Fingerprint Recognition System based on Big Data and Multi-feature Fusion

Mikai Yang
Shenzhen Knowsight System Co.,Ltd.
Shenzhen, P.R.C.
e-mail: michael@knowsight.com

Abstract—**This paper proposes a fingerprint recognition algorithm, which is based on deep learning and multi-feature fusion, is able to solve the shortcomings of traditional fingerprint recognition that purely relies on minutiae features for recognition, especially in the case of partially incomplete fingerprints or small-area fingerprints. For identification, while the user inserts a fingerprint in the terminal, the system will transmit raw data to the deep learning engine of the cloud in an anonymous and encrypted manner, which can quickly collect a large amount of fingerprint data in an aligned manner. Based on these data, parameters of the deep-learning model are adjusted incrementally, pursuing optimal accuracy of the system. Meanwhile, SaaS services are provided to other applications for fingerprint recognition.**

Fingerprint recognition, deep learning, SaaS, cloud computation

I. Introduction

Fingerprint recognition technology is currently used in various mobile devices and various scenarios. The market has new requirements for the design of security, integration, low cost and low power consumption. Fingerprint devices are also more inclined to use small-sized Fingerprint sensors (small-sized fingerprint sensors contain less user information), will inevitably put higher requirements on the fingerprint recognition algorithm. In this paper, a design and implementation of a fingerprint recognition algorithm based on big data deep learning and multi-feature fusion are designed. Specifically,(a) it can solve the problem of reduced recognition performance due to insufficient effective information of small-area fingerprint images; (b) the user's fingerprint image data is encrypted and transmitted to the web server, and a massive anonymous fingerprint database is established in a low-cost and efficient manner to provide data support for the fingerprint recognition deep learning engine; (c)deep learning engine of the server continuously optimizes parameters of the system, and also outputs user comparison results; (d)SaaS service API in the cloud provides fingerprint comparison function and fingerprint algorithm performance verification function for other applications; (e) the system can work locally or cloud-based. Per different usage scenarios, you can choose to work locally, work in the cloud, and work locally and in the cloud at the same time.

II. Fingerprint recognition system

This paper proposes an automatic fingerprint recognition system. Its system structure is shown in Figure 1 below. The system is obviously different from the traditional automatic fingerprint recognition system. After the user enters the finger in the fingerprint recognition terminal, the user can independently and automatically complete the fingerprint image pre-processing, feature information extraction, matching and output comparison results (unlocking, identity authentication, etc.) And the original fingerprint data of the user can be encrypted and transmitted to the Web server. This method can build a massive anonymous fingerprint database in a low-cost and efficient manner, and provide data support for the subsequent fingerprint recognition deep learning engine. Through the server's deep learning engine, the relevant parameters of the fingerprint recognition system are continuously optimized. With the user's use, its security and ease of use are characterized by self-improvement and adaptive adjustment. This technology will undoubtedly adapt to the user's usage habits to a higher degree. To enhance the overall experience of the product. Sections 2 introduces in detail the system working mode, fingerprint identification algorithm, and cloud SaaS service.

A. *Work Process of the System*

The fingerprint identification system proposed in this paper has a flexible working mode. After the fingerprint identification terminal collects the user's fingerprint information, it can not only complete the entire fingerprint identification locally and fully automatically, but also encrypt the user's original fingerprint data and transmit it to the web server. The comparison result is output by the server, or it can work locally or in the cloud according to the actual situation: (a)the automatic fingerprint recognition algorithm can run independently on the M3/M4 embedded platform; (b) the user's original fingerprint data is encrypted and transmitted to the Web server, and a massive anonymous fingerprint database is established in a low-cost and efficient manner to provide data support for the subsequent fingerprint recognition deep learning engine. The cloud fingerprint deep learning engine system usually only provides regular feedback update packages (including model optimization parameter information) to the user equipment. It is also feasible to directly return the comparison results to the user if needed. Its advantage is that the user equipment does not need to have a real-time stable connection with the cloud.

978-1-7281-8138-7/20/$31.00 ©2020 IEEE
DOI 10.1109/ICCST50977.2020.00097

The user equipment can independently complete all comparison and identification tasks without real-time assistance from the cloud. The deep learning engine in the cloud uses machine learning algorithms for incremental learning. With the continuous increase of data, these data are used for model training and learning, which can improve the performance of the model. (c) Local and cloud can be integrated. In the case of a stable network connection between the local and the cloud, only the process of fingerprint feature extraction is performed locally. The feature comparison process can use the powerful computing power of the cloud to achieve fast results, especially for large fingerprint indexing system.

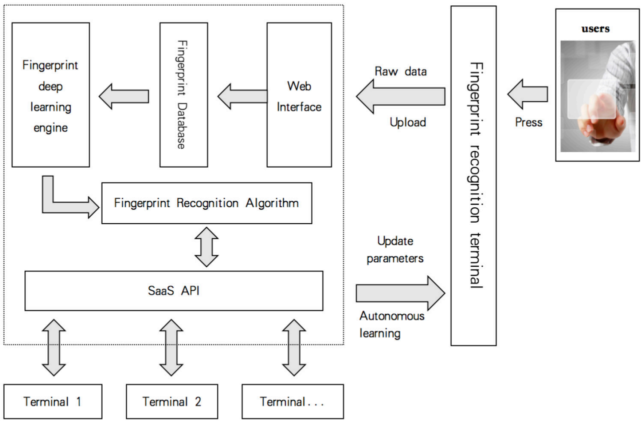

Figure 1. Fingerprint recognition system based on big data and multi-feature fusion

B. Algorithm of Small-sized Sensors

At present, there are relatively few fingerprint algorithms that are specifically designed for small area fingerprint recognition and can run on low-power, low-resource embedded platforms. For the actual use requirements, this paper has targeted the small area fingerprint images in the fingerprint feature extraction, feature comparison, and feature template update stage.

In the fingerprint feature extraction stage, a FSFD (Fingerprint Image Semantic Feature Point Extraction Method) is used. FSFD has the following characteristics: (a) the features are widely distributed in the fingerprint image, and a large number of missing or damaged fingerprints can also be extracted feature information; (b) feature expression ability is strong, and can be easily used in combination with other fingerprint features to improve the recognition effect; (c) features can be quickly and stably detected.

In the stage of fingerprint feature comparison, the pixel gray value and its auxiliary information (gradient information, curvature information, etc.) in the patch around the feature point are randomly sampled and deferentially encoded to form the descriptor of the feature point. The encoded information has the following features: (a) the coding information is invariant to direction; (b) the coding information has strong regional discrimination and robustness; (c) the coding information occupies less memory space, and uses binary descriptors to express the regional information; (d) the encoded information has a fast indexing mechanism and comparison scheme.The method of FSFD feature extraction is shown in formulas 2-1 ～ 2-5, whereI_x, I_{xx}, I_y, I_{yy}, I_{xy} respectively are the first-order and second-order Gaussian partial derivatives of the fingerprint image, which is the fingerprint semantic feature expression image, where the local extremum points are defined Feature points of fingerprint images.

$$K = \frac{I_{xx} I_{yy} - I_{xy}^2}{(1+ I_x^2 + I_y^2)} \qquad （2 -1）$$

$$H = \frac{I_{xx}\left(1+I_y^2\right) + I_{yy}(1+I_x^2) - 2I_x I_y I_{xy}}{(1+ I_x^2 + I_y^2)^{3/2}} \qquad （2 -2）$$

$$maxC = \ H + \sqrt{H^2 - K} \qquad （2 -3）$$

$$minC = \ H - \sqrt{H^2 - K} \qquad （2 -4）$$

The underlying semantics of the gray-level fingerprint image can be described as:

$$I_{TGL}(x,y) = maxC - minC \qquad （2-5）$$

In the self-updating stage of the fingerprint template, a flexible self-learning mode is used to update. The flexible update mode has the following characteristics: (a) the fingerprint feature template information of one finger

occupies a fixed amount of memory space; (b)The finger area is changed to adapt to user usage habit. The above-mentioned three-stage process does not demand too much computation and can be quickly run on a low-power embedded system with limited resources.

C. SaaS API

Services of fingerprint verification and recognition are provided in terms of cloud-based SaaS API. Using the Saas service API function in the cloud, related application terminals can easily and efficiently implement the design of fingerprint recognition products. Third-party algorithm designers can also quickly verify the performance of their algorithms. By taking advantages of the SaaS API in the cloud, end users reduce cost on software development so that they can focus on product innovation.

III. Conclusion and Future Work

The achievements of this paper include: (a) the establishment of a massive anonymous fingerprint database. Achieve PB-level data storage pre-processing capability; (b) design of fingerprint deep learning engine. According to the massive anonymous fingerprint database, the implementation of the fingerprint recognition algorithm can be continuously optimized according to the user's usage habits to obtain better and better performance of the system; (c) small-sized fingerprint recognition algorithm design, fully extract the feature point information, line information, and image in the fingerprint image Information, through information fusion technology to design a highly reliable and efficient fingerprint recognition and verification system; (d)supporting a low-power embedded system platform; (e) providing cloud SaaS service API for other application.

The fingerprint recognition algorithm with feature fusion and deep learning based on big data is a more advanced fingerprint recognition scheme. Its application range and recognition effect are greatly improved compared with traditional methods, overcoming the excessive reliance on details in traditional recognition. It has sufficient market value and can generate huge social benefits. In the future, we will further optimize the time and resource consumption of data transmission between the cloud fingerprint deep learning engine and the embedded smart device. This framework can be also applied to other embedded smart device applications, such as human face recognition, iris recognition, palm print recognition, voice recognition, etc. Multi-mode biometrics are feasibly integrated into a unified framework.

REFERENCES

[1] Loris Nanni, Alessandra Lumini. Descriptors for image-based fingerprint matchers[J].Expert Systems with Applications 36(2009)12414-12422.

[2] Matteo Ferrara, Davide Maltoni. Minutia Cylinder-Code: A New Representation and Matching Techniquefor Fingerprint Recognition[C].IEEE Transactions on Pattern Analysis And Machine Intelligence, VOL. 32, NO. 12, DECEMBER 2010.

[3] Shaharyar A K,Zahra Saleem,A Comparative Analysis of SIFT, SURF, KAZE,AKAZE, ORB, and BRISK[J].Proc. IEEE.2018.8346440.

[4] Roddy A R, Stosz J D. Fingerprint Features-Statistical Analysis and Aystem Performance Estimates[J]. Proc. IEEE,1997(85):1390-1421.

[5] Tsai-Yang Jea, Venu Govindaraju A minutia-based partial fingerprint recognition system[J]. Center for Unified Biometrics and Sensors, University at Buffalo, State University of New York,Amherst, NY USA 14228.