Journal of Biometrics & Biostatistics

Sul S. J Biomet Biostat 2011, 2:2
DOI: 10.4172/2155-6180.1000111

Research Article

Open Access

Classification-based Automatic Fingerprint Identification System for Large Distributed Fingerprint Database

Seungjin Sul

Danbi Soft, LLC, College Station, TX 77845, U.S.A

Summary

Fingerprint is the cheapest, fastest, most convenient and most reliable way to identify someone. And the tendency, due to scale, easiness and the existing foundation, is that the use of fingerprint will only increase. Cars, cell phones, PDAs, personal computers and dozens of products and devices are using fingerprints more and more. When it comes to deal with large-scale fingerprint database, the scalability of current fingerprint recognition system is not proved yet. Our target application is a centralized user authentication system for e-commerce including online shopping malls and for user identification for government web services. In this paper, we introduce a large-scale fingerprint recognition system which incorporates fingerprint classification, large-scale identification, multiple server based identification. Our experimental result shows that our multi-server system takes 5.2 - 5.36 seconds to identify a fingerprint from 100,000 fingerprints.

Keywords: Biometrics; Fingerprint recognition; Large distributed database; Automatic finger-print identification system; Classification

Introduction

User authentication by fingerprint recognition makes it possible to have more secure system than traditional system which is based on user password. Such biometric authentication systems provide great amount of convenience compared with password-based authentication system and also allow users not to remember or periodically change their passwords [1]. Centralized fingerprint authentication system widens its application of fingerprint authentication into e-commerce, e-business and user authentication in various web services. However, performance evaluation of fingerprint identification system with large fingerprint database has not been clear done in the previous work [2,3,4]. In this paper, we introduce a high-performance fingerprint identification system which incorporates with fingerprint classification, multi-server platform, multi-threaded, authentication server and evaluate the performance using a fingerprint database which populates 100,000 registered fingerprints.

Background

For achieving higher accuracy in fingerprint recognition technology, many literatures have been published on fingerprint image preprocessing, feature extraction, fingerprint pattern matching and automated fingerprint identification system (AFIS). In this work, the main goal is to develop a high performance fingerprint identification system based on multiple servers for comparing hundreds of thousands fingerprints. We have already proven the performance of our fingerprint recognition algorithm by developing stand-alone fingerprint recognition devices like fingerprint recognition mouses and fingerprint recognition door locks [5]. The fingerprint recognition algorithm for operating the devices are designed to be very resource-efficient because the devices are developed on ARM7 processing unit which has very slow CPU and small amount of available memory space. The fairly optimized and efficient algo-rithm is adopted for developing the identification system introduced here. We also propose a fingerprint classification algorithm based on image block classification method. First, preprocessed fingerprint image is divided into several blocks and the extracted characteristics of the blocks are used to classify the image into pre-specified categories such as arch, whorl, left loop, and right loop.

Along with the efficient recognition algorithm, large scale identification system returns the search result in reasonable amount of response time. In other words, it has to provide good response time to users. By designing the system on multi-threaded and multi-server platform, we can achieve the goal. In our implementation of the identification system, fingerprint images are stored in a distributed manner following the category of classification of fingerprints. Proper data mirroring and automatic backup services should be considered for safe storage. Each identification server processes search queries in parallel way. The multi-threaded search engine submits the features information extracted from fingerprint image into multiple servers using multi-threading. For the experiment, we configure a distributed database system and multiple identification servers.

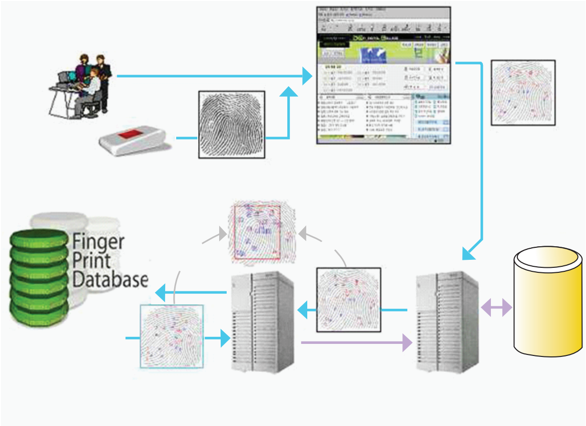

Figure 1: Overview of our fingerprint identification system.

***Corresponding author:** Sul S, Danbi Soft, LLC, College Station, TX 77845, U.S.A, E-mail: ssul0270@gmail.com

Received July 21, 2010; **Accepted** January 31, 2011; **Published** February 4, 2011

Citation: Sul S (2011) Classification-based Automatic Fingerprint Identification System for Large Distributed Fingerprint Database. J Biomet Biostat 2:111. doi:10.4172/2155-6180.1000111

Identifying fingerprints

Figure 1 shows the overall structure of our large-scale fingerprint identification system and the processing steps. First, the fingerprint image scanned from a user is registered to the database through web-based client. For scanning, we use two fingerprint scanners we have developed. Our fingerprint recognition mouse scans the image with electrical image sensor from Siemens. The other scanner we used which has an optical scanner. The reason why we used two scanners is that the optical scanner can acquire good quality images. Thus we would like to test the performance of identification based on a variety of fingerprint image quality. The main application for the identification system is user authentication for e-commerce through web service, thus we develop ActiveX component which can be easily inserted into any web page which needs the fingerprint user identification. The component scans fingerprint image from user and send the image to web server. Web server then request identification of the fingerprint image to identification servers. Each identification server processes the query and starts the matching with fingerprint images stored in distributed database. If the user is authenticated, the result is sent back to the web server, and the server retrieves the user information from its user information database and represents the information to web page.

Our fingerprint identification server takes advantage of multi-threading and multi-server paradigms to improve the response time for identifying fingerprints. During the registration process, the scanned fingerprint images are stored in distributed manner based on fingerprint classification [6,7,8]. Even if fingerprints are stored in distributed locations, the number of fingerprint images to compare is enormously large. To get a faster response time, reference fingerprints images should be searched in parallel. Once a fingerprint image submitted to the central server, it is classified based on ridge information which in turn decides which database should be searched. If database is selected, fingerprints stored in the database are compared by multi-threaded approach.

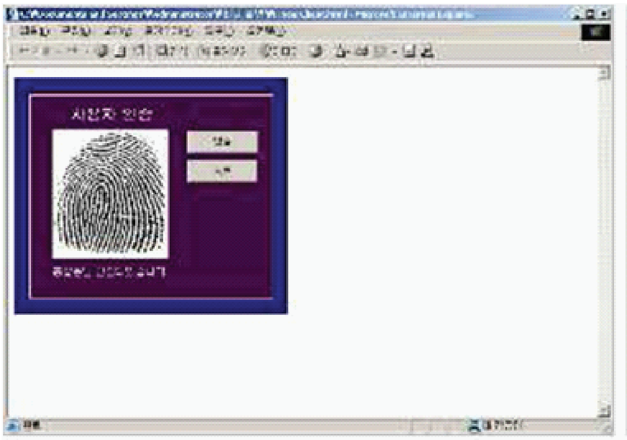

Figure 2: Fingerprint scanning and registration client component based on ActiveX.

```
    public native int JDFPGetFeature (
    int [ ] img ,            // fingerprint image
    int [ ] FeatureArray // minutiae
) ;
    public native int JDFPMatchFingerEx (
    int [ ] FeatureAttay1 ,   // base feature points
    int [ ] FeatureArray2 ,  // reference feature points
    int Level                      // matching level
) ;
```

Listing 1: JNI methods for fingerprint identification

Identification client

To register user fingerprint image to servers, a client program is used to scan fingerprints and send them to registration server. Identification client operates the physical scanner. We develop the client using ActiveX to allow users easily incorporate the component into their web-based applications. Figure 2 shows an example web page which has the scanning and registration component.

Implementation and experiment

Our identification server is implemented using Java language on Windows operating system. Recognition algorithm is compiled to DLL (Dynamic Link Library) and linked to Java identification server through JNI (Java Native Interface). We choose Java to maximize the portability. Listing 1 shows the fingerprint identification methods which are called through JNI. JDFPGetFeature gets the fingerprint image scanned from sensors and extracts features from the scanned images. Those features are stored in database for future identification. JDFPMatchFingerEx compares the feature points of input fingerprint with reference finger-print. The matching level controls the hardness of the comparison. If higher value of level is used, identification takes longer but produces more accurate result. Additional feature of JDFPGetFeature is the extracted feature information is encrypted before storing to guarantee security while transmission.

```
class MyShareVar {
    private boolean isFind = false ;
    private String threadName ;
    public boolean getIsFind ( ) {
    return isFind ;
}
public synchronized void
    setIsFind ( boolean value ) {
    isFind = value ;
}
public String getThreadName ( ) {
    return threadName ;
}
public void setThreadName ( String value ) {
    threadName = value ;
}
```

Listing 2: Shared thread class

Class	Number of fingerprints (%)
Arch	27,280 (27%)
Whorl	19,960 (20%)
Left loop	19,660 (20%)
Right loop	33,100 (33%)
Total	100,000 (100%)

Table 1: Number of fingerprints per category.

	Avg. 10 reps. (sec)	Avg. 100 reps. (sec)
Single-server	7.56	8.9
Multi-server	5.2	5.36

Table 2: Performance of our identification servers.

The experiments are done using two desktop PCs (Intel CPU 3.0GHz, RAM 4GB) with Windows Server operating system. The data sets are consisted of 1,000 scanned images from our lab and 4,000 NIST fingerprint images. The NIST fingerprint images are resized to match with the scanned images. The images are replicated and the total number of images is 100,000. Table 1 shows the distribution of the number of fingerprint images for each fingerprint category. We consider only four classes of fingerprints: arch, whorl, left loop, and right loop. The reason why we choose those four categories is to increase the classification accuracy which contributes to higher hit ratio of distributed database. In other words, when an input image is classified, the image is sent to specified database which stores only the fingerprints of the category.

The response time is recorded for both one identification server and two identification servers and averaged after 100 repetitions. Further, multi-threaded, multi-server case and single-threaded, single-server case are tested separately.

When trying to identify the input fingerprint image on the identification servers, each identification server starts multiple threads. As one of the threads find the matched finger-print, the other threads should stop its search. The synchronized keyword is used for the reason and makes all shared variables thread-safe. Listing 2 shows the multi-thread class used for the above purpose. Each thread checks the variable, ”isFind”. If isFind is set to true, it terminates itself because it means one of other threads has already found the matched fingerprint.

Table 2 shows the response time results. Again, single-server means single-threaded running on single server and multi-server means multi-threaded search on multiple servers. The result clearly shows that the multi server performs better than single server.

Summary

We introduce multi-thread, multi-server based large-scale fingerprint identification system which is designed to be applied government fingerprint recognition service and e-commerce systems. The experimental results with 100,000 test data sets show that multi-threaded, multi-server identification system performs better than single-threaded, single-server system. Notable feature of the identification system is that it utilizes the classification of fingerprints and stores the fingerprints physically distributed locations. To support web service developers with convenient way to have the fingerprint identification service on their web service, we provide them with a component-based client interface for fingerprint scanning and registration. The main part of the system is implemented by Java language so that it can maximize the portability. For security reason, the extracted feature points are encrypted. Our results show that the average response time is less than 10 seconds which satisfies the performance criteria of large-scale fingerprint identification system. Further, our classification accuracy is over 90% in average.

As part of our future work, we'll increase the classification accuracy up to 99% which in turn will result in higher identification performance. Further, we'll develop a test e-commerce web service and check the applicability of our system. At the same time, we should increase the number of servers up to hundreds of nodes based on cluster or grid to check the scalability.

References

1. Jain AK, Prabhakar S, Hong L, Pankanti S (2000) Filterbank-based fingerprint matching. IEEE Trans Image Process 9:846-859.
2. Bhanu B, Tan X (2001) A triplet based approach for indexing of fingerprint database for identification. Proceedings of 3rd International Conference Audio and Video-Based Biometric Person Authentication.
3. Cappelli R, Maio D, Maltoni D (2000) Indexing fingerprint databases for efficient 1:n matching. Proceedings of 6th International Conference on Control, Automation, Robotics and Vision.
4. Nalini K Ratha, Kalle Karu, Shaoyun Chen, Anil K Jain (1996) A Real-Time matching system for large fingerprint databases. IEEE Trans Pattern Anal Mach Intell 18: 8.
5. Joon-Seok Kim, Seung-Jin Sul (2003) An Efficient Fingerprint Recognition Algorithm for ARM7 CPU. Proceedings of 2003 Spring Conference on Information Processing, Korea Information Processing Society.
6. Jain AK, Prabhakar S, Hong L (1999) A multichannel approach to fingerprint classification. IEEE Trans. PAMI 21: 348-359.
7. Karu K, Jain AK (1996) Fingerprint classification. Pattern Recognition 29:389-404.
8. Cappelli R, Lumini A, Maio D, Maltoni D (1999) Fingerprint classification by directional image partitioning. IEEE Trans Pattern Anal Mach Intell 21: 402-421.