Identifying FKP-based Individuals Using the Feature Extraction of the Relaxed Local Ternary Patterns

Mahammad Anbari¹, Leila Zahedi²

¹Department of Electrical Engineering, Tafresh University, Tafresh, Iran
²School of Computing and Information Sciences, Florida International University.

Correspondence to: Zahedi L. (E-mail: lzahe001@fiu.edu)

Abstract

Identification based on biometric parameters is an effective way to identify people. The fingerprint effect is a feature with small image dimensions, and at the same time, distinguishable features in low image resolution and is used as a reliable biometric identifier. In this paper, a new method for identifying FKP-based individuals using the extraction feature of the Relaxed Local Ternary Patterns (RLTP) is suggested. The RLTP method has been proposed to identify faces and has led to favorable results. In this method, large neighborhood differences that are immune to noise are encoded in two specific states, and small neighborhood disturbances that are vulnerable to noise are encoded in an uncertain state. The chi-square distance criterion is used to calculate the similarity between the extraction features of the input and reference FKP images. The advantage of this method is low computational complexity while improving the high accuracy of recognition. Experimental results on a standard database confirm the success of the proposed method.

Keywords: Relaxed Local Ternary Patterns, Biometric Parameters, Fingerprint, Small Neighborhood Disturbances, FKP Images.

Received: 27 May 2020, Accepted: 24 June 2019
DOI: 10.22034/jbr.2020.232978.1024

1. Introduction

Verification of people's identities is important in many applications such as entering sensitive places, cars, computers, mobile phones, etc. Identification based on biometric parameters is more reliable than methods based on the ID card or input RAM. Different biometric identifiers such as the face, iris, voice, etc. have been used. Among these, hand-based image methods such as fingerprint, palm, hand geometry, and Finger Knuckle Print (FKP) are particularly popular. In this paper, the recognition of an individual using FKP is considered. Wrinkles and skin patterns on the outer surface of the fingertip are called fingerprint effects and are a valid identifier in distinguishing individuals. This feature, while having small image dimensions compared to some features such as palm effect, and therefore less time-consuming in terms of processing because the image is more distinct than other methods, such as fingerprints, it has clinical reliability. In [1], Wodwar, in 2005, they were the first researchers to use a fingerprint image to identify people. Their efforts led to the beginning of further research in this area. Method [1] uses the geometric characteristics of the image on the back surface of the three adjacent fingers to extract the feature and does not use image texture specifications. In [2], Kumar used a combination of geometric features and the texture of the image behind four fingers to create an identification system. In [3], Kumar used the RLOC code method, which was suggested in [4] for palm recognition, to identify FKP. Zhang Lin and his colleagues in [2] proposed an economic analytical system for authentication based on a person's fingerprint. The system consists of four
main parts: FKP imaging, extraction area attention, ROI, feature extraction, and feature injection. The small size of the imaging device and its special design shown in Figure (1-A), simplifies the pre-processing steps such as image segmentation and ROI extraction. Because the fingertips are curved during imaging, the skin's tissue patterns are well reflected, and the unique and distinctive features of FKP are better extracted. Figure (1-B) shows an image of the resulting FKP sample. Figure (1-C) shows the process of extracting ROI, and Figure (1-D) shows the resulting image. In [2], the combination of directional and extraction domain information from Gabor filters are used in the identification section. As with any classification process, FKP-based authentication systems play an essential role in improving results.

The data transmission is a major issue when there are multiple interconnected networks of sensor modules, and compressing methods are considered as a potential solution. The details about the application of compressed sensing are presented in [6-8]. These methods can also be adapted for image data, to reconstruct the signal more accurately [9]. In another study, Lin and his colleagues in [10] used competitive methods based on Gabor filter-based encryption to extract studies for the local image, as well as FKP features. Competitive encryption was proposed in [11] to recognize the palm of the hand. In [12], to calculate the similarity between the two FKP images, the Band-Limited Phase-Only Correlation (BLPOC) algorithm is used. In [13], FKP images are hierarchically encrypted using a Monogenic Code encryption method. The generated RAM, by applying a single gene signal to each pixel, reflects the direction and phase information and is stored as a three-bit vector. The results showed that the proposed system operated twice as fast using the monogenic code RAM from the perspective of adaptation speed compared to other methods. In [14], To verify and verify people's identities, they proposed a new method of recognizing the fingerprint effect using encryption based on a local binary pattern. In this method, first each ROI image is divided into sections and each section is converted to binary patterns and then to histogram after passing through Gabor filter bank. The BioHashing method is used to match the extracted features of the input and stored FKP images. In [15], they used a local binary pattern to identify people based on fingerprints. In this effort, first the FKP images are divided into equal parts and then, using the local binary pattern, the local features of the image are extracted. The histogram of binary patterns is used as a vector of a feature and is compared between the input and recorded images of the FKP, using the histogram subscription distance criterion. In [16] a general overview of the proposed methods in the field of FKP identification has been done.

In this paper, a new method for identifying FKP-based individuals using the extraction feature of the Relaxed Local Ternary Patterns (RLTP) is suggested. The RLTP method has been proposed in [17] to identify faces and has led to favorable results. In this method, large neighborhood differences that are immune to noise are encoded in two specific states, and small neighborhood disturbances that are vulnerable to noise are encoded in an uncertain state. The chi-square distance criterion is used to calculate the similarity between the extraction features of the input and reference FKP images. In the continuation of the article in section 2, we will introduce the proposed method. Recognition results are presented in Section 3. Section 4 is devoted to summarizing and conclusion.
2. Suggested Method

The local binary pattern encrypts the pixel differences between neighboring and central pixels. For example, \( LBP_{P,R} \) encode the pixel differences between the central pixel and the neighboring \( p \) in a circle of radius \( R \). The \( LBP \) code is obtained through Equation 1. In this equation, the gray surface of the central pixel with \( i_c \) and the gray surface of the circular neighborhood with \( i_p \) are displayed.

\[
LBP_{P,R} = \sum_{p=0}^{P-1} s(i_p - i_c)2^p
\]  

(1)

In Equation 1, \( s(z) \) is the threshold function.

\[
s(z) = 1 \text{ if } z \geq 0
\]  

(2)

The base \( LBP \) is sensitive to noise. A small image noise can change the cryptocurrency difference from 0 to 1 or vice versa. The sensitivity to localized triple pattern noise (LTP) introduced in [18] is lower than that of \( LBP \). In this method, the small pixel difference is encrypted in another separate mode. The LTP code is calculated by Equation 3.

\[
LT_{P,R} = \sum_{p=0}^{P-1} s'(i_p - i_c)3^p
\]  

(3)

In this equation, \( s'(z, t) \) is the threshold function and \( t \) is a pre-set threshold value. The threshold function is defined as follows:

\[
s'(z, t) = \begin{cases} 
1 & \text{if } z \geq t \\
0 & \text{if } |z| < t \\
-1 & \text{if } z \leq -t 
\end{cases}
\]  

(4)

The dimensions of the LTP histogram is very large. \( LT_{P,2} \) results a histogram with \( 3^8 = 6561 \) bins. For this reason, in [18] the LTP code is divided into two positive and negative LBP code.

\[
s'_p(z, t) = \begin{cases} 
1 & \text{if } z \geq t \\
0 & \text{if } z < t 
\end{cases}
\]  

(5)

\[
s'_n(z, t) = \begin{cases} 
1 & \text{if } z \leq -t \\
0 & \text{if } z > -t 
\end{cases}
\]  

(6)

However, a significant amount of information may be lost during this process. On the other hand, the positive and negative LBP histograms are strongly correlated. That is why a lot of plugin information remains on both histograms. The Relaxed Local Triple Pattern (RLTP) presented in [16], solves the problem of \( LBP \) and LTP. In this method, the threshold function of the local triple pattern is defined as follows:

\[
s''(z, t) = \begin{cases} 
1 & \text{if } z \geq t \\
X & \text{if } |z| < t \\
0 & \text{if } z \leq t 
\end{cases}
\]  

(7)

State 0 and 1 refer to two large states of pixel difference. These conditions are less likely to be affected by noise and are more reliable. State \( X \) represents the unknown state. In this case, the pixel difference is small and the noise can easily change from 0 to 1 and vice versa. Therefore, in this method, a small pixel difference is encrypted regardless of its size and range. This encryption method is less sensitive to noise. The goal is to reduce the number of \( X \) states and turn them into strong states [19]. It is difficult to pinpoint the exact size of a small pixel difference. Therefore, the \( X \) state is likely to be encoded in two strong states, 0 and 1. With this assumption, the triple code becomes the binary code. Consider the pixel difference \( z \). \( P^1 \) is the probability of encoding the unknown state to 1 and \( P^0(z) = 1 - P^1(z) \) is the probability of encoding to 0. Therefore, Equation 7 is rewritten as Equation 8:

\[
P^1(z) = \begin{cases} 
1 & \text{if } z \geq t \\
0.5 & \text{if } |z| < t \\
0 & \text{if } z \leq t 
\end{cases}
\]  

(8)

The encryption process is shown in Figure 2. The image piece is first encoded into a triple code. Then, the triple code becomes the binary code. The zero and fifth bits are encrypted in both 0 and 1 states. In this example, the triple code is converted to two binary codes. When a histogram is formed, each 25.0 binary code is added to the corresponding histogram.

Figure 2. Display RLTP encryption method. First, the 11X1001X triple code is extracted from the image and then converted to two binary code.
The proposed RLTP is significantly different from LTP. When there is only one unknown bit, both methods generate two LBP codes. These two codes are written in two different histograms for LTP and in one histogram for RLTP. When there are more unknown bits, the RLTP will be completely different from the LTP. Consider the triple code 11X1001X Figure 2. The LTP method results in two LBP codes: 11010010 and 00001100, which are mapped in two positive LBP and LBP histograms, respectively. In the RLTP method, four non-coded codes are given in Figure 2. The first and fourth code correspond to the positive LBP code and the negative LBP code, respectively. These four codes are mapped to a binary histogram. Each code will add 0.25 to the corresponding histogram.

3. Experimental Results
In order to evaluate the proposed algorithm, the U_PolyFKP database is used in [20]. This database contains 165 fingerprint images. These people are between 20 and 50 years old. These images were collected in two-time intervals of about 25 days. From each index and middle finger of each person's left and right hands, 12 samples were collected. Therefore, 48 samples are available for each person. The database contains a total of 7920 images of 660 fingers. In this study, 6 image samples are used for training and the remaining 6 samples are used for testing. First, the image size is changed to 64 × 64. Each image is divided into 16 × 16 equal pieces, so that each piece is 8 rows and the column overlap with its previous piece. For each vector, RLTPb,2 is obtained and its histogram is extracted. To reduce the effect of brightness changes, images, such as the one suggested in [18], are passed through a pre-processing block including gamma correction, Gaussian differential filter, and light smoothing. The e-distance criterion is used to calculate the similarity between the input and reference FKP images, and the closest neighbor class is used for classification [21-22]. An adaptive extended Kalman filter is applied in the proposed algorithm to reduce the noises. Hamed et al. [23] showed that using a state-feedback controller with extended Kalman filter can decrease the noise of the signal significantly. In [24], since the natural frequency of the system is unknown in the system identification process, empirical mode decomposition and Hilbert Huang Transform used to characterize the system. The results are presented in two sections: Identification and Confirmation of Identity.

3.1. FKP Identification
In this case, the identity of the input user is unknown. The acquired information from the input user is compared with the information of all users of the data base and the most similar pattern is considered as the identity of the unknown person. The effectiveness of the proposed method on each finger separately and different combinations of fingers (integration) at the level of the feature (evaluated). Also, the proposed method has been compared with two other methods. In one method, the PCA algorithm, and in another, the combination of PCA and LDA algorithms applied to FKP images, is compared with the proposed method. Experimental results in the form of recognition rates are summarized in Table (1 and 2). In the Table 2, right index finger, right middle finger, left index finger and left middle finger are arranged in abbreviated letters RI, RM, LI, LM.

3.1. FKP Identity Confirmation
Unlike identity identification, in this case the user claims individual identity. On the other hand, authentication only includes comparisons with claims identical to the claimed identity.

<table>
<thead>
<tr>
<th>Finger Type</th>
<th>Recognition rate using different methods (%)</th>
<th>Suggested Method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PCA</td>
<td>PCA+LDA</td>
</tr>
<tr>
<td>Left Index</td>
<td>34.04</td>
<td>51.62</td>
</tr>
<tr>
<td>Right Index</td>
<td>34.44</td>
<td>57.17</td>
</tr>
<tr>
<td>Right Middle</td>
<td>38.08</td>
<td>59.70</td>
</tr>
<tr>
<td>Left Middle</td>
<td>38.08</td>
<td>56.97</td>
</tr>
</tbody>
</table>

The results of the authentication tests are shown in the ROC curve in Figure 3. This curve is plotted by adjusting the adjustment threshold and drawing the
wrong acceptance rate (FAR) versus the wrong non-acceptance rate (FRR) for all possible thresholds. Also, the results are shown in the form of equal error rate (point FAR equal to FRR) in the Table 3.

Table 2. Recognition rate resulting from finger composition

<table>
<thead>
<tr>
<th>Finger Combination</th>
<th>Recognition rate using different methods (%)</th>
<th>Suggested Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>LI+RI</td>
<td>38.89 75.96 94.14</td>
<td></td>
</tr>
<tr>
<td>LI+LM</td>
<td>41.11 70 95.15</td>
<td></td>
</tr>
<tr>
<td>LI+RM</td>
<td>41.52 76.36 95.75</td>
<td></td>
</tr>
<tr>
<td>LM+RI</td>
<td>42.63 80.20 94.74</td>
<td></td>
</tr>
<tr>
<td>LM+RM</td>
<td>43.74 80.61 96.76</td>
<td></td>
</tr>
<tr>
<td>RI+RM</td>
<td>41.74 86.87 95.35</td>
<td></td>
</tr>
<tr>
<td>LI+LM+RI</td>
<td>44.44 78.59 96.36</td>
<td></td>
</tr>
<tr>
<td>LI+LM+RM</td>
<td>45.05 77.88 97.87</td>
<td></td>
</tr>
<tr>
<td>LM+RI+RM</td>
<td>46.77 87.27 97.67</td>
<td></td>
</tr>
<tr>
<td>LI+RI+RM</td>
<td>44.75 85.45 97.87</td>
<td></td>
</tr>
<tr>
<td>Four Fingers</td>
<td>47.79 89.03 98.58</td>
<td></td>
</tr>
</tbody>
</table>

Table 3. Comparison of performance of different methods of FKP recognition

<table>
<thead>
<tr>
<th>Method</th>
<th>EER (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competitive Coding [10]</td>
<td>1.66</td>
</tr>
<tr>
<td>Robust Line Orientation Code [4]</td>
<td>1.91</td>
</tr>
<tr>
<td>Monogenic Code [13]</td>
<td>1.72</td>
</tr>
<tr>
<td>Production of the binary pattern using Gabor filter bank [14]</td>
<td>1.69</td>
</tr>
<tr>
<td>Histogram local binary pattern [15]</td>
<td>1.72</td>
</tr>
<tr>
<td>Relaxed Local Ternary Patterns</td>
<td>1.57</td>
</tr>
</tbody>
</table>

4. Conclusion
In this paper, a new algorithm for identifying people based on FKP images is presented. First, the properties of each finger are extracted using a relaxed local triple pattern. Then, the chi-square distance criterion and the closest class closeness criterion were used for the match. The experimental results presented in Section 3 show the acceptability of this method for recognizing each finger compared to the other two conventional methods. The results of experiments performed on the Poly-U standard database show that the rate of recognition of the proposed algorithm has increased significantly with the integration of different finger features compared to a single finger and at the same time, it has been more successful than the other two methods. For future works in this field, low power analog circuits such as [25] can be used to create an power efficient on board model of the proposed technique.

Conflict of interest
The authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest, or non-financial interest in the subject matter or materials discussed in this manuscript.

Acknowledgments
The authors would like to thank anyone who participated in this study.

References


