A PSEUDO-SPlicing ALGORITHM FOR
PARTIAL FINGERPRINT RECOGNITION
BASED ON SIFT

Zheng Zhu, Aiping Li*, Rong Jiang, Yulu Qi, Dongyang Zhao, Yan Jia
School of Computer Science,
National University of Defense Technology, Changsha 410073, China

ABSTRACT

At present, many fingerprint recognition techniques are applied to public infrastructures. Their
targets are mainly for normal-sized fingerprints. However, with the rise of small-sized fingerprint
sensors, the acquired partial fingerprints containing only part of information of the finger, which
causes that many researchers change their research directions to partial fingerprint recognition.
This paper proposes a SIFT-based pseudo-splicing partial fingerprint recognition algorithm.
This algorithm uses the SIFT algorithm to pseudo-splice the input fingerprints during the
fingerprint enrollment to increase the robustness of the fingerprint feature database. The
comparisons of the accuracy of the recognition among this algorithm, the minutia-based
fingerprint recognition algorithm and the fingerprint recognition algorithm based on image
similarity, that shows the first performs well. Moreover, this paper proposes an algorithm to
evaluate the quality of partial fingerprint by calculating the invalid blocks of fingerprint image.
The result shows that the evaluation algorithm can effectively filter out low-quality fingerprints.

KEYWORDS

Fingerprint Recognition, SIFT, Partial Fingerprint, Pseudo-splicing

1. INTRODUCTION

In recent years, fingerprint recognition techniques have been widely applied to various areas[1],
such as management, access control, finance, public security and cyber security etc. With the
popularity of fingerprint recognition techniques, it has been used on a large scale in the security
verification of mobile terminals (mobile phones, personal computers, tablet computers, etc.). In
the common fingerprint recognition techniques, the size of the fingerprint scanners is generally
1" × 1" or even larger[3]. Many minutia-based fingerprint recognition algorithms are effective in
these size[4]. With the commercialization of fingerprint recognition techniques, the requirement
that have better and smaller scanners is increasing. Miniaturization of fingerprint sensors has led to
small sensing areas usually varying from 1" × 1" to 0.42" × 0.42" [5]. However, fingerprint
scanners with a sensing area smaller than 0.5" × 0.7", which is considered to be the average
fingerprint size[6], can only capture partial fingerprints. These partial fingerprints contain much
fewer features than full fingerprints and it may be rotated. Common fingerprint recognition
algorithms are no longer suitable for partial fingerprints. Therefore, this paper proposed a novel
fingerprint recognition algorithm suitable for partial fingerprint.

This paper proposes a SIFT-based pseudo-splicing partial fingerprint recognition algorithm to
improve the accuracy of the recognition. The comparisons of the accuracy of the recognition
among this algorithm, the minutia-based fingerprint recognition algorithm and the fingerprint

Natarajan Meghanathan et al. (Eds) : SPPR, SCAI, CSIA, WiMoA, ICCSEA, InWeS, NECO, GridCom - 2018
recognition algorithm based on image similarity, that shows the deficiency of the common fingerprint recognition techniques and this algorithm is better suitable for partial fingerprint. The remainder of this paper is organized as follows. The second part introduces the related work on fingerprint recognition techniques. The third part introduces a SIFT-based pseudo-splicing partial fingerprint recognition algorithm and fingerprint quality assessment algorithm. The fourth part is the result of the fingerprint comparison. The fifth part is a conclusion and future works.

2. RELATED WORK

With the development of fingerprint technology, many researchers have made many contributions in the fingerprint recognition and many algorithms have been proposed[7, 8]. Jia et al.[9] proposed a double matching method that combines the local minutia matching algorithm and the global matching algorithm. Their experimental results showed that the accuracy of the recognition on normal-size fingerprints is well, but they ignored the test for partial fingerprints. Cappelli et al. [10] introduced a novel minutiae-only local representation aimed at combining the advantages of both neighbor-based and fixed-radius structures, without suffering from their respective drawbacks. Gudavalli et al. [11] proposed a multi-biometric fingerprint recognition system based on the fusion of minutiae and ridges as these systems render more efficiency, convenience and security than any other means of identification. In order to reduce the number of templates compared with the input fingerprint in the verification stage and accelerate the speed of matching, Zhu et al. [12] proposed a method that splicing the features of multiple template fingerprints into one. They still ignored the test for partial fingerprints, but they mentioned the idea of splicing fingerprint template. For partial fingerprint, single image contained fewer features. It was useful for recognition by splicing multiple partial fingerprints.

Due to the unique features of the partial fingerprints, many researchers tried to recognize fingerprints based on image[13]. Zanganeh et al.[14] proposed a region-based fingerprint recognition algorithm. This method was used to image matching by calculating the local similarity in the image region and the overall correlation coefficient. Ito et al. [15] proposed an efficient fingerprint recognition algorithm combining phase-based image matching and feature-based matching. Liu et al. [16] proposed an efficient fingerprint search algorithm based on database clustering, which narrows down the search space of fine matching. Feng et al. [17] established a fingerprint matching algorithm combining ridge correlation and minutia feature points. This algorithm performed better than original minutia-based algorithm and was suitable for some nonlinear distorted images. However, the ridge direction was difficult to distinguish for partial fingerprints.

Nowadays, some researchers start studying the algorithm of fingerprint recognition based on local features[18, 19, 20, 21]. Aguilar-Torres et al. [22] presented a fingerprint recognition method using a combination of the Fast Fourier Transform (FFT) with Gabor filters for image enhancement, and fingerprint recognition was carried out using a novel recognition stage based on Local Features and Hu invariant moments for verification. Ceguerra et al. [23] presented a new approach for combining local and global recognition schemes for automatic fingerprint verification (AFV), by using matched local features as the reference axis for generating global features. Madhuri et al. [24] realized that most of the minutiae-based algorithms are not suitable for partial fingerprints, then proposed a fingerprint recognition technique using local robust features. Matching algorithms based on local features include SIFT (Scale Invariant Feature Transform)[25] and SURF (Speeded Up Robust Features)[26]. Their experimental results showed that the algorithm presented better effect on rotated fingerprints and partial fingerprints, but the test data used in their experiments was inconsistent with the size of the fingerprints discussed in our paper.
3. SIFT-BASED PSEUDO-SPICING PARTIAL FINGERPRINT RECOGNITION ALGORITHM

3.1. SIFT Algorithm

SIFT (Scale Invariant Feature Transform), proposed by David G. Lowe [25], is a description of the image processing field. The SIFT features not only keep invariance to rotation, brightness changing, but also keep a certain degree of stability for viewing angle changing, affine transformations, and noise, and it is a very stable local feature. It is not only suitable for fast and accurate matching of massive feature libraries, but also can be easily combined with other feature vectors.

The SIFT feature matching algorithm has two stages.

The first stage is the SIFT feature generation stage. This stage mainly extracts feature vectors that are rotation-independent, and luminance-independent from the images. Firstly, it searches for image locations on all identifies potential points of interest for rotation invariant using Gaussian differentiation functions; then it determines position through a fine-fitting model at each candidate location. The selection of key-points depends on their degree of stability; Next according to the gradient direction of the local image, one or more directions are assigned to each key-point position, all subsequent operations on the image data are relative to the direction and position of the key-points; Finally, the gradients of the local image are measured at selected scales within the neighborhood around each key-point. These gradients are transformed into a representation that allows for relatively large Local shape deformation and illumination change.

The second stage is the SIFT feature vectors matching stage. After the SIFT feature vectors of the two images are generated, the next step is to use the Euclidean distances of the key-point feature vectors as the similarity determination metrics of the key-points in the two images. Take a key-point of one of the images and find the closest two key-points in the other image by traversing. In the two key-points, if the value of the closest distance divided by the value of the next closest distance is smaller than a certain threshold, it is determined as a pair of matching points.

3.2. Pseudo-Splicing Algorithm for Partial Fingerprints

Due to fewer features of the partial fingerprint, one or two partial fingerprints are insufficient to cover the fingerprint information of an entire finger. A complete fingerprint database during the fingerprint enrollment stage is required. This paper proposes a pseudo-splicing algorithm to optimize the accuracy of fingerprint matching and simplify the complexity of fingerprint matching algorithm.

The SIFT algorithm has characteristics of invariant to rotation and brightness changing, so it can be used to realize pseudo-splicing of the partial fingerprint by using SIFT algorithm repeatedly. Fingerprint recognition is mainly divided into two stages, namely the fingerprint enrollment stage and the fingerprint verification stage. The fingerprint feature database needs to be constructed in the enrollment stage, and the matching result to be output by comparing raw fingerprint with the fingerprint database in the verification stage. Fingerprint splicing is a method that constructs a fingerprint feature database during the enrollment stage.
Algorithm 1 Pseudo-splicing algorithm for partial fingerprints

Input: Fingerprint feature set \( I_A \); Fingerprint similarity threshold \( \theta \); The maximum number of finger feature set \( \mu \); Raw fingerprint fp

Output: Fingerprint feature set \( I_A \)

1. \( I_A = \emptyset \);
2. When the number of \( I_A < \mu \):
3. \hspace{1em} for \( I_{A_i} \) in \( I_A \):
4. \hspace{2em} \( score_i = \text{get score using SIFT matches } fp \text{ and } I_{A_i} \);
5. \hspace{2em} if maximum of \( score_i < \theta \):
6. \hspace{3em} \( I_A = I_A \cup fp \);

Assuming a feature set \( I_A \) is one of the user A’s fingers. At the beginning, the \( I_A \) is an empty set, namely \( I_A = \emptyset \). When a fingerprint is obtained in the enrollment stage, the SIFT matching is performed between the raw fingerprint and all the fingerprints in the set \( I_A \), and the matching score is calculated. If the maximum value among these scores is smaller than the predefined threshold \( \theta \) (\( \theta \) is the fingerprint similarity threshold), the raw fingerprint is accepted and put it into the set \( I_A \). If the number of the set \( I_A \) is greater than the predefined threshold \( \mu \) (\( \mu \) is the maximum number of finger features of one person), the process of enrollment stage is terminated, and the set is now \( I_A = \{ I_{A_1}, I_{A_2}, \ldots, I_{A_\mu} \} \). The pseudo-code of the algorithm is shown in Algorithm 1.

The fingerprint feature database created by pseudo-splicing can improve the accuracy of fingerprint matching in the verification stage. However, if a low-quality fingerprint is encountered, it can pollute the fingerprint feature database. Therefore, this paper proposes an algorithm to evaluate the quality of fingerprints during the fingerprint enrollment stage and fingerprint verification stage.

### 3.3. Fingerprint Quality Assessment Algorithm

The fingerprint studied in this paper is the image of 96 pixels × 96 pixels, as shown in Figure 1.

![Figure 1. (a) high-quality fingerprint (b) low-quality fingerprints](image)

Figure 1 (a) shows a high-quality fingerprint and Figure 1 (b) shows three low-quality fingerprints. As can be seen from the figure 1, the distribution of the ridges of the high-quality fingerprint is relatively homogeneous, and there are no large area of white blocks or black blocks. If we put low-quality fingerprints into the fingerprint feature database, it will pollute the fingerprint database, which will cause a great influence on the verification of the fingerprint. This is very important to guarantee the performance of a biometric system, especially during the enrollment [27]. Therefore, this paper proposes a fingerprint quality assessment algorithm to improve the accuracy of verification of the fingerprint.

When a fingerprint is acquired, the width and height of the image are calculated, then the image is traversed in step s, and a sub-image is cropped with the side length of b to calculate the ratio of the black block. As shown in Formula 1.
In formula 1, \( r \) is the calculated ratio of the black block of the sub-image, \( m \) and \( n \) are the width and height of the sub-image respectively, \( p_{ij} \) indicates whether the pixel at \((i,j)\) is black, and \( c_{ij} \) is the value of the pixel at \((i,j)\), where \( \alpha \) is the threshold for judging color. If the value of one pixel is larger than the threshold, it is regarded as white, otherwise it is black.

After traversing the above rules, a set of black blocks are calculated, namely \( R = \{r_1, r_2, \cdots, r_L\} \), where \( r_k (1 \leq k \leq L) \) is the ratio of black block calculated from formula 1, and \( L \) is the total number of traversed blocks. Then counting the number of invalid blocks using formula 2, as shown in Formula 2.

\[
N = \sum_{k=1}^{L} q_k, \text{where } q_k = \begin{cases} 
1, & r_k > \beta \text{ or } r_k < 1 - \beta \\
0, & \text{Others}
\end{cases}
\]  
(Formula 2)

In formula 2, \( N \) denotes the number of invalid blocks, \( q_k \) denotes whether the \( k \)-th black block is an invalid block, and \( \beta \) is the ratio threshold of the invalid block. If the ratio of the black block is greater than \( \beta \) or less than \( 1 - \beta \), it is regarded as an invalid block.

Finally, determining whether the fingerprint quality is qualified by comparing the number of invalid blocks \( N \) with the fingerprint quality threshold \( \varepsilon \). Here is given the fingerprint quality assessment algorithm as shown in Algorithm 2.

---

**Algorithm 2 Fingerprint quality assessment algorithm**

**Input**:
- Raw fingerprint \( fp \);
- Step \( s \);
- Side length of block\( b \);
- Color threshold \( \alpha \);
- Invalid block ratio threshold \( \beta \);
- Fingerprint quality threshold \( \varepsilon \);

**Output**:
The result of fingerprint quality assessment

Get the width \( fp\_width \) and height \( fp\_height \) of the fingerprint image \( fp \);

The number of invalid blocks \( invalid\_num = 0 \);

for \( i \) from 0 to \( fp\_width \) step \( s \):

4. for \( j \) from 0 to \( fp\_height \) step \( s \):

5. Cropping a sub-image \( sub\_fp \) with the starting point \((i,j)\) and side length \( b \);

6. Binarizing sub-image \( sub\_fp \) with the color threshold \( \alpha \);

7. Calculating the ratio of the black block \( black\_ratio \) and the ratio of the white block \( white\_ratio \) of the binarized sub-image;

8. if \( black\_ratio > \beta \) or \( White\_ratio > \beta \):

9. \( invalid\_num = invalid\_num + 1 \);

10. return \( invalid\_num < \varepsilon \);
4. EXPERIMENT

4.1. Experimental Data

The fingerprint data used in this paper is 96 pixels × 96 pixels images, as shown in Figure 1 above. In the fingerprint data set, not all images are available. As shown in (b) on Figure 1, these images should be discarded. Therefore, the fingerprint quality assessment algorithm is used to filter out the low-quality fingerprints during enrollment stage. Then the fingerprint recognition algorithm based on the minutia points, the similarity of the image and the pseudo-splicing partial fingerprint with SIFT are respectively tested. The experimental data of this paper uses 120 persons’ fingers. Each finger has 40 fingerprints. The first 20 fingerprints are used to create fingerprint feature database, and the rest are used to test. The feature database has 120 personal features and each person has 5 fingerprint features. In the minutia-based feature database, 5 minutia features are extracted randomly; in the image similarity-based feature database, 5 fingerprints are sampled randomly; in SIFT-based pseudo-splicing feature database, 5 fingerprints are trained by the pseudo-splicing algorithm.

4.2. Experimental Strategy

This experiment matches each fingerprint in the test set with each feature in the feature database of 120 individuals. Each fingerprint in the test set will get a score, and then according to the predefined similarity threshold $\theta$, the fingerprint is attached with a label, that is, if the fingerprint is successful matched, the label of the fingerprint is assigned to 1, otherwise it is assigned 0. Thus we get a set of binary relations $\{(x_{11}, y_{11}), (x_{12}, y_{12}), \ldots, (x_{ij}, y_{ij})\}$, where $i$ represents the fingerprints of the $i$-th person in the test set, and $j$ represents the features of the $j$-th person in the feature database, and $q$ represents the features of the $q$-th fingerprint of the $i$-th person in the test set. So $x_{ijq}$ represents the result of matching the q-th fingerprint of the i-th person in the test set with the features of the j-th person in the feature database, and $y_{ijq}$ represents the value of the label corresponding to $x_{ijq}$. $y_{ijq}$ is equal to 1 if $i$ equals $j$, otherwise it is 0. Then a value $V$ is calculated by Formula 3, and if $V$ is less than 0, it is regarded as false rejection, otherwise it is regarded as false acceptance. Finally, calculating the False Rejection Rate (FRR) and the False Acceptance Rate (FAR) corresponding to the current similarity threshold $\theta$.

$$V = \frac{x_{ijq} - \theta}{|x_{ijq} - \theta|} - y_{ijq}, \text{when } x_{ijq} = \theta, \frac{x_{ijq} - \theta}{|x_{ijq} - \theta|} \text{ regarded as 0} \quad \text{(Formula 3)}$$

The false acceptance rate [28], or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. The false recognition rate [29], or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. This paper shows the accuracy of the recognition of different algorithms by calculating FRR and FAR.
4.3. Experimental Result

The minutia-based fingerprint recognition algorithm in this experiment is tested using the edit distance algorithm. The similarity-based algorithm is tested using the perceptual hash algorithm. The result of the comparison are shown in Figure 2.

The ROC curve is used to describe the effect of the fingerprint algorithm. The ordinate represents FAR, the abscissa represents FRR, and the Equal Error Rate (EER) is a balance point between FAR and FRR. The lower the equal error rate value, the higher the accuracy of the biometric system [30].

As shown in figure 2, the yellow curve represents the result of the minutia-based fingerprint recognition algorithm; the blue curve represents the result of the similarity-based fingerprint recognition algorithm; the green curve represents the SIFT-based pseudo-splicing fingerprint recognition algorithm. The curve of the minutia-based fingerprint recognition algorithm and the curve of the similarity-based fingerprint recognition algorithm have higher ERR than the curve of the SIFT-based pseudo-splicing fingerprint recognition algorithm. Obviously, the SIFT-based pseudo-splicing fingerprint recognition algorithm works best.

There are two important parameters that affect the accuracy of recognition in the SIFT-based pseudo-splicing fingerprint recognition algorithm. One is the number of features of the fingerprint feature database, and the other is the similarity threshold in the pseudo-splicing algorithm. The rest of the paper presents the algorithm is optimized by adjusting these parameters.

This experiment tests the number of features of the fingerprint feature database differently, and keeps the other parameters unchanged. The results are shown in Figure 3.

In the legend of figure 3, the number behind N represents the number of features of the fingerprint feature database. As can be seen from the figure 3, with the increasing of the number of features of the fingerprint feature database, the lower the EER, the better accuracy of the recognition.
Figure 3. The result of comparison under different number of features of the fingerprint feature database

Now, keeping the number of features and other parameters of the fingerprint feature database unchanged, and testing the different fingerprint similarity threshold in the pseudo-splicing algorithm. The results are shown in Figure 4.

In the legend of figure 4, the number behind A represents the fingerprint similarity threshold in the pseudo-splicing algorithm. The curves between neighboring threshold are dense. This paper shows the result of comparison under different fingerprint similarity thresholds by dividing into four parts. It can be seen from Figure 4 (a), the lowest EER occurs when the threshold is 5. It can be seen from Figure 4(b), when the threshold is 7, the EER is the lowest. It can be seen from (c) and (d) in figure 4 that when the threshold is between 5 and 7, the EER is lower and the algorithm works well.

According to the comparison above, it shows that the more number of features of the fingerprint feature database, the better accuracy of the recognition, but with the number of features of the fingerprint feature database increasing, the consumption of the time of recognition becomes higher. So the number of features of the fingerprint feature database should be adjusted according to the specific application scenarios. In addition, the algorithm performs well when the fingerprint similarity threshold is between 5 and 7 in the pseudo-splicing algorithm.
CONCLUSION

This paper proposes a SIFT-based pseudo-splicing partial fingerprint recognition algorithm, aiming at improving the accuracy of the fingerprint recognition algorithm for partial fingerprints. Through the comparison, the proposed algorithm has better accuracy of recognition for partial fingerprints, and the algorithm is optimized to increase the accuracy of recognition for partial fingerprints by adjusting different parameters. In the future, we will try to combine other algorithms to improve the accuracy of the recognition for the partial fingerprint.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (No. 61732004, 61472433, 61732022, 61672020, 61502517); National Key Research and Development Program of China (2017YFB0802204, 2016YFB0800802, 2016YFB0800803, 2016YFB0800804, 2016QY03D0601, 2016QY03D0603, 2016YFB0800303).
REFERENCES


