Advances in Computer Science Research, volume 80
International Conference on Computer Science, Electronics and Communication Engineering (CSECE 2018)

The Research of Internet Identity Authentication System Based on Fingerprint Information

Feng Xiao, Yue Zhang, Fei Zhang and Yongzhen Li*
Department of Computer Science & Technology YanBian University YanJi, China
*Corresponding author

***Abstract*—With the Internet stepping into thousands of households, human beings really come into in the age of the Internet, When people are cheering for their achievements, however, information security has gradually become our incubus. And how to ensure the security of information is the most urgent problem to be solved. Because of the advantages of biometric identification, it has become a new trend in the Internet authentication. Among numerous biological characteristics, fingerprint has the characteristics of uniqueness, stability, and being collected easily. What's more, researches of identification based on fingerprint are more mature than others. Therefore, we chose the fingerprint identification as the authentication methods of our Internet authentication system. In the process of the research, we used for reference some mature fingerprint identification algorithms, and carried out a series of operations on fingerprint information which including preprocessing, feature extraction, matching and so on. After many tests and modifications, the certification system basically achieved the expectant results.**

Keywords*—information security; biological characteristic; fingerprint identification; identify authentication

I. INTRODUCTION

Human beings have only spent decades entering the information age from the Atomic age. The advent of the information age, so that our lives are filled with the color of science and technology, and the most obvious is the development of the network. In the virtual world of network, in order to set up personalized scenes, maintain order and ensure security, we need to distinguish and locate each individual. With the further development of the information age, the traditional authentication method has not satisfied the requirement of user identification in today's society. A variety of ways to crack the user's password, coupled with a growing human and network links, a variety of confidential information, property, as well as private information is transmitted and stored in the network. Using the traditional authentication method, once the user password is cracked, the loss can be disastrous, people need a more secure and reliable way to authenticate the Internet.

Biometric features have become a new trend in internet identity recognition. In many biometric features, fingerprints have long existed as a tool for identity authentication. As early as the 7000 to the first 6000 BC, fingerprints have been used as identification tools in ancient China and ancient Syria [1]. For the first time in 1880, the characteristics of fingerprint were expounded; in the same year, Henry Fonde first made a scientific exposition of the uniqueness of human biological characteristics of fingerprints, which laid the foundation for the development of modern fingerprint authentication technology. In 1974, Osterburg passed the argument that the probability of two fingerprints appearing at 12 of the same character but not of the same person was about one in ten trillion [1],for the fingerprint identification of the "12 feature points" rule provides a theoretical basis, and fingerprint recognition has been recognized by the vast number of users, which shows a very broad market and prospects. In recent years, the research on fingerprint identification has been more mature. Therefore, this paper chooses fingerprint information as the focus of the research, and focuses on the research of Internet identity authentication based on biological feature.

II. COMPARISON AND SCREENING OF FINGERPRINT RECOGNITION ALGORITHMS

A. Basic Steps of Fingerprint Identification

A complete fingerprint identification process, roughly including four steps: fingerprint image acquisition, fingerprint image preprocessing, fingerprint feature value extraction and fingerprint information matching (Figure 1.). By reference to some existing fingerprint recognition algorithms, two algorithms are selected to compare.

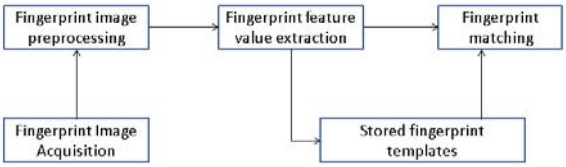

FIGURE I. AUTOMATIC FINGERPRINT IDENTIFICATION PROCESS

B. Fingerprint Recognition Algorithm Based on Point Pattern Matching

The human finger usually has 80-120 detail feature points, of which the most commonly used detail features are both vertebrae and branch points. The most commonly used feature point matching method is to use the fingerprint minutiae model proposed by the FBI to make the detail matching [2,3]. The specific algorithm is as follows:

- Normalization: The purpose is to eliminate the noise caused by the acquisition equipment and the change of the intensity of the finger, and the normalization can solve the problem so as to follow.

- Directional filtering: The algorithm uses the average separating filter based on the spatial domain directional filter to enhance the fingerprint t image.
- Banalization: The gray information needs to be removed and only the black and white color information is saved to reduce the information amount of the image.
- Thinning: Delete the edge pixels of the lines on the basis of the line's connectivity, until the line is single pixel wide, and the main purpose is to reduce the amount of computation.
- Detail feature extraction: The detailed extraction method of the algorithm is to extract the ridge tip and the fulcrum in the thinning graph of the fingerprint.

The key technical difficulty of this method is how to extract the detail features effectively and accurately, and avoid mixing pseudo features as far as possible. So it uses the 8 neighborhood codes commonly used in image processing to track the image, thus the effective extraction of the true detail feature is completed.

C. Fingerprint Recognition Algorithm Based on Texture Feature

Different from the previous algorithm, the algorithm is based on texture characteristics. The object is the characteristics of the whole stripe line, such as the curvature of the lines. In addition, the algorithm is very different from the first algorithm in the processing of directional filtering[4].

The specific algorithm is as follows:

- Direction diagram: The algorithm is used to calculate the directional graph by using Multi window method. The fingerprint direction graph is divided into several 4x4 blocks, in order to calculate the direction of each block area, it is necessary to consider the 8 neighboring blocks of the neighborhood . A direction D which has the most occurrences among the four peak directions is selected as the area direction of the 4 × 4 sub-block. The direction of the area of each sub-block is sequentially obtained to obtain the block pattern of the fingerprint.
- Seek the center point: The center point is defined as the maximum curvature of the ridge curve of fingerprint. In the matching algorithm based on point pattern, the center point as a matching reference point has strong consistency. The algorithm is based on the fingerprint direction map, and the algorithm is simple and adaptable to the type.
- Gabor filtering: Since the extracted fingerprints are the local structure of the fingerprint texture, the grid scheme of the fingerprint sub blocks chosen in this algorithm is a circular grid. Therefore, before the Gabor filter is filtered, the image should be fanned and then the ridge frequency estimated.

By carefully comparing the advantages and disadvantages of the two algorithms, and according to the problems we encounter in the concrete practice, we use the fingerprint recognition algorithm based on the point pattern matching to carry on our design research.

III. FINGERPRINT IMAGE PROCESSING

A. Fingerprint Information Collection

We use optical fingerprint collector. The fingerprint samples collected are as follows:

FIGURE II. SAMPLE

B. Fingerprint Image Preprocessing

1) Normalization of fingerprint images

The normalization of an image is an operation on each pixel point on the original grayscale image, which changes its gray value artificially. The purpose of normalization is to adjust the contrast and average grayscale of different original images to a fixed level, to reduce the influence of different contrasts of different fingerprint images, to eliminate the noise caused by the collector itself and to be caused by the difference of finger pressure The difference of the gray level, the average separation filter based on spatial domain directional filtering is used to filter the fingerprint image, which is more effective for filling holes and broken lines, providing a more uniform image specification for subsequent processing. Calculating the gray mean and variance of the whole image [5]:

$$M(I) = \frac{1}{N^2}\sum_{0}^{N-1}\sum_{0}^{N-1} I(i,j),\ (i,j) \in I$$

$$VAR(I) = \frac{1}{N^2}\sum_{0}^{N-1}\sum_{0}^{N-1} (I(i,j) - M(I))^2,\ (i,j) \in I$$

Normalize the fingerprint image:

$$G(i,j) = \begin{cases} M_0 + \sqrt{VAR_0 * (I(i,j) - M(I)^2)/VAR(I)}, & I(i,j) \geq M(I) \\ M_0 - \sqrt{VAR_0 * (I(i,j) - M(I)^2)/VAR(I)}, & I(i,j) < M(I) \end{cases}$$

Let the fingerprint image I be the size of N × N, and I(i ,j) be the gray level of the pixel point(I,j). M and VAR are the mean and variance of the fingerprint image respectively.

G(j) is the original gray value of the input pixel. M0 is the expected average gray value of the image. VAR0 is the difference of the expected image. M represents the estimated mean gray level of the real input image. Var represents the estimated gray variance of the real input image, and G(j) represents the normalized image gray value. Subsequent fingerprint images are processed on this basis.

Most of the research on the enhancement of grain lines has been done, and most of the lines are used as the parameters of the enhancement algorithm. For example, Hong proposed a Gabor function filter to improve the quality of low-quality fingerprint images, the effect is better, but the algorithm is quite complicated and time-consuming, it is difficult to meet the real-time requirements. Sherlock [6] and others designed to achieve the fingerprint image enhancement, but the algorithm does not use the frequency domain information of the ridge. O 'Gorman and others[7]proposed a method of designing a set of directional filters to improve the quality of the fingerprint image, which is faster and more accurate when the direction information of the fingerprint is more accurate. Because the fingerprint direction of the paper is more accurate, we use o ' Gorman and other people's methods.

2) Fingerprint image filtering

Because the fingerprint is directional and special image of alternating ridges, in the filter design must consider its particularity, according to the different direction of pixels using the principle of design of different filter templates are as follows [5]:

- The filter template size should be appropriate. The size of the filter template requires one or a half cycle of the ridge.
- The size of the template must be odd so that the template can be symmetrical about the x-axis and y-axis through the center.
- In order to improve the contrast between ridges and valleys and achieve the effect of edge sharpening, the template should be designed such that the coefficients of the central part are positive and the coefficients of both sides are negative perpendicular to the direction of the ridge.
- The filtering result should be independent of the average gray level of the original image, so the algebraic sum of all the coefficients in the filter template should be zero.

A basic directional filter (shown as c in Figure 3.) is composed of the averaging filter (a in Figure 3.) and the decoupling filter (b in Figure 3.). The average filter coefficients satisfy: X≥Y≥Z≥0, if there is a breakpoint in the image, that is, the gray value of this point is much smaller than the surrounding points, and its average gray value is close to the average after the filter processing Point of the gray value. So the average filter has the effect of connecting breakpoints. The coefficients of separation filtering satisfy: P + 2Q + 2R = 0. In the image, the connecting point of the fork is the point connecting the adjacent two ridge lines. Therefore, the gray value of the upper and lower rows of the connecting point of the fork is larger while the gray value of the neighboring point on the same row is smaller. Through the processing of the separation filter, the gray value of the fork will be significantly reduced, so the separation filter has the effect of removing the fork connection point.

Z	Z	Z	Z	Z	R	R	R	R	R	M	M	M	M	M
Y	Y	Y	Y	Y	Q	Q	Q	Q	Q	L	L	L	L	L
X	X	X	X	X	P	P	P	P	P	K	K	K	K	K
Y	Y	Y	Y	Y	Q	Q	Q	Q	Q	L	L	L	L	L
Z	Z	Z	Z	Z	R	R	R	R	R	M	M	M	M	M

a. averaging filter b. decoupling filter c. directional filter

FIGURE III. FILTER

The filtered image is processed by two valued fingerprint images, and the gray image is transformed into two gray level images, which can be used to reduce the amount of information of the image. We combine the advantages of the two algorithms to improve the refinement effect. First of all, the fast thinning algorithm is used to make a preliminary refinement, the thinning fingerprint is wider, and then the improved OPTA algorithm is further refined [8].

C. Feature Value Extraction of Fingerprint Image

The detail extraction method of the fingerprinting algorithm based on the point pattern is to extract the tip of the ridge and the branch point on the thinning map of the fingerprint. The accuracy of this method is relatively high, and the complexity of the algorithm is also relatively low, easy to implement.

At present, most systems use the method of extracting features from the thinned binary image. This method is relatively simple. Only a 3 × 3 template can be used to extract the tip and bifurcation points after a reliable thinned binary image is obtained come out. For the refinement of binary images, there are only two kinds of gray values of pixels (assume that 0 represents the gray level of the background point and is represented by the white dot; 1 represents the gray level of the dark line dotted line). N is the number of pixels Point, X1, X2 ... X8 is its 8 neighborhood points, R (1), R (2) ... R (8) are the gray values of X1, X2 ... X8. If N is a vertex, then its 8 neighborhoods satisfy [9]:

$$C_N = \sum_{k=1}^{8} | R(k+1) - R(k) | = 2, R(9) = R(1)$$

If N is a bifurcation point, then its 8 neighborhood points are satisfied:

$$C_N = \sum_{k=1}^{8} | R(k+1) - R(k) | = 6, R(9) = R(1)$$

Using ridge tracking technology, the number of its 8-neighborhood documents is defined as:

$$S_N = \sum_{k=1}^{8} R(k)$$

$$\begin{matrix} X_8 & X_1 & X_2 \\ X_7 & N & X_3 \\ X_6 & X_5 & X_4 \end{matrix}$$

FIGURE IV. N POINT 8 NEIGHBORHOOD

For the tip point, the neighborhood of 8 ridge points SN = 1, that is, there is only one ridge point 8 neighborhood. This point is the next point of the line tracking. For the middle point of the ridge, the number of adjacent ridge points in 8 is SN = 2, that is, there are two ridge points in the neighborhood of 8, and the last point to be tracked is removed, and the remaining point is the next point to be tracked. For the bifurcation point, 8 neighborhood ridge points SN = 3, that is, there are three ridge points in 8 neighborhoods. For the bifurcation point tracking, we can start from these three ridge points separately, tracking along three different ridge lines respectively. Combined with the distribution of the detail feature points in the thinned fingerprint, the pseudo-feature points of the fingerprint details are filtered out and the false feature structures such as burrs, triangles and broken lines are identified and filtered, and finally the true feature points are obtained.

IV. THE SPECIFIC REALIZATION OF FINGERPRINT MATCHING

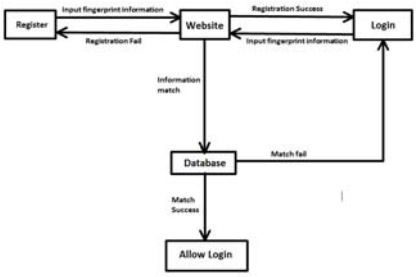

FIGURE V. FINGERPRINT MATCHING FLOW CHART

Through the fingerprint image processing, we will get the fingerprint information into the database. In order to simulate user login and better complete the related research, we made a simple login website. At this point, all the preparatory work is completed. Next, the identity authentication of the user is the most important step in our entire study. Among the main problems to be solved are:

- Real-time processing efficiency of user fingerprint information.
- Threshold setting of matching algorithm.

Through the actual testing of the data obtained from some of the relevant algorithms and experience threshold, we have made the authentication system threshold as follows: For users whose fingerprinting matching rate is higher than 90%, they are regarded as legal users and pass the authentication. Match rate higher than 75% lower than 90% of users, give hints for the second authentication; For users whose matching rate is less than 75%, they are regarded as illegal users. Authentication fails and login is denied. Based on the above settings, we have done a lot of tests on the system. After statistics, we found that the passing rate of user authentication of the system is 89%, which achieves the expected result basically.

V. CONCLUSION

Through this study and related confirmatory experiments, we have a deeper understanding of the importance of the security of Internet identity authentication and the tendency of biological features to replace the traditional login methods. The work we do is far from enough and we hope to get more results in the future. Here, thank our guidance teacher, thank all in these months to help our predecessors and classmates.

REFERENCES

[1] Hao Li, Xi Fu, Proficient in Visual C++ And Algorithms Implement of Fingerprint Pattern Recognition System [M]. Posts & Telecom Press, BeiJing,2008

[2] LI Chen-Dan, XU Jin. Facilities Implementation of Fingerprint Image Preprocessing and Feature Extraction [J] .Computer Science and Engineering, 2002,31 (7)

[3] Wang Chong wen, Li Jian Wei, Zheng Zhiwei. A fingerprint identification method based on model [J]. Journal of Chongqing University, 2002,25 (6): 27-31

[4] Zhu Lingyun, Chen Shao Chun. Fingerprint recognition algorithm based on texture features [J]. automation and instrumentation, 2009, (2)

[5] Zhang Ming. Fingerprint image enhancement algorithm based on directional filtering, [J]. microcomputer development, 2005, 15 (33): 86

[6] Sherlock D, Momro D M, Millard K. Fingerprint enhance-ment by directional Fourierfilter[J]. IEEEProceedingsof Vi-sion Image and Signal Processing, 1994,141(2):87-94.

[7] O'Gorman L, Nickersion J V.An approach to fingerprint fil-ter design[J]. Pattern Recognition, 1989,22(1):29-38.

[8] Wang Lixiang. Research on fingerprint thinning algorithm [J]. Heilongjiang science and technology information, 2009, 15-42

[9] Liu Ling li. Fingerprint image preprocessing and feature extraction [D].2005.11-33