pixcels. Their palmprint capture device includes ring source, CCD camera, lens, frame grabber, and A/D (analogue-to-digital) converter [1]. The images were collected by special equipments: the thumbs have been removed, the brightness is uniform and the valley points them are very obvious.

The specific steps are as follows:

(1) Read the original image $orignal\_I$ (Fig. 3(a)).
(2) Smooth the image with the sequential statistics filter (Fig. 3(b)).

$$ord\_I = ordfilt2(orignal\_I, 300, ones(20, 40)).$$

(3) Set the threshold and binarize the smoothed images (Fig. 3(c)).

$$I_{binarymap} = \begin{cases} 1, I_{ord} > 8 \\ 0, I_{ord} \leq 8 \end{cases}.$$

(4) Extract the edge of the image. We use four edge detection operators ([011], [110], [011]′, [110]′) to detect the boundary of $I_{binarymap}$, and get I_{edge} (Fig. 3(d)).
(5) Detect the key points. A circle C with a radius r along the edge image I_{edge} scans the binary image $I_{binarymap}$, when the area which the circle C intersect with the binary image $I_{binarymap}$ is maximal, the center of the circle is the first key K_1 (Fig. 3(e)), remove this point and its neighborhood (Fig. 3(f)), the second key point K_2 is got with the same method (Fig. 3(g)).

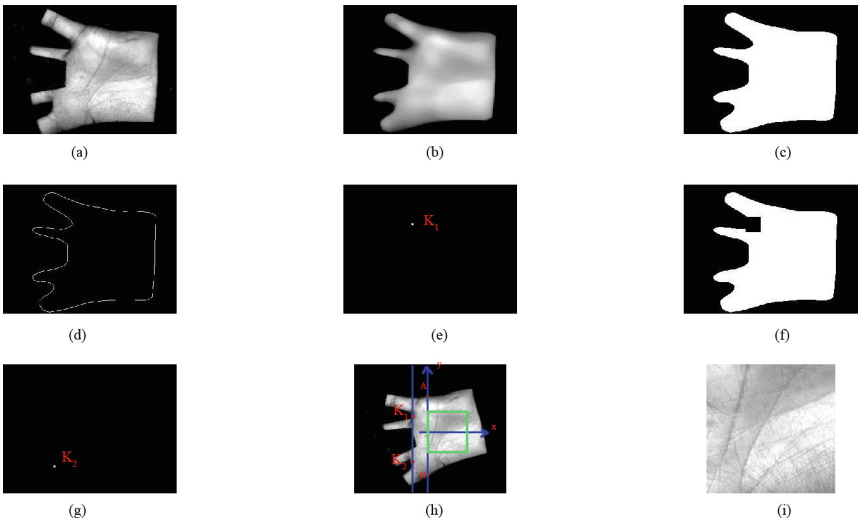

Fig. 3. The program runs on the polyU database.

(6) Build the coordinate system and extract ROI from palmprint. Connect K_1K_2, calculate the length of K_1K_2 l and the slope of K_1K_2 k; Rotate the original image $orignal\_I$ $tan^{-1}k$ to get $orignal\_I$' (Fig. 3(h)), correspondingly. Rotate K_1K_2 to $K_1'K_2'$, moves the line $K_1'K_2'$ by $1/4l$ unit to the right, which will intersect with the edge of the image at A and B. Then set the length of the line segment AB to d, then the midpoint of AB is the coordinate origin, the direction of BA is the y-axis, and the x-axis is perpendicular to the BA direction. Then we extract $[0, +\frac{d}{2}] \times [-\frac{d}{4}, +\frac{d}{4}]$ in the rotated image as the ROI (Fig. 3(i)).

The result of this experiment is shown in Tables 1 and 2. Table 3 gives the comparison results of our algorithm with several previous algorithms. Figure 4 shows the relationship between the correct extraction number and the radius. Figure 5 shows the relationship between the total extraction time and the radius.

Analysis of the results: we find that with the increase of the radius, the correct rate is also increased, and correspondingly the extraction time also becomes longer. When the radius is equal, the arc method has a shorter time and a higher recognition rate compared with the area method.

4.2 Plain-Text Matching

In this section, we use three different methods to extract palmprint features, and compare their performance. Since each person has 6 images, we use 2 images as template images, and the other 4 are used as fresh images.

Table 1. Experimental results of different radius (area-method)

Radii	Test images	Correct	Recognition rate (%)	Total time (s)	Averaging time (ms)
13	600	580	99.67	203.918	339
14	600	582	97.00	230.266	383
15	600	587	97.83	252.548	420
16	600	590	98.33	268.046	446
17	600	593	98.33	288.956	481
18	600	594	99.00	317.131	528
19	600	595	99.17	344.761	574
20	600	597	99.50	371.090	618
21	600	598	99.67	396.137	660
22	600	598	99.67	396.137	702
23	600	599	99.83	421.718	762
24	600	600	100	457.404	804
25	600	600	100	482.819	849
26	600	600	100	537.327	895
27	600	600	100	562.910	938

Table 2. Experimental results of different radius (arc-method)

Radii	Test images	Correct	Recognition rate (%)	Total time (s)	Averaging time (ms)
13	600	591	98.50	202.058	336
14	600	596	99.33	220.301	337
15	600	596	99.33	239.395	398
16	600	598	99.67	259.870	433
17	600	598	99.67	275.202	458
18	600	599	99.83	299.360	498
19	600	599	99.83	325.165	541
20	600	600	100	345.969	576
21	600	600	100	372.364	620
22	600	600	100	402.543	670
23	600	600	100	426.053	710
24	600	600	100	455.431	759
25	600	600	100	476.773	794
26	600	600	100	519.209	865
27	600	600	100	548.246	913

Table 3. Comparison results of different algorithms

Algorithms	Published year	Correction rate of location (%)
Proposed by [38]	2004	97.8
Proposed by [39]	2012	98.83
Proposed by this paper	2017	100

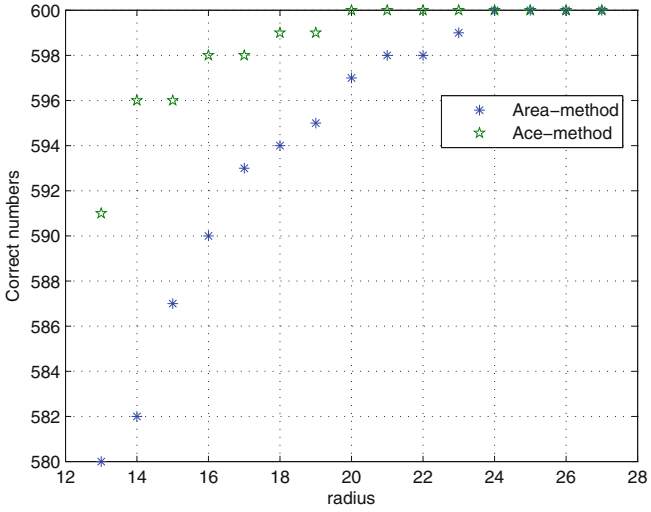

Fig. 4. The relationship between the correct extraction number and the radius.

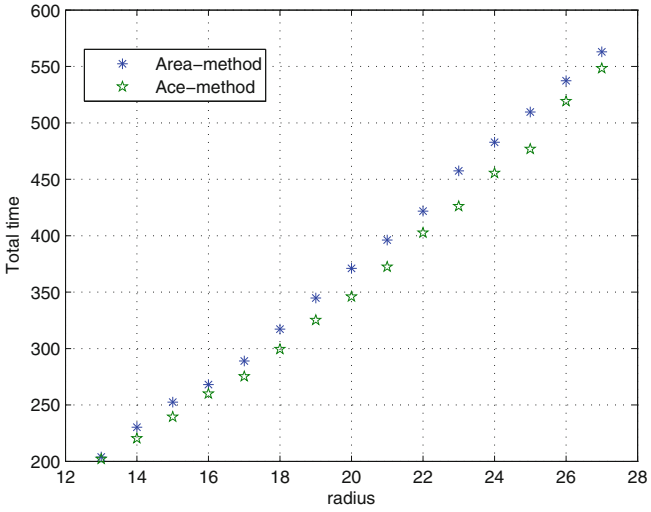

Fig. 5. The relationship between the total extraction time and the radius.

The Image Feature Method. In this method, the palmprint ROI comes directly from the binarization of the image, and the binarized image matrix is used as the feature matrix.

The Texture Feature Method. The procedure is divided into two steps. The first step is to obtain the gradient image of the ROI, and the second step is:

use the average gray value method to binarize the gradient image, and take the obtained binarized matrix as the feature matrix.

The LBP Method. First, we use the LBP method to get the LBP encoding of palmprint, then we use Gauss filter to smooth it. Finally, we use the average gray value method to binarize the image.

Analysis of the Experimental Results. The experimental results show that the LBP method is obviously better than the other two methods. When the recognition rate is 99%, the error recognition rate of the image method, the texture method and the LBP method are 4%, 5% and 0.1% respectively; When the recognition rate is 95%, the error recognition rate of the image method, the texture method and the LBP method are 0.5%, 0.1% and 0.003% respectively; When the recognition rate is 90%, the error recognition rate of the image method, the texture method and the LBP method is 0.2%, 0.03% and 0% respectively. It is obvious that the feature area extracted by the LBP method is very large. The hamming distances between different people are basically within $[0.39, 0.41]$, and

Table 4. Experimental results based on image feature method

Threshold	Correct recognition rate (%)	Error recognition rate (%)
0.34	100	34.492
0.33	100	27.03
0.32	100	20.773
0.31	99.75	15.558
0.3	99.5	11.154
0.29	99.5	7.828
0.28	99	5.455
0.27	99	3.664
0.26	98.75	2.439
0.25	98.75	1.654
0.24	98.25	1.121
0.23	97.5	0.717
0.22	94.5	0.437
0.21	93	0.263
0.2	88.25	0.124
0.19	83.25	0.063
0.18	79	0.033
0.17	76.5	0.015
0.16	68.75	0.003

Table 5. Experimental results based on texture feature method

Threshold	Correct recognition rate (%)	Error recognition rate (%)
0.4	100	76.144
0.395	100	53.141
0.39	99.75	33.003
0.385	99.75	18.467
0.38	99	9.816
0.375	99	4.866
0.37	98.75	2.371
0.365	98	1.187
0.36	97.5	0.629
0.355	96.75	0.311
0.35	95.75	0.177
0.345	94.75	0.098
0.34	94	0.048
0.335	92.5	0.038
0.33	90.75	0.03
0.325	89.5	0.023
0.32	88	0.013
0.315	85.5	0.005
0.31	82.75	0.005
0.305	79.5	0.005
0.3	75	0.003

the distances for the same person is around 0.36. This implies that the optimal threshold value can be set to 0.375 (Table 4).

Comparisons. The equal error rate is the recognition rate when the false acceptance rate is equal to the true rejection rate. The equal error rate is an important index to measure the quality of a biometric system. When the equal error rate becomes lower, the system becomes better.

4.3 Dimension Reduction

The feature matrix we derived is in size of 128×128. In order to reduce the storage cost and improve the efficiency of the subsequent encryption steps, we use the RP method to reduce the dimension of the original feature matrix. We also carry out matching experiments on the results after dimension reduction.

Table 6. Experimental results based on texture feature method

Threshold	Correct recognition rate (%)	Error recognition rate (%)
0.4	100	96.202
0.395	100	66.677
0.39	100	29.172
0.385	100	10.975
0.38	99.75	4.01
0.375	99.25	1.374
0.37	99.25	0.465
0.365	99.25	0.174
0.36	98.75	0.063
0.355	98.5	0.038
0.35	98.25	0.028
0.345	97.75	0.023
0.34	97.25	0.02
0.335	96.25	0.018
0.33	96	0.01
0.325	96	0.005
0.32	95.25	0.003
0.315	93.75	0

Table 7. Comparison of equal error rates of different palmprint recognition systems

Palmprint system	Proposed year	Error recognition rate
Proposed by [6]	2014	2.36%
Proposed by [32]	2017	1.22%
Proposed by this paper	2018	0.12%

Dimension Reduction with Features from the Image Method. In order to verify the feasibility of the dimension reduction, it is necessary to compare the matching results. We first match the extracted features based on image method. We test the performance of matching with features reducted to 100 bits, 200 bits, 300 bits, 400 bits, and 1000 bits respectively. The results are as follows (Table 5).

Analysis of the Result. Since the dimension reduction process may cause information loss, the matching results are not as good as from the original data. And since the reduction process carries out two calculations, it causes greater loss of information. For two 1000-bit vectors, when the recognition rate is 97%,

Table 8. Matching experimental results to 100 dimension

Threshold	Correct recognition rate (%)	Error recognition rate (%)
0.27	100	84.497
0.26	99.75	77.197
0.25	99.25	68.091
0.24	99.25	68.091
0.23	98.75	46.326
0.22	98.75	46.326
0.21	97	35.417
0.2	88.75	16.97
0.19	88.75	16.97
0.18	83.75	10.487
0.17	64.5	3.376
0.16	64.5	3.376
0.15	52.75	1.662
0.14	28.75	0.311
0.13	19	0.101
0.12	9.5	0.033
0.11	9.5	0.033

Table 9. Matching experimental results to 300 dimension

Threshold	Correct recognition rate (%)	Error recognition rate (%)
0.29	100	87.301
0.28	99.75	74.174
0.27	99.5	60.598
0.26	99.25	45.386
0.25	98.25	30.914
0.24	97	22.556
0.23	94	10.601
0.22	92.5	6.636
0.21	83.75	3.023
0.2	67	0.924
0.19	57.75	0.482
0.18	44.75	0.167
0.17	29.25	0.028
0.16	21.25	0
0.15	13	0

Table 10. Matching experimental results to 1000 dimension

Threshold	Correct recognition rate (%)	Error recognition rate (%)
0.27	100	46.737
0.26	99.75	30.316
0.25	99	17.394
0.24	99	9.417
0.23	97.5	3.838
0.22	95.25	1.715
0.21	88.5	0.616
0.2	79.25	0.177
0.19	66.75	0.081
0.18	51.5	0.015
0.17	35	0.003
0.16	22.75	0

the error recognition rate is 3%, which shows that the dimension reduction is also practical.

Comparison of Experimental Results. Jong-Hyuk et al. [40] also applied the RP method to palmprint recognition, but the result is not particularly satisfactory. The following results show the comparison of equal error rates with Jong-Hyuk's work.

Table 11. Comparison of equal error rates with Jong-Hyuk dimension reduction

Dimensionality reduction method	Proposed year	Equal error rate (%)
Proposed by [40]	2016	15
Reduced to 100 dimensions by this paper	2018	13
Reduced to 200 dimensions by this paper	2018	8
Reduced to 300 dimensions by this paper	2018	7
Reduced to 400 dimensions by this paper	2018	6
Reduced to 1000 dimensions by this paper	2018	3

4.4 Confidential Matchings

We take 13 as the sk and $(78443, 97, 99991)$ as the pk. Map 1 to a multiplier of 17 and map 0 to a random number less then 17. Assume m_1 and m_2 are two binary vectors, x_1 and x_2 are two prime vectors derived with our method.

Table 12. Security comparison experiment

m_1	m_2	x_1	x_2	c_1	c_2	c	d	d_1	d_2	D	M
1	0	85	16	(20808, 46841)	(59922, 6092)	(69197, 81049)	1360	1	0	1	1
1	1	119	34	(139, 27588)	(21674, 48111)	(12956, 5734)	4046	1	1	0	0
0	0	14	9	(55692, 25926)	(2833, 67173)	(89629, 83942)	126	0	0	0	0
1	1	170	153	(82541, 95541)	(78443, 30557)	(46440, 9110)	26010	1	1	0	0
1	1	272	34	(86608, 84838)	(353, 70687)	(75369, 83472)	9248	1	1	0	0
1	0	68	15	(23963, 9973)	(2833, 11964)	(93281, 27709)	1020	1	0	1	1
1	0	238	15	(49067, 16968)	(88153, 44192)	(92564, 17347)	3570	1	0	1	1
0	0	11	8	(17256, 79985)	(89373, 76198)	(59295, 45598)	88	0	0	0	0
1	0	68	13	(51504, 23205)	(59295, 49914)	(4558, 58617)	884	1	0	1	1
0	0	8	3	(18556, 6285)	(52128, 28379)	(74225, 78062)	24	0	0	0	0
1	0	119	10	(96329, 83887)	(49067, 65413)	(473, 94224)	1190	1	0	1	1
1	1	170	85	(88153, 34218)	(92863, 14330)	(88851, 88067)	14450	1	1	0	0
1	1	221	136	(12956, 64173)	(22666, 25232)	(87120, 58873)	30056	1	1	0	0
0	1	2	238	(18556, 26569)	(33016, 1495)	(39, 24228)	476	1	0	1	1
1	0	238	4	(88153, 27907)	(8183, 60947)	(20925, 1019)	952	1	0	1	1
0	1	14	85	(86368, 61809)	(78443, 5866)	(74819, 4228)	1190	1	0	1	1
0	0	6	8	(13186, 43787)	(90928, 64994)	(84518, 48427)	48	0	0	0	0
1	1	119	102	(2840, 91412)	(42743, 53932)	(1046, 75720)	12138	1	1	0	0
1	1	170	221	(13483, 14669)	(78234, 43950)	(23963, 60573)	37570	1	1	0	0
0	0	12	16	(59695, 8260)	(26609, 3568)	(67220, 74326)	192	0	0	0	0
1	1	204	51	(98163, 66133)	(34241, 49136)	(1818, 3570)	10404	1	1	0	0
1	1	221	68	(51606, 5421)	(23963, 9973)	(45881, 68493)	15028	1	1	0	0

Take c_1 and c_2 as the result of encryption for x_1 and x_2, and c as the result of $c_1 \times c_2$, d as the result of decryption of c. d_1, d_2, D, M is given by the following formula (Tables 6, 7, 8, 9, 10, 11 and 12).

If $d \ mod \ 17 \equiv 0$, then $d_1 = 1$, otherwise $d_1 = 0$; if $d \ mod \ 289 \equiv 0$, then $d_2 = 1$, otherwise $d_2 = 0$; $D = d_1 \oplus d_2$, $M = m_1 \oplus m_2$.

5 Conclusion

We have proposed an privacy-preserving palmprint authentication scheme. First we employ three algorithms to extract feature vectors from plamprint images and compared their performance. Then we use the RP method to reduce the dimension of the feature vector. Finally, we use ElGamal to implement confidential comparisons. Experiments show that the scheme can meet practical requirements in small or media application scenarios.

Acknowledgements. This work was partially supported by the National Natural Science Foundation of China (Grant Nos. 61772150, 61862012), the National Cryptography Development Fund of China under project MMJJ20170217, the Guangxi

Key R&D Fund under project AB17195025, the Guangxi Natural Science Foundation under grant 2018GXNSFAA281232, and the open project of Guangxi Key Laboratory of Cryptography and Information Security (Grant Nos. GCIS201622, GCIS201702).

References

1. Zhang, D., Kong, W.K., You, J., et al.: Online palmprint identification. IEEE Trans. Pattern Anal. Mach. Intell. **25**(9), 1041–1050 (2003)
2. Jain, A.K., Flynn, P., Ross, A.A.: Handbook of Biometrics. Springer, New York (2008). https://doi.org/10.1007/978-0-387-71041-9
3. Aadhaar: India top court upholds world's largest biometric scheme. BBC News, 26 September 2018. https://www.bbc.com/news/world-asia-india-44777787
4. Pagnin, E., Mitrokotsa, A.: Privacy-preserving biometric authentication: challenges and directions. Secur. Commun. Netw. **2017**, 1–9 (2017)
5. Tuyls, P., Škoric, B., Kevenaar, T. (eds.): Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-counterfeiting. Springer, London (2007). https://doi.org/10.1007/978-1-84628-984-2
6. Han, Y., Sun, Z., Wang, F., Tan, T.: Palmprint recognition under unconstrained scenes. In: Yagi, Y., Kang, S.B., Kweon, I.S., Zha, H. (eds.) ACCV 2007. LNCS, vol. 4844, pp. 1–11. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76390-1_1
7. Riaz, N., Riaz, A., Khan, S.A.: Biometric template security: an overview. Sens. Rev. **38**(1), 120–127 (2018)
8. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP J. Adv. Signal Process. **2008**, 113 (2008)
9. Teoh, A.B.J., David, C.L.N., Goh, A.: Personalised cryptographic key generation based on FaceHashing. Comput. Secur. **23**(7), 606–614 (2004)
10. Ngo, D.C.L., Andrew, B.J.T., Goh, A.: Biometric hash: high-confidence face recognition. IEEE Trans. Circuits Syst. Video Technol. **16**(6), 771–775 (2006)
11. Ong, T.S., Jin, A.T.B., Ngo, D.C.L.: Application-specific key release scheme from biometrics. IJ Netw. Secur. **6**(2), 127–133 (2008)
12. Jin, A.T., Beng, D.N., Ling, C., Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognit. **37**(11), 2245–2255 (2004)
13. Chin, C.S., Jin, A.T.B., Ling, D.N.C.: High security iris verification system based on random secret integration. Comput. Vis. Image Underst. **102**(2), 169–177 (2006)
14. Chong, S.C., Teoh, A.B.J., Ngo, D.C.L.: Iris authentication using privatized advanced correlation filter. In: Zhang, D., Jain, A.K. (eds.) ICB 2006. LNCS, vol. 3832, pp. 382–388. Springer, Heidelberg (2005). https://doi.org/10.1007/11608288_51
15. Connie, T., et al.: PalmHashing: a novel approach for cancelable biometrics. Inf. Process. Lett. **93**(1), 1–5 (2005)
16. Sutcu, Y., Sencar, H.T., Memon, N.: A secure biometric authentication scheme based on robust hashing. In: Proceedings of the 7th Workshop on Multimedia and Security, pp. 111–116. ACM (2005)
17. Ratha, N., et al.: Cancelable biometrics: a case study in fingerprints. In: 18th International Conference on Pattern Recognition. ICPR, vol. 4, pp. 370–373. IEEE (2006)
18. Ratha, N.K., et al.: Generating cancelable fingerprint templates. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 561–572 (2007)

19. Zuo, J., Ratha, N.K., Connell, J.H.: Cancelable iris biometric. In: International Conference on Pattern Recognition, pp. 1–4. IEEE (2008)
20. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: ACM Conference on Computer and Communications Security, pp. 28–36. ACM (1999)
21. Teoh, A.B.J., Kim, J.: Secure biometric template protection in fuzzy commitment scheme. IEICE Electron. Express **4**(23), 724–730 (2007)
22. Hao, F., Anderson, R., Daugman, J.: Combining crypto with biometrics effectively. IEEE Trans. Comput. **55**(9), 1081–1088 (2006)
23. Van Der Veen, M., et al.: Face biometrics with renewable templates. In: Security, Steganography, and Watermarking of Multimedia Contents VIII, Vol. 6072, p. 60720J. International Society for Optics and Photonics (2006)
24. Juels, A., Sudan, M.: A fuzzy vault scheme. Des. Codes Cryptogr. **38**(2), 237–257 (2006)
25. Clancy, T.C., Kiyavash, N., Lin, D.J.: Secure smart card based fingerprint authentication. In: Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications, pp. 45–52. ACM (2003)
26. Uludag, U., Jain, A.K.: Fuzzy fingerprint vault. In: Proceedings of the Workshop: Biometrics: Challenges Arising from Theory to Practice, pp. 13–16 (2004)
27. Li, C., Jiankun, H.: A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures. IEEE Trans. Inf. Forensics Secur. **11**(3), 543–555 (2016)
28. Wu, X., et al.: A novel cryptosystem based on iris key generation. In: Fourth International Conference on Natural Computation, ICNC 2008, vol. 4, pp. 53–56. IEEE (2008)
29. Luo, Z.: Research on blind identity authentication protocol based on biometrics. Ph.D. thesis, Beijing Jiaotong University, Beijing (2014)
30. Qu, Y.: Research on palmprint authentication based on homomorphic encryption. Ph.D. thesis, Southwest Jiaotong University (2015)
31. Erkin, Z., Franz, M., Guajardo, J., Katzenbeisser, S., Lagendijk, I., Toft, T.: Privacy-preserving face recognition. In: Goldberg, I., Atallah, M.J. (eds.) PETS 2009. LNCS, vol. 5672, pp. 235–253. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03168-7_14
32. Wang, H., Ding, Y., Tang, S., Wang, J.: An efficient privacy-preserving palmprint authentication scheme based on homomorphic encryption. In: Wen, S., Wu, W., Castiglione, A. (eds.) CSS 2017. LNCS, vol. 10581, pp. 503–512. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-69471-9_39
33. Ojala, T., Pietikäinen, M., Harwood, D.: A comparative study of texture measures with classification based on featured distributions. Pattern Recognit. **29**(1), 51–59 (1996)
34. Achlioptas, D.: Database-friendly random projections: Johnson-Lindenstrauss with binary coins. J. Comput. Syst. Sci. **66**(4), 671–687 (2003)
35. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory **31**(4), 469–472 (1985)
36. Aykut, M., Ekinci, M.: Developing a contactless palmprint authentication system by introducing a novel ROI extraction method. Image Vis. Comput. **40**, 65–74 (2015)
37. Wong, K.-S., Kim, M.-H.: A privacy-preserving biometric matching protocol for iris codes verification. In: 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC), pp. 120–125. IEEE (2012)

38. Wu, X., Wang, K., Zhang, D.: HMMs based palmprint identification. In: Zhang, D., Jain, A.K. (eds.) ICBA 2004. LNCS, vol. 3072, pp. 775–781. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-25948-0_105
39. Wu, G., et al.: A contour extraction algorithm of palmprints based on corner point features. In: 2012 IEEE International Conference on Automation and Logistics (ICAL), pp. 501–505. IEEE (2012)
40. Wang, Y., Malluhi, Q.M.: Privacy preserving computation in cloud using noise-free fully homomorphic encryption (FHE) schemes. In: Askoxylakis, I., Ioannidis, S., Katsikas, S., Meadows, C. (eds.) ESORICS 2016. LNCS, vol. 9878, pp. 301–323. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-45744-4_15