New Developments in Automatic Identification

MARIA VLAD, ALEXANDRA ANISIE, MADALIN STEFAN VLAD
Faculty of Automatic Control and Computers,
"Politehnica" University of Bucharest,
313, Spaiul Independentei, Sector 6, Bucharest,
ROMANIA
E-mail: maria@ac.pub.ro, alex4ndco@gmail.com, madalinv@ac.pub.ro

Abstract: Nowadays security is the top most priority in every field: personal protection, data and asset protection, including building security. Biometric recognition refers to the use of distinctive physiological and behavioral characteristics for automatically recognizing an individual. Fingerprint recognition has been nominated as the lead biometric identifier used by most modern security systems. Fingerprint technology has matured over the past 60 years and new methods are constantly being developed.

Keywords: automatic identification, fingerprint recognition, access control system

1. Why Fingerprints?

With increasingly urgent need for reliable security, biometrics is being spotlighted as the authentication method for the next generation. Among numerous biometric technologies, fingerprint authentication has been in use for the longest time and bears more advantages than other biometric technologies do.

Fingerprint authentication is possibly the most sophisticated method of all biometric technologies and has been thoroughly verified through various applications. Fingerprint authentication has particularly proved its high efficiency and further enhanced the technology in criminal investigation for more than a century.

Even features such as a person's gait, face, or signature may change with passage of time and may be fabricated or imitated. However, a fingerprint is completely unique to an individual and stayed unchanged for lifetime. This exclusivity demonstrates that fingerprint authentication is far more accurate and efficient than any other methods of authentication.

Also, a fingerprint may be taken and digitalized by relatively compact and cheap devices and takes only a small capacity to store a large database of information. With these strengths, fingerprint authentication has long been a major part of the security market and continues to be more competitive than others in today's world.

Fingerprints are now being used as a secure and effective authentication method in numerous fields, including financial, medical, e-commerce and entrance control applications. Modern applications of fingerprint technology rely in large part on the development of exceptionally compact fingerprint sensors.

2. Fingerprint Identification Process

Fingerprint identification process consists of two essential procedures: enrollment and authentication. Taking the steps shown in figure 1 completes each procedure.

As shown in the diagram, fingerprint identification system compares the input fingerprint image and previously registered data to determine the genuineness of a fingerprint. All the steps described above affect the efficiency of the entire system, but the computational load of the following steps can be reduced to a great extent by acquiring a good-quality fingerprint image in the first step.

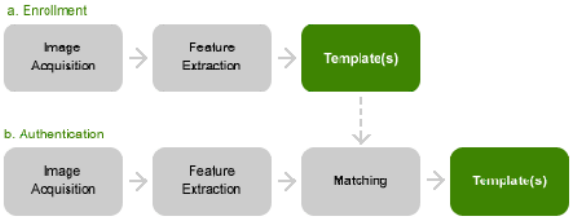

Fig 1. Fingerprint Identification Process

2.1 Image Acquisition

Real-time image acquisition method is roughly classified into optical and non-optical. Optical method relies on the total reflection phenomenon on the surface of glass or reinforced plastic where the fingertip is in contact. The sensor normally consists of an optical lens and a CCD module or CMOS

ISBN: 978-1-61804-044-2

image sensor. In contrast, semiconductor sensors, as a typical example of non-optical sensors, exploit electrical characteristics of a fingertip such as capacitance.

Ultrasonic wave, heat, and pressure are also utilized to obtain images with the non-optical fingerprint sensors. Non-optical sensors are said to be relatively more suitable for massive production and size reduction such as in the integration with mobile devices. Detailed comparison is found in Table 1.

	Optical	Non-optical
Measuring Method	light	pressure, heat, capacitance, ultrasonic wave
Strength	highly-stable performance physical/electrical durability high-quality image	low cost with mass production compact size integrated with low-power application
Weakness	relatively high cost limit to size-reduction relatively easy to fool with a finger trace or fake finger	physical/electrical weakness performance sensitive to the outer environment(temperature, dryness of a finger)
Application	entrance, time, and attendance control banking service PC security	PC security e-commerce authentication mobile devices & smart cards

Tab 1. Sensor comparison

2.2 Feature Extraction

There are two main ways to compare an input fingerprint image and registered fingerprint data. One is to compare an image with another image directly. The other is to compare the so-called 'features' extracted from each fingerprint image. The latter is called feature-based/minutia-based matching. Every finger has a unique pattern formed by a flow of embossed lines called “ridges” and hollow regions between them called “valleys.” As seen in the figure 2, ridges are represented as dark lines, while valleys are bright.

Fig 2. Minutiae of Fingerprints – Ending and Bifurcation

2.3 Matching

The matching step is classified into 1:1 and 1:N matching according to its purpose and/or the number of reference templates. 1:1 matching is also called personal identification or verification. It is a procedure in which a user claims his/her identity by means of an ID and proves it with a fingerprint. The comparison occurs only once between the input fingerprint image and the selected one from the database following the claim by the user.

On the contrary, 1:N matching denotes a procedure where the system determines the user's identity by comparing the input fingerprint with the information in the database without asking for the user's claim. A good example of this is AFIS(Automated Fingerprint Identification System) frequently used in criminal investigation.

The output result of the matching step is whether or not the input fingerprint is identical to the one being compared in the database. Then how could the accuracy of the matching procedure be represented in number? The simplest measures are FRR(False Reject Rate) and FAR(False Accept Rate). The former is the rate of genuine user's rejection and the latter is the rate of impostor's acceptance.

3. Fingerprint Technologies

Aside from the demonstrated technologies, new ones are coming into focus, some of which are really promising.

3.1 Touchless 3D Fingerprinting

Even though fingerprint technology has been introduced over 60 years ago, fingerprinting has always been two dimensional. Despite the iconic TV imagery of ink and rolling fingers, most modern fingerprinting is done with digital scanners. Fingers are pressed against a plate of glass and the print is recorded. The image taken is two dimensional, distorted by pressure, and can be confused by sweat and oil left on the glass. It typically takes several minutes to process all ten fingers.

ISBN: 978-1-61804-044-2

The US department of Homeland Security and the National Institute of Justice are hoping to change that. They've given grants to dozens of companies to perfect touchless 3D fingerprinting. Two universities (University of Kentucky and Carnegie Mellon) and their two respective start up companies (Flashscan 3D and TBS Holdings) have succeeded. Fingerprints have reached the third dimension and they are faster, more accurate, and touchless.

The 3D fingerprinting from the University of Kentucky and Flashscan 3D, however, takes just 1 second per finger. Because there is no contact between the scanner and the finger, there is no danger of distortion or interference from oils and sweat. The scanner shines a series of striped lines of light on the finger (called structured light illumination, SLI) to highlight the depth of the contours of the print and obtain a 3D image. SLI, coupled with a 1.4 megapixel camera, gives the Flashcan system a resolution of about 1000 pixels per square inch. That's twice the requirement for AFIS. To integrate with that database, Flashscan has special software to flatten the 3D print into 2D without cracks or stretches. The project intents to get the scan time down to 0.1 second and to be able to scan all ten fingers at once. Flashscan 3D doesn't have a fieldable product yet, but was able to use its prototype to compare its 3D fingerprinting to traditional 2D scanners. On a scale of 1 to 5 (with 1 being best) the Flashscan scored 1.1519, beating a traditional device at 1.7125.

The competition comes from Carnegie Mellon and TBS Holdings. TBS already has both a single and 10-finger scanner (actually, it does 4 fingers at a time, and then both thumbs) and has slated serial production of their devices for 2010. The accuracy, speed, and flattening software (3D to 2D) for both companies are similar.

Fig 3. Flashscan's fingerprinting uses stripes of light to capture a 3D image with no touching

3.2 Photogrammetric fingerprint unwrapping

Joanneum Research, the Institute of Digital Image Processing, has developed a photogrammetric workflow for nail-to-nail fingerprint reconstruction: A calibrated sensor setup with typically 5 cameras and dedicated illumination acquires adjacent stereo pairs. Using the silhouettes of the segmented finger a raw cylindrical model is generated. After preprocessing (shading correction, dust removal, lens distortion correction), each individual camera texture is projected onto the model. Image-to-image matching on these pseudo ortho images and dense 3D reconstruction obtains a textured cylindrical digital surface model with radial distances around the major axis and a grid size in the range of 25–50 μm.

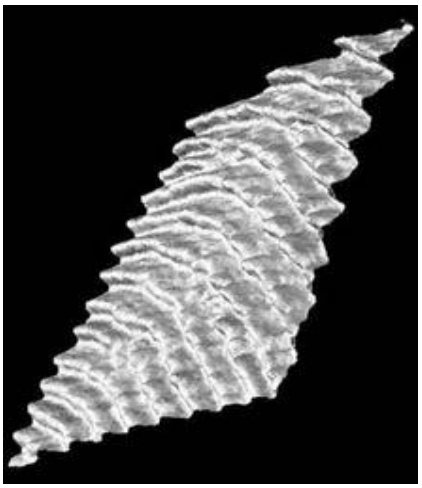

Fig 4. Flashscan's technology produces a 3D map of the fingerprint like this one

The model allows for objective fingerprint unwrapping and novel fingerprint matching algorithms since 3D relations between fingerprint features are available as additional cues. Moreover, covering the entire region with relevant fingerprint texture is particularly important for establishing a comprehensive forensic database.

3.3 Finger "on the fly"

Sagem Sécurité (Safran group) made headlines at Biometrics 2009, the leading European trade show and exhibition dedicated to biometrics, by unveiling its new "Finger on the Fly" technology that reads fingerprints on a moving hand - "on the fly". For the first time, a contactless biometric recognition technology can capture and process the fingerprints from four fingers on a hand in movement, in just a few seconds.

Well suited to current requirements, this technology enhances security and speeds up flows in crowded areas, such as airports. It can also be used as the basis for a more user friendly

ISBN: 978-1-61804-044-2

identification system, involving fewer restrictions for users.

3.4 Methods of identifying warped fingerprints

Many other fingerprint techniques have tried to identify a few key features on a finger print and laboriously match them against a database of templates. The University of Warwick researchers consider the entire detailed pattern of each print and transform the topological pattern into a standard co-ordinate system. This allows the researchers to "unwarp" any finger print that has been distorted by smudging, uneven pressure, or other distortion and create a clear digital representation of the fingerprint that can then be mapped on to an "image space" of all other finger prints held on a database. Instead of laboriously comparing a print against each entry in a database any new print scanned by the system is unwarped and over laid onto a virtual "image space" that includes all the fingerprints available to the database. It does not matter whether it's a thousand or a million fingerprints in the database the result comes back in seconds.

This unwarping is so effective that it also allows comparison of the position of individual sweat pores on finger print. This has not previously been possible as the hundreds of pores on an individual finger are so densely packed that the slightest distortion prevented analysts from using them to differentiate fingerprints.

4. Fingerprint Applications

Markets for fingerprint technology include entrance control and door-lock applications, fingerprint identification mouses, fingerprint mobile phones, and many others. The fingerprint markets are classified as show in figure 5.

As the advanced technology enables even more compact fingerprint sensor size, the range of application is extended to the mobile market. Considering the growing phase of the present mobile market, its potential is the greatest of all application markets.

4.1 Access Control System Using Fingerprint Recognition

In today's environment, it's more important than ever to deploy a building access system with state-of-the-art security features. The presented access control system has been implemented through the use of the above mentioned biometric identifier, shaping both an efficient as well as a low-cost security system based on fingerprint recognition.

Fig 5. Market of Fingerprint Technology

The following system is based on a classic fingerprint recognition method, making use of a biometric scanner provided by Bergdata Biometrics. The scanner, Bergdata FingerChip USB scanner BDB-100, is an optical one, that comes with a library defining a series of functions to analyze 8-bit grayscale fingerprint images, extract a unique data set (denoted as fingerprint code or fp-code) which represents the fingerprint in a not reconstructable way, create a particular fp-code (denoted as template) from a set of fp-codes representing the same finger, match a single fp-code with one or more templates.

Fig 6. Bergdata Biometric Scanner

The scanner should only be active for as long as a scan is required. The solution was the use of a button that activates the scanner upon request. The button is connected to the computer through an ATMega8 Atmel microcontroller that was programmed to implement an USB functionality allowing it to connect to the computer using USB rather than through an RS232 port. The microcontroller can also control an electromagnetic lock that opens upon positive identification from the computer, stays open for a few seconds and locks itself again.

ISBN: 978-1-61804-044-2

The application, developed using C#, uses a database that holds the fingerprint templates of the enrolled users. Enrollment can also be done through the use of this software. In order to create a template for a finger five scans are required to obtain a best quality template. Once a template was created, it is stored in the database and will be matched against any fingerprint that requires an identification.

The software allows for both identification and verification, the first one searching for a match through the whole template database, while the second checks for a positive match again a selected template.

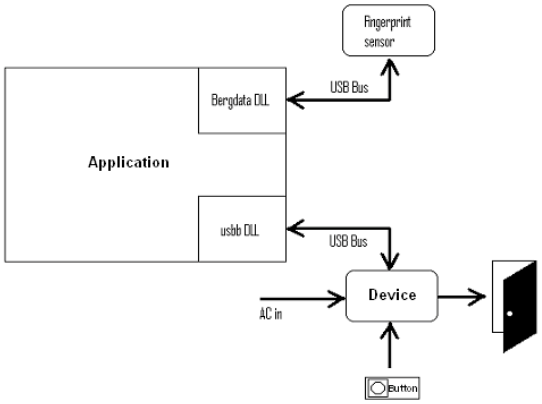

Fig 7. System Architecture

Extra features have been added to the system. It can now hold a log that can easily be transformed into a means of clocking the employees of the company and can also be used to keep track of the persons entering a restricted area.

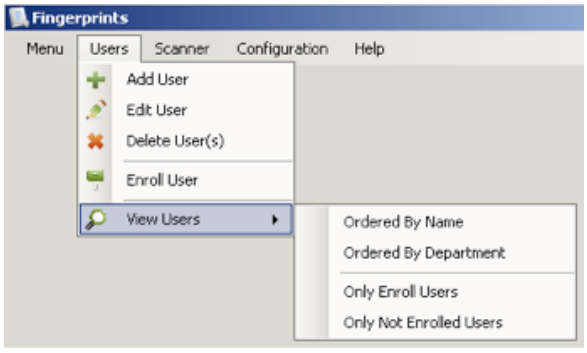

Fig 8. Fingerprints Application (1)

A speech synthesizer was also implemented in the system, one that can be activated or deactivated by the system administrator. If active, the system can greet a identified user with a standard “Hello username” message or can verbally announce whether or not there was a positive identification.

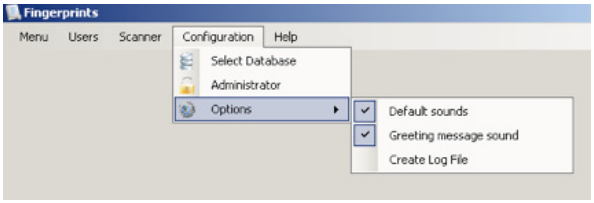

Fig 9. Fingerprints Application (2)

5. Conclusion

Fingerprint is the cheapest, fastest, most convenient and most reliable way to identify someone. That's why fingerprint alone has 2/3 of the biometric world market (according to an International Biometric Group independent report). 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.

Even identical twins have different fingerprints. Fingerprints have been used in identification for thousands of years and even today, with huge databases with millions of fingerprints, it hasn't been found one that is identical to another. Besides, each finger and toe has a completely different fingerprint from each other.

Any biometric method may present some rejection problem, because they involve human and biological characteristics. That means that even a person whose fingerprint is already recorded may not be recognized. This is called "false rejection" and happens with any technology and manufacturer. This problem rarely occurs (below 0.1% of the cases), but it is important to keep this possibility in mind during the implementation, so you can plan on what to do if that happens. The individuals that present this kind of situation are the elderly and children up to 6 years old. Some chemical products may also provoke the temporary reduction of a fingerprint quality. In addition, some people don't have fingerprints on some periods of the year, due to biological conditions associated to weather or to their own organism. In these cases alternative methods must be used, such as use of documents, passwords or access cards.

Although this is a standard security system, it does have a series of advantages over all other types of access control systems. Fingerprints are unique so that any person can be irrevocably identified based on fingerprint recognition. A password can be forgotten or passed to another person and a token can be lost or borrowed, while a fingerprint, being a biometrical identifier can not be lost, forgotten or borrowed, ensuring an exact identification.

ISBN: 978-1-61804-044-2

If any of the previous methods of fingerprint recognition would be used instead of the classic one, many more advantages would be ensured: enrollment could take one second at most instead of five consecutive scans of the same finger, a more accurate identification could be made, with a smaller error rate and a far better image quality could be achieved.

At present, there are no guidelines for using biometric hardware and software that could lead to improved usability and interaction techniques. However, new technologies are being developed everyday and there won't be long until all of those technologies will merge together for a new and improved fingerprint recognition system.

References:

[1] Cadmium Advanced Technologies, Inc. (2009) Biometrics Security News and Information, *Available from:* http://biometricsnew.net *Accessed:* 2009-10-15

[2] Griaule Biometrics (2009) Articles, *Available from:* http://griaulebiometrics.com/page/en-us/article/10 *Accessed:* 2009-10-15

[3] Maltoni, D.; Maio, D.; Jain, K. A. & Prabhakar, S. (2005). *Handbook of Fingerprint Recognition,* Springer, ISBN 0-7923-7856-3, United States of America

[4] Ratha, N. & Bolle, R. (2005). *Automatic Fingerprint Recognition Systems,* Springer, ISBN 0-387-95593-3, New York

[5] Zhang, D. D. (2000). *Automated Biometrics: Technologies and Systems,* Kluwer Academic Publishers, ISBN 0-387-95431-7, United States of America