ISSN 2616-5775 Vol. 4, Issue 4: 46-50, DOI: 10.25236/AJCIS.2021.040408

Fingerprint cipher design and matching based on orientation pattern

Yang Yue[1, 3], Haomiao Niu[1, 3], Senhao Jiang[2]

[1]North China University of Science and Technology Mathematical Modeling Innovation Lab, Tangshan, Hebei, 063210, China
[2]College of Mechanical engineering, North China University of Science and Technology, Tangshan, Hebei, 063210, China
[3]College of Chemical Engineering, North China University of Science and Technology, Tangshan, Hebei, 063210, China

Abstract: *First, the image is normalized to improve the clarity of the fingerprint image, and then the fingerprint image is cut to improve the accuracy of feature extraction. Then the fingerprint image is smoothed to reduce the noise. Based on the obvious directionality of fingerprint image orientation, the trend of striations was analyzed by the slicing method, and based on orientation, the binarization refinement operation was carried out to eliminate the skeleton of the fingerprint. When the detail feature points are determined on the fingerprint skeleton image, the relationship between the feature points and the core points can be compared to determine whether the fingerprint matches. Before matching, the effective feature points are obtained by two methods: edge removal and distance removal. After the coordinates of feature points are obtained, a series of simplified and abstract operations are carried out to convert the coordinates into hexadecimal numbers and arrange them according to certain rules. Finally, the "fingerprint password" of less than 200 bytes is obtained.*

Keywords: *Fingerprint password, Fingerprint identification, Binarization, Slitting method*

1. Introduction

Fingerprints, also known as handprints, are the bumps and bumps in the skin on the front end of a person's finger, which are arranged in a regular way to form different patterns. The starting point, endpoint, junction point, and bifurcation point of the ridge are called the detail feature points of the fingerprint. Fingerprints are produced by heredity and environment, so everyone has fingerprints, but they are not the same. Fingerprint information is too redundant if it is stored by pictures, so a new method is needed to store fingerprint passwords.

2. Fingerprint image processing

2.1 Fingerprint image normalization

Since the fingerprint image acquired initially contains too much redundant information, which may affect the subsequent processing process, image normalization is carried out to improve the clarity of the fingerprint image. The image normalization can eliminate the grayscale changes caused by different focal points in the process of fingerprint collection, and make the mean value and variance of the image meet the established value. It not only enhances the visual effect but also provides the same benchmark for subsequent operations by using the consistency of the image.

① Calculate the variance m and mean value f of the fingerprint image:

② Traverse the image and calculate the new gray value according to the given mean M_0 and variance F_0.

2.2 Fingerprint image cutting

The purpose of fingerprint cutting is to process unnecessary information and improve the accuracy of feature extraction. According to the degree that the fingerprint image is interfered with by the noise

ISSN 2616-5775 Vol. 4, Issue 4: 46-50, DOI: 10.25236/AJCIS.2021.040408

signal, we divide the image into four parts according to the region:

(1) The white background area, which refers to the boundary area that does not contain the striations. This area often presents different shades of gray because of the dirt in the scanner lens and other reasons;

(2) The foreground area, refers to the effective fingerprint ridges without noise interference;

(3) Background area, refers to the area seriously disturbed by noise, the striations can not be identified, almost impossible to recover;

(4) The fuzzy area, the fingerprint line is not clear, but the interference degree is not too serious area.

The cutting of the fingerprint image is to remove the white background area and the background area and keep the foreground area as much as possible.

Implemented in code as shown in the figure:

Figure 1: Normalize and cut sample diagrams

2.3 The denoising of fingerprint image

There are many black stomata in the white ridgeline. If the refinement is carried out directly, holes will appear where there are stomata, forming pseudo feature points.

At the same time, there are some white islands between the white ridges. If the thinning is carried out directly, these islands will become short lines and form false feature points. Therefore, we need to remove the noise first for subsequent operation.

2.4 The binarization of fingerprint image

The alternation of ridges and valleys forms the striate structure of fingerprint. The free combination of parallel, intersection, and separation forms the characteristic point information, direction information, and frequency information of fingerprint. The orientation of each position of the fingerprint image can be calculated, and the orientation map is the set of all the orientation information. At the same time, fingerprint patterns can also provide effective and reliable information for subsequent feature extraction and feature matching.

Figure 2: Binary schematic diagram

2.5 Deburring and black holes

The principle of deburring and black hole proposed in this paper is as follows: for a pixel point, if the color of three-pixel points in its four fields is inconsistent with that of the pixel point, it is determined that the pixel point is at the boundary of the hole or island, and the gray value of the pixel point should be reversed. After each traversal, the area of the holes and islands will shrink, and the process will end when the gray value of none of the pixels changes.

ISSN 2616-5775 Vol. 4, Issue 4: 46-50, DOI: 10.25236/AJCIS.2021.040408

2.6 Thinning of fingerprint image

Thinning, also known as skeletonization, refers to the process of converting image lines with a width greater than one pixel into images with a width of one pixel without affecting the topological connection of the original image, which is represented by extracting the skeleton of the image. In addition, thinning can reduce the memory occupied by images, simplify the data structure in data processing, and fully meet the requirements of ontology. The thinning algorithm should meet some properties: convergence, connectivity, topology, retention, refinement, axis, rapidity, and so on.

Figure 3: Schematic diagram after refinement

2.7 Feature point extraction

1) The extraction of feature points is the key step of the fingerprint matching algorithm based on feature points. Only when the obtained feature points are more reliable can the matching results be authentic. In this paper, the local feature points and the core points (also known as singularities) of the fingerprint are used for common comparison to complete the matching.

2) Before fingerprint matching, the pseudo feature points generated in the binarization and thinning phases of fingerprint images should be deleted.

The principle of false in the ideal state: remove every false feature point and do not delete every true feature point by mistake. In this paper, the process of de-falsification has gone through edge de-falsification and distance de-falsification.

a) Edge removal

A large number of endpoints are distributed at the junction of the background point and foreground point (i.e. the edge of fingerprint). These endpoints are generated at the edge of the fingerprint collector, which is pseudo feature points and should be removed.

This kind of pseudo feature point has a background region in the range of distance D (D =15, obtained empirically) at the edge. Principle of edge removal pseudo feature point algorithm: detect whether there is a background area in the neighborhood of 31*31 where the feature points to be measured are centered. If it exists, this point is a false feature point, and it will be removed.

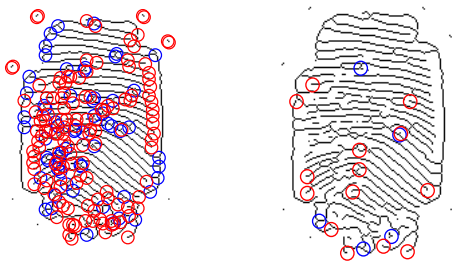

Figure 4: To fake before and after comparison

b) Distance to fake

Distance deleveraging is used to remove false feature points that are too close together, including short lines and breakpoints. Principle: The Euclidean distance between any two real feature points is generally farther than the average distance of the ridge. If the latter is further away, it indicates that there is at least one false feature point. In this case, because it is difficult to further judge the truth or

ISSN 2616-5775 Vol. 4, Issue 4: 46-50, DOI: 10.25236/AJCIS.2021.040408

falsification, two points are removed simultaneously. The breakpoint should be on the same ridgeline, and it should be the nearest point on the two breakpoints. The short line should also be on the same ridgeline and reach the other end within a certain distance from one end of the ridgeline.

The most widely used method in fingerprint identification is the Poincare index method, which is not affected by the rotation and translation of the picture, that is, it is not related to the absolute position and direction of the pixel in the image. This method is based on the orientation information of the fingerprint image. Principle: The closed curve formed around a pixel in the direction diagram is tracked and the sum of its direction difference is calculated. After a circle of track, if the direction difference changes by 180°, the pixel point is the core point; If not changed, the point is changed to a common point; If the Angle is changed by 360°, the point is triangular.

Figure 5: Schematic diagram of center point location

3. Generate fingerprint password

After correlative processing of the obtained fingerprint images, we can get the specific values of the coordinates of the corresponding bifurcation points and endpoints of each fingerprint image. Due to the specificity of fingerprint, the coordinate information, number, and distance of these feature points are different. It can realize the one-to-one correspondence relationship between fingerprint and human. The design of the fingerprint password in this paper is also aimed at this.

Because the direct storage of coordinate information will make the fingerprint password store too much information, so before image preprocessing, the size of the picture is scaled, and the scaling process will further reduce the information.

According to a literature survey, fingerprint recognition can be realized when the number of feature points is 13-20. After repeated attempts, it is found that the image size can be scaled by 0.5 times to meet the requirements of the relevant problems. The subsequent preprocessing operation is also based on the reduced image. On this basis, the hexadecimal transformation of the storage numbers is carried out. And transpose the password after the hexadecimal system. The example of "fingerprint password" after the following processing is shown in the following table.

Table 1: Schematic diagram of fingerprint password

1	8A69869DDE 748E9553E7 65AA885B8579A77779AABBBBDEEE 37C566F91F18AD1DD40E3DEF959A

After the above-improved processing method, the number of bytes of fingerprint passwords is less, and the storage is more streamlined, and all of them are less than 200 bytes.

4. Conclusion

In this paper, the fingerprint image is firstly processed, and its characteristic point coordinates are transformed into hexadecimal system and transpose. Finally, the fingerprint password with less than 200 bytes is obtained, which reduces the storage space.

ISSN 2616-5775 Vol. 4, Issue 4: 46-50, DOI: 10.25236/AJCIS.2021.040408

References

[1] Chen Ming. Research and Implementation of Fingerprint Identification Algorithm [D]. University of Electronic Science and Technology of China, 2005.
[2] Wang Chaolan. Research on fingerprint recognition algorithm [D]. Beijing Forestry University, 2019.
[3] Chang Liang. Research on fingerprint recognition based on triangle similarity principle [D]. Dalian University of Technology, 2005.
[4] He Dongyu, Cai Yuanli. Research on fingerprint preprocessing method based on pattern [J]. Computer Engineering and Application, 2004(14): 77-80.
[5] Liang Wendong. Fingerprint feature point extraction based on MATLAB image processing [J]. Computer CD Software and Application, 2014, 17(04): 24-26.
[6]Ma Ning. Research on binarization and thinning of fingerprint images [D]. Nanjing University of Science and Technology, 2006.