Automated Fingerprint Identification System Application
For System's Equal Error Rate Evaluation

Marko Kočevar, Zdravko Kačič
Margento R&D d.o.o., Gosposvetska cesta 84, 2000 Maribor, Slovenija
Fakulteta za elektrotehniko, računalništvo in informatiko, Smetanova 17, 2000 Maribor, Slovenija

ABSTRACT
Automated fingerprint identification system has an increasingly important role in modern times. This study presents the steps of the automated fingerprint identification system and presents an application for fingerprint identification and system's equal error rate evaluation. The algorithm for fingerprint image enhancement is a key element of the system. A fingerprint image can be damaged, damp, too dry, worn, scratched, etc. Therefore it is necessary to enhance the image to the point where we can obtain a clearly defined structure of ridges and valleys and consequently also correctly determined features. This study also presents a comparison of error rate evaluation between the original fingerprint image and the enhanced fingerprint image, and introduces an application for fingerprint matching. The matching algorithm compares two fingerprints and establishes a correct match, if the fingerprints belong to the same person, or a non-match, if they belong to different persons.

Keywords: Fingerprint recognition, fingerprint enhancement, biometrics, and fingerprint matching

1. INTRODUCTION
Because of increasing demands for automated, precise and fast identity verification, biometric system for identity verification has become well established and accepted as part of our everyday lives. Biometric characteristics have the following advantages:

- they are unique,
- they are non-transferable,
- one cannot lose or forget them,
- it is difficult to hide or change them,
- etc.

Automated fingerprint identification system is one of biometric systems which are today used for identification of persons according to their characteristics. The use of biometric recognition is increasing and can be traced in various activities, where it is applied for various purposes: defence systems, national security, intelligence services, prison management, state borders measures, passports, banks and financial institutions, information systems, etc.

We know two types of person's identity verification:

- **Identification** (establishing persons identity on the basis of his/her biometric data)
- **Verification** (establishing whether the person is really who he/she claims to be)

Biometric characteristics are divided into two groups: physiological or physical (fingerprints, face, iris pattern, hand geometry, etc.) and behavioural (signature, voice, typing).

1.1 Fingerprint
Fingerprint is a biometric physiological characteristic used for verification and identification of persons. Among all biometric characteristics (iris, face, voice, hand) fingerprint has the highest degree of reliability [1]. The surface of a fingerprint consists of ridges (black lines) and valleys (white lines); see Figure 1.

![Fig 1: Ridges and valleys on the surface of a fingerprint](image)

The most well-known fingerprint characteristics are called minutiae [1]. The most useful are two types of minutiae (Figure 2):

- minutiae point where a ridge ends, and
- minutiae point where a ridge divides into two ridges.

![Fig 2: Minutiae points where ridges end or divide into two ridges](image)
2. AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

Automated fingerprint identification system consists of the following steps: fingerprint capturing, fingerprint image enhancement, fingerprint features extraction, fingerprint features matching, classification and evaluation of the success rate of the entire system.

2.1 Fingerprint Image Capturing

Two techniques are used to capture a fingerprint image [1]:

- Static image capturing: finger is pressed on the surface of the sensor window, which is of the same size as a fingerprint, for as long as it takes to capture the image (Figure 3);
- The second capturing method is to use a rectangular window with the same width as the image and the height of only a few points, over which the finger is vertically swept (Figure 4).

2.2 Fingerprint Image Enhancement

To increase the accuracy of person's identification the captured fingerprint image needs to be enhanced. Because of several uses fingerprints can be dirty, damp, very dry, worn out, etc. Therefore the image needs to be enhanced to the point where we can clearly determine the structure of ridges and valleys. Fingerprint image enhancement can be done in the spatial or in the frequency domain. Spatial-domain techniques are the following: contextual filters [2], Gabor filters [3, 5, 6], a curved Gabor filter [7], anisotropic filters [8], directional filters [9, 10, 11] and compensation filters [12, 13].

Frequency-domain techniques are the following: Log Gabor filter [14], wavelet transform [15], fast Fourier transform [16, 17, 18], directional Fourier filtering [19], short time transform [20], discrete cosine transform [21] and two-stage enhancement scheme for low-quality fingerprint images by learning from images [22]. Further enhancement techniques are presented in [1]. Most often enhancement techniques are based on contextual information, such as: ridge orientation and ridge frequency.

2.2.1 Image Pre-Processing

The initial step of fingerprint image pre-processing involves enhancement techniques which are based mostly on enhancement of fingerprint image contrast. This includes mostly techniques such as histogram equalization [23], normalization [3] and Wiener filtering [8]. With the normalization procedure we get a new intensity value for each individual pixel with the following equation:

\[
\text{norm}(i,j) = \begin{cases} 
M_e + \frac{\text{VAR}(L) - M}{\text{VAR}} & \text{if } I(i,j) > M \\
M_e - \frac{\text{VAR}(L) - M}{\text{VAR}} & \text{else} 
\end{cases}
\]  

where \( \text{norm}(i,j) \) is the normalized image of the greyscale image \( I(i,j) \), \( M \) and \( \text{VAR} \) are the average and the variance of the fingerprint image respectively, \( M_e \) and \( \text{VAR}_e \) are the desired mean value and variance, determined experientially (\( M_e = 0, \text{VAR} = 100 \)).

2.2.2 Determining Ridge Orientation

Gradient-based procedure (22, 23, 24, 25) is widely and effectively used for determining ridge orientation [3]. It is calculated for individual image block of size 16 x 16 pixels with the following equation:

\[
G_{xy} = \sum_{k=-8}^{8} \sum_{l=-8}^{8} V_x(x_i + h, y_j + k) V_y(x_i + h, y_j + k)
\]  

\[
G_{xx} = \sum_{k=-8}^{8} \sum_{l=-8}^{8} V_x(x_i + h, y_j + k)^2,
\]

\[
G_{yy} = \sum_{k=-8}^{8} \sum_{l=-8}^{8} V_y(x_i + h, y_j + k)^2.
\]

where \( V_x \) and \( V_y \) are gradient components, determined with the Sobel mask of size 3x3 in directions x and y. The oriented image (Figure 5) needs to be smoothed with Gaussian filter.

2.2.3 Determining Ridge Frequency

The second important contextual characteristic is ridge frequency between two consequent grey value peaks
in the direction of the local ridge. A widely applicable procedure is based on x–signature (Figure 6) [3] of ridges and valleys with the following equation.

\[
f_{ij} = \frac{4}{s_1 + s_2 + s_3 + s_4}
\]

(5)

2.2.4 Spatial Domain Enhancement

Unlike with conventional filtering, filter characteristics change with contextual filtering according to the context of the fingerprint image. Filters, calibrated to the parameters of ridge orientation and frequency, can effectively remove unwanted noise while keeping the correct ridge structure. Usually the filter sets are pre-calculated and then chosen for a particular image area.

2.2.5 Frequency Domain Enhancement

Multiplication of point by point in the frequency domain is the same as convolution in the spatial domain [23]. In the frequency domain the filter is defined by the following function:

\[
F(p, \theta) = F_{\text{radial}}(p) \cdot F_{\text{angular}}(\theta)
\]

(6)

where \( F_{\text{radial}} \) depends on the local ridge distance \( p = 1/f \) and \( F_{\text{angular}} \) depends on the local ridge orientation \( \theta \).

Both \( F_{\text{radial}} \) and \( F_{\text{angular}} \) are defined as band-pass filters, and are defined by mean value and bandwidth [1]. Filtering is performed as follows:

- on image \( I \) FFT (Fast Fourier Transform) is calculated to get image \( F \),
- in each point the transfer function of filter \( F_i \) is multiplied by \( F \),
- inverse FFT of image \( P \) is performed.

2.3 Minutiae Extraction

Most automated fingerprint identification systems are based on minutiae matching [1]. Reliable minutiae extraction is thus of key importance. Most well-known minutiae are the points where the ridge ends (ridge end) or divides into two (ridge bifurcation), as shown in Figure 2. Every minutia has assigned information such as type, location and orientation. Algorithms for minutiae extraction have to locate minutiae points effectively and precisely. There are roughly four types of algorithms for minutiae extraction [1]:

- The first category is based on minutiae extraction directly from greyscale image without binarization or edge thinning.
- The second category is based on minutiae extraction from a binarized image.
- The third category is based on minutiae extraction with machine learning method.
- The fourth category is based on minutiae extraction from a skeletonised binary image.

On the basis of extracted minutia a template is then created, which is needed in the next step of fingerprint matching.

2.4 Matching

The fingerprint matching algorithm compares two fingerprints and according to the threshold value establishes their match [1]. If the result is above the threshold value, the fingerprints match, and if the result is under the threshold value the fingerprints do not match. Some algorithms operate directly on the greyscale image, but most matching algorithms require an intermediate step in which minutiae are extracted. The minutiae matching system determines which extracted minutia from the new sample matches or does not match the template.

2.5 Classification and Verification System Error

Classification of a fingerprint is an important step in the automated fingerprint identification system [1]. It is required to reduce the number of one-on-one fingerprint comparisons. To identify a person the fingerprint that is to be identified needs to be compared with all the fingerprints saved in the database. This database can be very big, including up to several millions of fingerprints. In such cases identification takes longer than it is acceptable. The usual strategy to speed up identification is to divide the fingerprint database into several bins, based on predefined classes. The fingerprint that is to be identified is compared only with a fingerprint in an individual database bin and on the basis of its class [1]. The successfulness of the verification system is determined with a ROC curve (Figure 7). The ROC curve shows FMR (False Match Rate) and FNMR (False Non Match Rate) according to the following equation:

\[
\text{FNMR} = \frac{\text{Number of rejected genuine claims}}{\text{Total number of genuine accesses}} \times 100\%
\]

(7)

\[
\text{FMR} = \frac{\text{Number of accepted imposter claims}}{\text{Total number of imposter accesses}} \times 100\%
\]

(8)

It needs to be noted that FMR is also known as FAR (false acceptance rates) and FNMR as FRR (false rejection rate). EER (Equal Error Rate) was used as a
success rate indicator, marking the point where FNMR and FMR are equal [12].

\[
EER = \frac{FMR + FNMR}{2}, \quad \text{if FMR} = \text{FNMR}
\]

Fig 7: EER success rate indication where FNMR and FMR are the same

3. EXPERIMENTAL PART

The experimental part presents an application for evaluation of equal error rate, calculation of the equal error rate between the original image and the image enhanced with a two-stage algorithm [22] and display of fingerprints matching.

3.1 Evaluation of Equal Error Rate and Matching

To evaluate the equal error rate we used the FVC2004 DB2_A fingerprint database. For minutiae extraction we used the MINDTCT algorithm and BOZORTH3 to evaluate their matching [24]. Both algorithms are a part of the NIST software, which was developed in cooperation with NIST (National Institute of Standards and Technology) for FBI (Federal Bureau of Investigation) and DHS (Department of Homeland Security).

3.1.1 Image Enhancement

For image enhancement we used a two-stage algorithm presented in [22]. Figure 8.a shows the original image and Figure 8.b shows the enhanced fingerprint image from the FVC2004_DB2A database.

Fig 8: (a) original image (FVC2004_DB2A); b) enhanced image

3.1.2 Minutiae Extraction

We extracted the fingerprint minutiae points with mindtct algorithm. The input into the mindtct algorithm has to be a fingerprint image in jpg format (e.g. 101_1.jpg). In databases FVC2000, FVC2002, FVC2004 in FVC2006 fingerprint images are saved in the tiff format and they must be converted to jpg format. Figure 9.a shows a list of fingerprint images from database FVC2004_DB2_A. Every extracted minutia point has recorded its location (coordinates x and y) and orientation (t). The result of the mindtct algorithm is a feature "image_name.xyt", as shown in Figure 9.b.

Fig 9.(a): database of captured images; b) the created minutiae template
3.1.3 Minutiae Matching And Evaluation Of System's Success Rate

The result of matching is with algorithm BOZORTH3 given in numerical form, i.e. in a range from 0 to approximately 500. The higher the matching result the higher is the similarity between two fingerprints. A threshold of matching is usually set, on the basis of which the system either allows or denies access. If the result is above the threshold, the identity is verified. According to equations (7) and (8) the recognition system is as follows:

- Genuine fingerprint recognition: For all 100 fingers the first fingerprint is matched with other seven fingerprint of the same person, the second fingerprint with six, etc. so that we get 28 matches for one fingerprint of the same person. We thus get 2800 for the whole fingerprint database.
- Impostor fingerprint recognition: To recognize impostor fingerprints every first fingerprint of the 8 same fingerprints available is used. The first fingerprint is matched with other 99 prints of different persons, the second fingerprint is then matched with 98 fingerprints, etc. We thus get 4950 matches for the whole fingerprint database.

Figure 10 shows the equal error rate (EER) for database FVC2004 DB2_A, where FNMR = FMR.

Figure 11 shows the equal error rate for enhanced images from database FVC2004 DB2_A.

On the basis of the equal error rate evaluation we determine the efficiency of the enhancement algorithm and
consequently of the automated fingerprint identification system. Table 1 shows a tabulated presentation of the equal error rate (EER) for the original image and the image enhanced with Yang algorithm [22].

<table>
<thead>
<tr>
<th></th>
<th>Original</th>
<th>Yang</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FVC_2004_DB2A</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EER (%)</strong></td>
<td>12.82%</td>
<td>7.72%</td>
</tr>
</tbody>
</table>

Table 1: Equal error rate (%) for original images and images enhanced with Yang algorithm [22] from database FVC_2004_DB2A

Figure 12 shows a match for two fingerprints of the same person.

4. CONCLUSION

This study presents the steps of the automated fingerprint identification system. In this system the fingerprint image enhancement algorithm is of key importance and it influences the efficiency of the entire automated fingerprint identification system. Application for equal error rate evaluation shows a way of assessing the efficiency of the entire system and thus also shows the importance of fingerprint image enhancement algorithms. Because of poor fingerprint image quality, features on the basis of which two fingerprints match or do not match may be determined incorrectly, as shown by the application in Figure 12. On the basis of equal error rate evaluation we can determine the threshold and thus the efficiency of the automated fingerprint identification system. With lower thresholds it is more probable that an impostor fingerprint is approved (FMR). With higher thresholds however it is more probable that a genuine fingerprint is rejected (FNMR). Where the threshold is set depends on the level of security in the service where the system is used. Where the security level is higher, the threshold should also be high. In our case (Figure 10) 28 is the threshold where all impostor fingerprints are rejected.

ACKNOWLEDGEMENT

This operation is partly financed by the European Union, European Social Fund. The operation is implemented in the framework of the Operational Programme for Human Resources Development for the Period 2007-2013, Priority axis 1: Promoting entrepreneurship and adaptability, Main type of activity 1.1.: Experts and researchers for competitive enterprises.

REFERENCES


