

Intelligent Access Control System Based on Fingerprint Identification

Shaojie Chen^a, Na Qu^{b,*} and Huilin Bai^c

School of Safety Engineering, Shenyang Aerospace University, Shenyang, China

^a18451315385@163.com, ^bmn_qn@qq.com, ^c934601811@qq.com

Keywords: Intelligent access control system, fingerprint identification, hardware design

Abstract: This paper designs the hardware and software of intelligent access control system based on fingerprint recognition. The hardware is designed with STC89C52 as the CPU, mainly including the main control chip, fingerprint module, power module and so on. Fingerprint recognition algorithm includes fingerprint image normalization, image enhancement, binarization and thinning, fingerprint feature extraction and fingerprint matching.

1. Introduction

Fingerprint recognition technology is a kind of computer intelligent technology that uses fingerprint acquisition equipment to collect living fingerprints, then extracts fingerprint features from the obtained fingerprint images by using computer image processing technology, and finally obtains the recognition results by using matching algorithm. Generally, it includes fingerprint collection, fingerprint image preprocessing, fingerprint feature extraction, data storage, feature point comparison and matching. This paper designs an intelligent access control system and a fingerprint recognition program with a single chip microcomputer as the core processor, so as to realize the function of entrance guard.

2. Fingerprint Recognition Algorithm

Fingerprint recognition algorithm includes fingerprint image normalization, image enhancement, binarization and thinning, fingerprint feature extraction and fingerprint matching. The algorithm flow is shown in Figure 1.

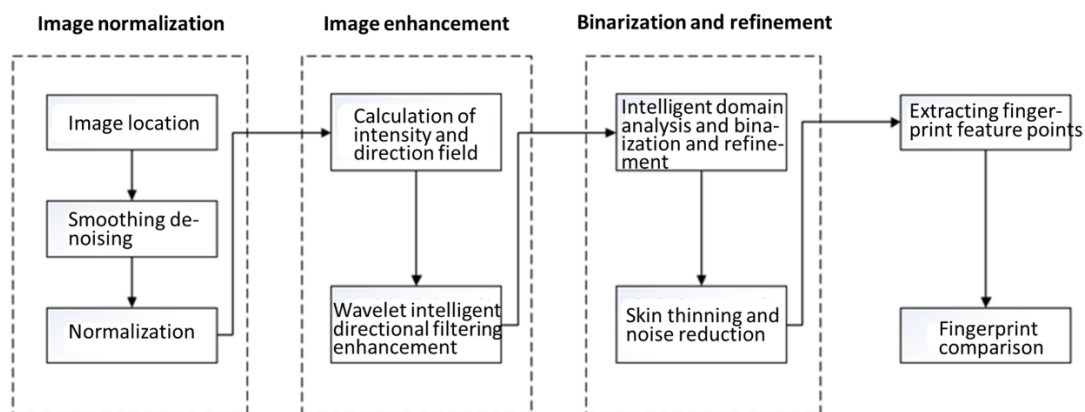


Figure 1 Fingerprint identification algorithm flow

2.1 Normalization

Normalization is to adjust the contrast and grayscale of fingerprint images to a fixed level. Suppose the fingerprint image is I , the width is W , and the height is H . $I(i, j)$ represents the gray value of row i and column j , and the average value of the whole image is obtained by formula (1) and

formula (2).

$$M(I) = \frac{1}{W \times H} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} I(i, j) \quad (1)$$

$$VAR(I) = \frac{1}{W \times H} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} (I(i, j) - M(I))^2 \quad (2)$$

The normalized fingerprint image G is the formula (3).

$$G(i, j) = \begin{cases} M_0 + \sqrt{\frac{VAR_0(I(i, j) - M(I))^2}{VAR}}, & I(i, j) > M \\ M_0 - \sqrt{\frac{VAR_0(I(i, j) - M(I))^2}{VAR}}, & \text{others} \end{cases} \quad (3)$$

2.2 Gabor Filter Enhancement

Gabor filter enhancement is the most common fingerprint enhancement algorithm using directional field images to enhance. The definition of the usual two-dimensional Gabor filtering operator is like formula (4) - (6).

$$h(x, y, \theta, f) = \exp \left[-\frac{1}{2} \left(\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2} \right) \right] \times \exp(i2\pi f x_\theta) \quad (4)$$

$$x_\theta = x \cos \theta + y \sin \theta \quad (5)$$

$$y_\theta = -x \sin \theta + y \cos \theta \quad (6)$$

2.3 Image Binaryzation

In this paper, low pass filtering is used to image binaryzation. Assuming the pixel value of any point on the enhanced fingerprint image is G (i, j), the image can be filtered by using formula (7).

$$G'(i, j) = \sum_{u=i-\frac{W}{2}}^{u=i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{v=j+\frac{W}{2}} G(u, v) \quad (7)$$

G (I,J) represents the filtered image. The equation iVar is to compare the value of the image before and after filtering, and then use the formula (8) to binary the image.

$$iVar = \begin{cases} 255, & G(i, j) > G'(i, j) \\ 0, & \text{others} \end{cases} \quad (8)$$

2.4 String Distance Matching Algorithm

In this paper, the matching algorithm used for fingerprint matching is based on string distance. First, the rotation angle and calibration point position of two sets of feature points in a Cartesian coordinate system are estimated by the least squares fitting method, and the angle of rotation which falls into the maximum number of matching points of the bounding box is used as the rotation angle. Then the two-dimensional feature points are reduced to one-dimensional strings, then the distances of two kushima are calculated by the string matching algorithm, and the results are normalized and converted to the fingerprint matching number.

3. Hardware Design of Access Control System

The hardware part of the access control system is designed by the STC89C52 MCU as the core processor, mainly including the main control chip, fingerprint module, power module, etc. The hardware circuit diagram is shown in Figure 2.

4. Fingerprint Identification Program

The function of the fingerprint identification program is to determine whether the two fingerprint images are from the same finger, and the interface of the fingerprint identification system is shown in Figure 3.

Click "Enter the System", then click on the "Input fingerprint", select a fingerprint image in the folder, the system will be the fingerprint image preprocessing, and display the finished image respectively, as shown in Figure 4.

Click "Identify fingerprint" and select another fingerprint image in the folder, the system is loaded as shown in Figure 5.

Click "Start Recognition", the system appears a small window, while displaying the fingerprint matching results, as shown in Figure 6.

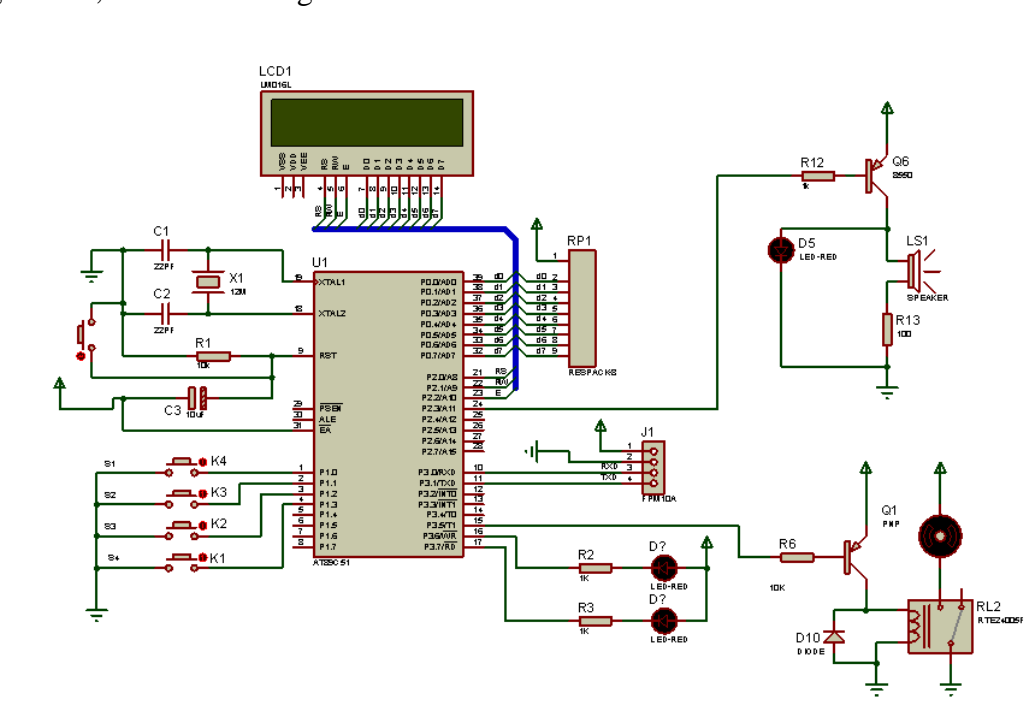


Figure 2 Access control system hardware circuit

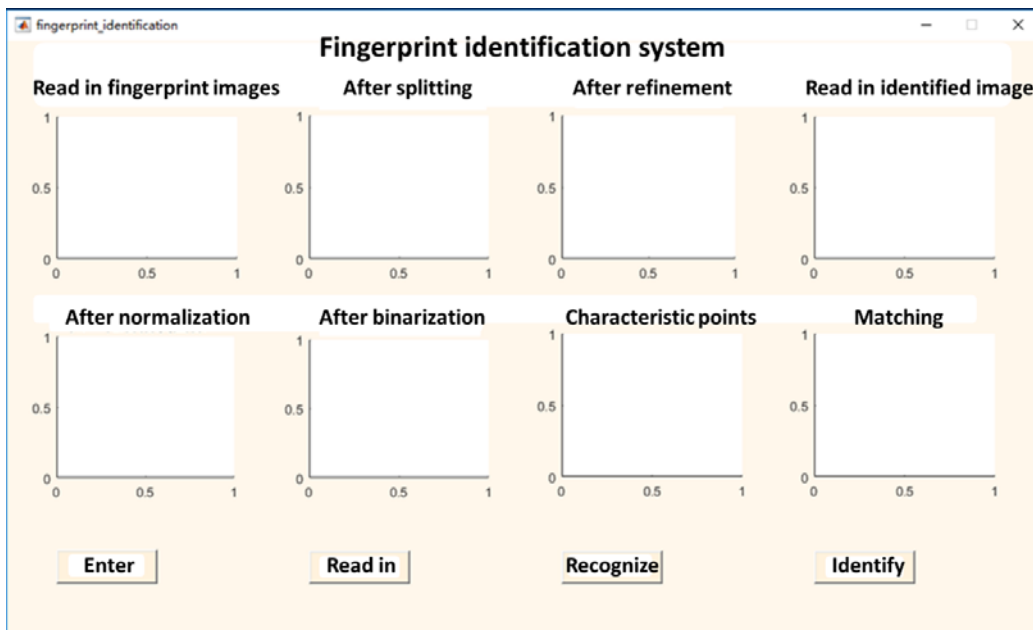


Figure 3 Fingerprint Identification System interface

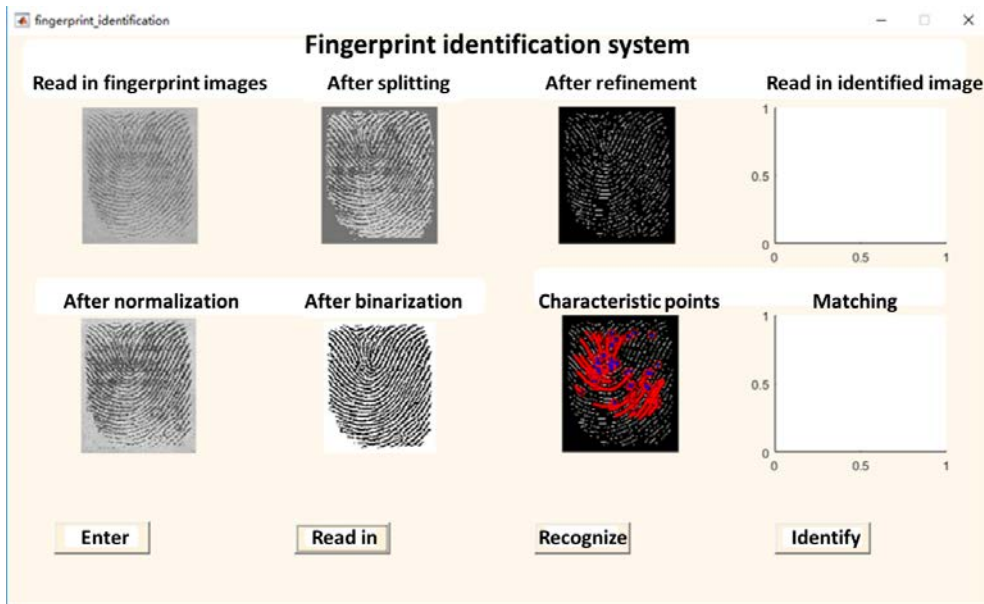


Figure 4 fingerprint image after preprocessing

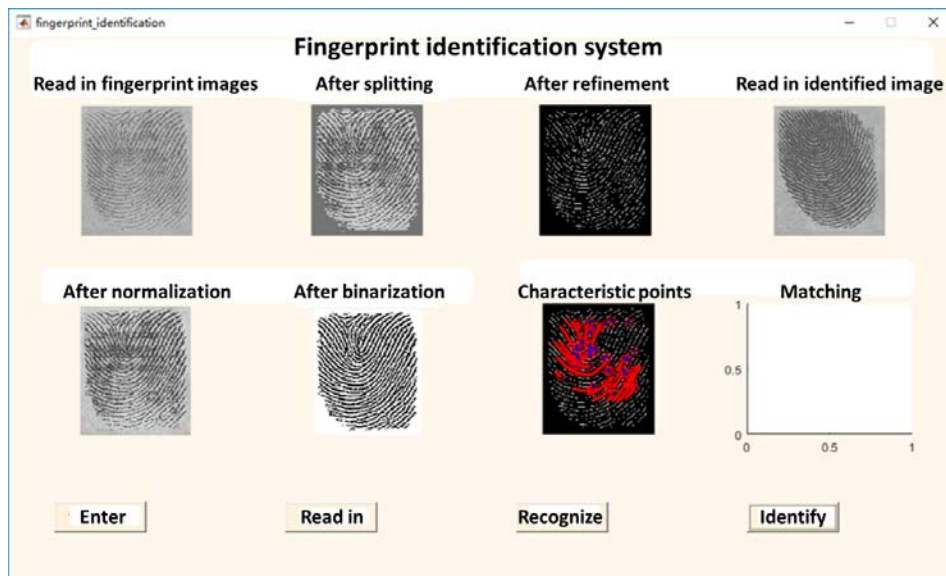


Figure 5 The interface after loading the fingerprint

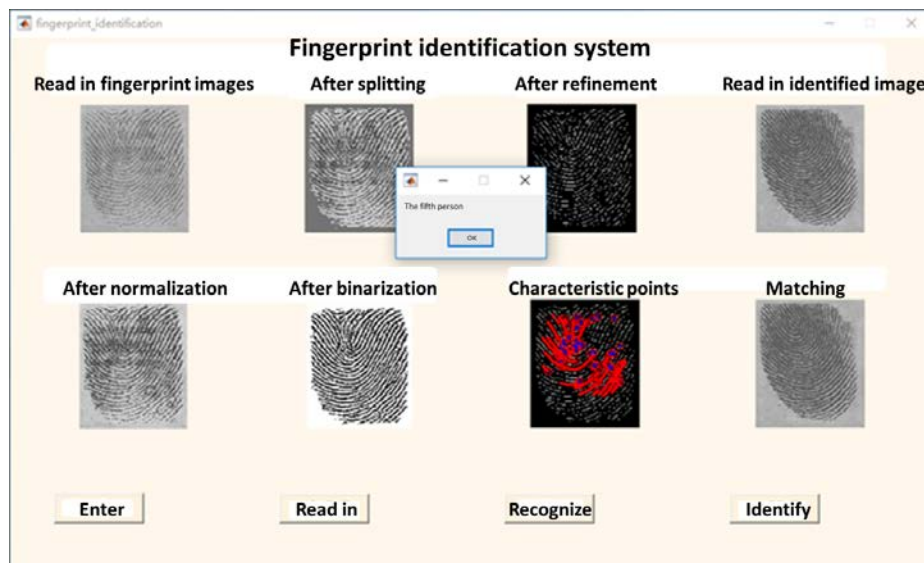


Figure 6 Results of fingerprint system matching

5. Conclusion

In this paper, the hardware part of Intelligent Access Control System is designed with STC89C52 MCU as the core processor, and the interface of fingerprint recognition system is designed by the software of Matlab. Fingerprint recognition algorithm includes fingerprint image normalization, image enhancement, binarization and thinning, fingerprint feature extraction and fingerprint matching. And simulation results show that this system is more effective.

References

- [1] Hung Liu. Application of fingerprint identification Technology [J]. China New Communications, 2017, 19(13):102-103.
- [2] Qiangmengye, pipe element, Miushlei, Wang Dong Lin. Fingerprint identification based on log Gabor filter and invariant moment [J]. Information Technology, 2017(06):133-136.
- [3] Wang Yani, Wu Zhendong, Zhang Jianwu. Research on low-quality fingerprint recognition based on convolutional neural network [J]. Communication Technology, 2017, 50(06):1276-1280.
- [4] Zoncheddu, Uranus. Research on feature point extraction algorithm of fingerprint image [J]. Information Technology, 2017(05):147-149+152.