Automatic identification technologies

Maria VLAD, Alexandra ANISIE and Madalin Stefan VLAD

***Abstract*—**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. In this paper there are proposed two systems based on biometric identification, in conjuction with smart card, for proof of advanced security offered by the systems. There are presented also background of fingerprint recognition, along with data storage on smart cards and RFIDs.

***Keywords*—** biometry, identification, identity, RFID.

I. Introduction

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.

II. Automated Information Systems

The use of biometrics and/or smartcards must work in tandem with some form of Automated Information System (AIS) to meet a minimum level of assurance. Whether it is a workstation on a desk or an embedded system within a vending machine, strong user authentication is based on proper integration of the separate components. Use of these systems requires that it is trusted to perform the operations desired and only those specific operations. An example would be that a vending machine is expected to only debit a stored value application within a smartcard and not attempt to digitally sign legal documents. "Trust" in an AIS is earned when the AIS's functionality is perceived to be correct with respect to an established security policy. Use of a robust multi-application smartcard with the appropriate security features can help mitigate risk when utilizing an AIS of questionable origin.

There are several ways to establish different levels of trust in an AIS. One method is to use a Trusted Operating System (TOS). A TOS has been verified to perform correctly and if a failure occurs, it will fail safely, so that no restricted information is compromised. Verification methods of this trust include testing and formal mathematical analysis. Other less stringent methods to gain trust in a system can include physical isolation (no network or dial-up connections), purchasing products through trusted vendors, and of course physical security to prevent tampering.

The level of trust in an AIS required for a specific application is dependent on the value of the information at risk. An AIS restricting access to a classified room should not be connected to the Internet. Ensure that the platform used for your application really is "trustworthy".

III. Fingerprint Identification Process

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

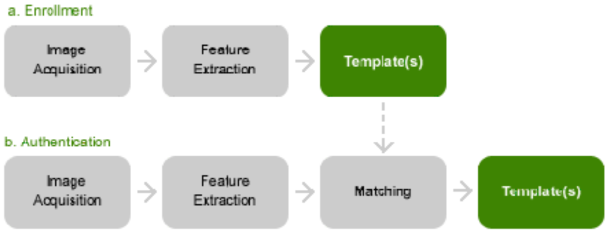


Fig 1. Fingerprint Identification Process

Manuscript received November 28, 2011: Revised version received March 4, 2008.

This work was supported in part by the Romanian National Autority for Scientific Research, Grant no PD 196/2010

Maria VLAD is with the University POLITEHNICA of Bucharest, Splaiul Independentei 313, Bucharest, Romania, phone: +40 214029310; e-mail: maria@ac.pub.ro.

Alexandra ANISIE is with the University POLITEHNICA of Bucharest, Splaiul Independentei 313, Bucharest, Romania, e-mail: alexandra@ac.pub.ro.

Madalin Stefan Vlad is with the University POLITEHNICA of Bucharest, Splaiul Independentei 313, Bucharest, Romania, e-mail: madalinv@ac.pub.ro.

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.

A. *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 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

B. *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.

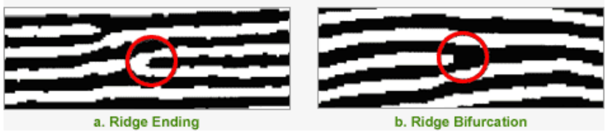


Fig 2. Minutiae of Fingerprints – Ending and Bifurcation

C. *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.

The algorithm used in minutiae comparison requires a specific mode of storing features, using polar coordinates, which also brings the advantage of reducing the memory space needed. The parameters are:

- *x and y coordinate* of the minutia point
- *orientation*, defined as the local ridge orientation of the associated ridge.
- *type of the minutia point*, which is whether the minutia is ridge ending or ridge bifurcation.
- *associated ridge*.

IV. Fingerprint Technologies

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

A. *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.

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.

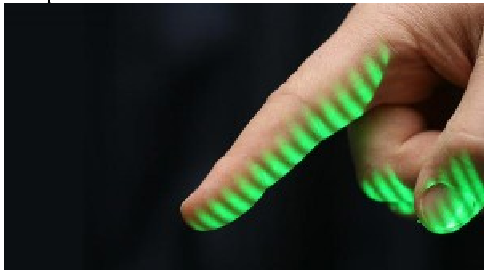


Fig 3. Flashscan's fingerprinting uses stripes of light to capture a 3D image with no touching

B. 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.

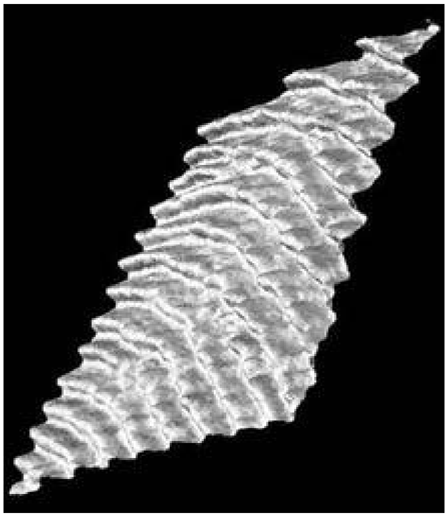


Fig 4. Flashscan's technology produces a 3D map of the fingerprint like this one

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.

C. 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 identification system, involving fewer restrictions for users.

D. 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.

V. 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.

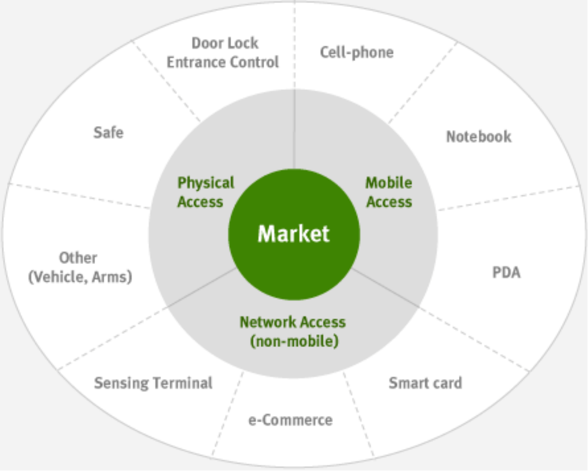


Fig 5. Market of Fingerprint Technology

The risks of frauding the an automated system based on biometrics and smart cards are imminent, and they appear mostly due to smart card. But the application or the data on the smart card have the same risk of being copied or altered as the other application stored there.

The specific sensitive data placed on the smart card will consist of:

- Private signature key of the user.
- Private key exchange key of the user
- The authentication certificate
- Other sensitive information such as account balances, security codes, etc.

The data on the smart card can be lost in the following ways:

- Physical attack on the smartcard
- Incorrect implementation of an algorithm
- Back doors and implementation flaws due to poorly designed/test implementation of the smartcard.
- Placing a “Trojan Horse” application in the host PC to capture I/O information
- Tapping the line between the host and the smartcard
- Providing a bogus host to capture the information from the smartcard

To break a smart card it is a must to break the private key. Most smartcards do not allow private keys to be obtained directly from the interface. The most likely way of obtaining the private key is via a physical attack.

VI. Structure Of The Application For Access Control

We propose an integrated system for automatic identification and also for access control, using smart card and fingerprint features. The goal of the application is to do both a biometric verification and identification, with the personal data stored on the smart card.

The problem of personal identification in the Digital Era has many aspects and many developments. Most of them are based on secure authentication, authentication over secure channels, and the physical ways of implementing these concepts are web servers, smart cards, and biometrics and so on.

The main concepts involving digital identification are based on several principles, such as:

- who you are,
- what you have,
- what you know.

Smartcards and biometrics by themselves each provide a considerable boost to the Identification and Authentication (I&A) mechanism of any system. Together, they can provide a comprehensive solution of the three principles described above A common understanding of the underlying technologies is required to fully grasp how each component contributes toward a comprehensive I&A solution.

Contact cards contain physical contact points on the surface of the card that allow transmission of commands, data and status information between the card and the reader. A contact card requires insertion into a smart card reader with a direct connection to a conductive micro-module on the surface of the card (typically gold plated). It is via these physical eight contact points that transmission of commands, data and card status takes place; their functional assignments are shown in figure 6:

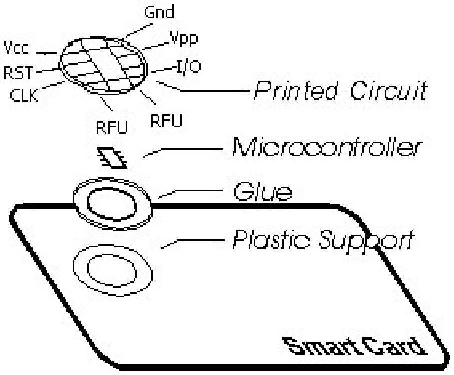


Fig. 6. Contact smart card

- The Vcc point supplies power to the chip. Vcc voltage is 3 or 5 volts, with a maximum deviation of 10 percent.
- The RST point is used for sending the signal to reset the microprocessor-this is called *warm reset*. A *cold reset* is done by switching the power supply voltage off and on again.
- Smart card processors do not possess internal clock generation. The CLK point supplies the external clock signal from which the internal clock is derived (usually 3.5795 MHz or 4.9152 MHz) and is also used as the reference for the serial communication link.
- The GND point is used as a reference voltage; its value is considered to be zero volts.
- The Vpp point is optional and is used in older cards. When used, it supplies the programming voltage with two levels. The voltage change is necessary to program EEPROM memory in some old smart card chips.
- The I/O point is used to transfer data and commands between the smart card and the outside world in half-duplex mode.
- The RFU points are reserved for future use

The advantages of using a biometric for identification are obvious. Each of us has forgotten our password and, in an effort not to forget it the next time, written it down, or chosen one that was easy to remember. In essence we have undermined security for the sake of convenience. The use of biometrics changes all of this. Instead of using what we know to prove who we are, we use some unique feature of ourselves such as a fingerprint, handprint or the sound of our voice. A world that replaces a memory test with a fingerprint scanner is quiet attractive, and there are numerous devices available today that provide secure access based solely on a biometric.

In this way, the first important step is considered to be the enrollment. Therefore, a new user, who will be involved in the system, comes to an authority and gets his finger scanned for several times (usually 3-5 times), in order to get the best fingerprint. From the images captured by the biometric sensor, the features are extracted, and the best feature string, with maximum number of minutiae will be stored on the smart card.

The algorithm of extracting minutia for enrollment phase is similar with the one used either in verification or in identification. Sending and storing the minutiae string on the smart card are done in a secure way, with several mechanism of authentication, in order for the personal data to be perfectly protected.

After the enrollment has been successfully done, the used has the ability of using the system for further verification, such as access control or personal identification.

The use of the system permits, as mentioned above, two actions to be undertaken: identification and verification. Depending on the specific type of comparison, there are several modules in the application that interact with each other, as in fig 7.

In development framework, two subsystems were considered:

- on-card application, which stores the minutiae string, and have several methods for restricting access to them
- off-card application, the client part of the system, responsible for several activities, such as:
    - establish secure connection and communication with the smart card
    - establish secure connection and communication with the database
    - reading information from the biometric sensor
    - comparing the minutiae string

The application runs on an experimental embedded system, formed by specific components:

- Computer: Pentium III, 1,2 GHz, 384 Mb RAM
- Biometric sensor: Bergdata
- Smart card reader: Gemplus GCR 410, Serial Connection
- Smart cards Gemplus GemXpresso PK 211, with 16 KB RAM

Bergdata sensor have some special characteristics, which made it very sutable for development such kind of application. We monetion some of them:

- High image quality
- Fingerprint image size 320x440 pixel
- Resolution 500 dpi (FBI standard)
- Atmel FingerChip(TM) sensor
- Self cleaning sensing area
- User friendly finger guide for sweep sensor
- Metal back plate for stable stand on desktop
- Temperature range +5 ... +45 °C
- ESD resistance > 16 kV

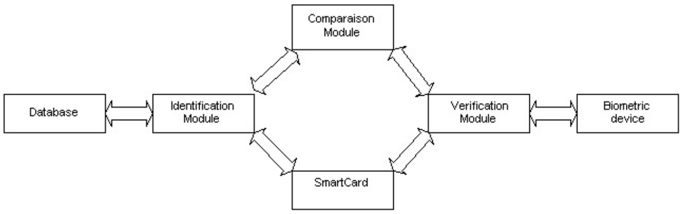


Fig 7. The modules of the integrated system

VII. Client Application

As mentioned above, from user point of view, the client performs two actions: verification and identification.

For experimental reasons, there is only a single application, which can perform the two types of identification. From the menu it can be chosen what kind of action it will do.

A. Verification System

Verification is used mainly for access control into specific location. The system, through the both subsystems – the biometric sensor and the smart card reader, waits for an external event. When one is produced, the user is prompted for the complementary action. After the two conditions were satisfied, the computer side applications starts to extract the minutiae from the image acquired through the sensor. This step is performed using the VeriFinger methods. The steps of the application can be seen in fig. 8.

Upon extraction of the fingerprint features, the minutia string stored on the smart card is read. Then, the two strings are compared, and if a percent of matching is met, the access is granted, otherwise is denied. The percent of matching, called threshold can be established within the program, depending on the FAR/FRR rate required at the specific location where access control takes place.

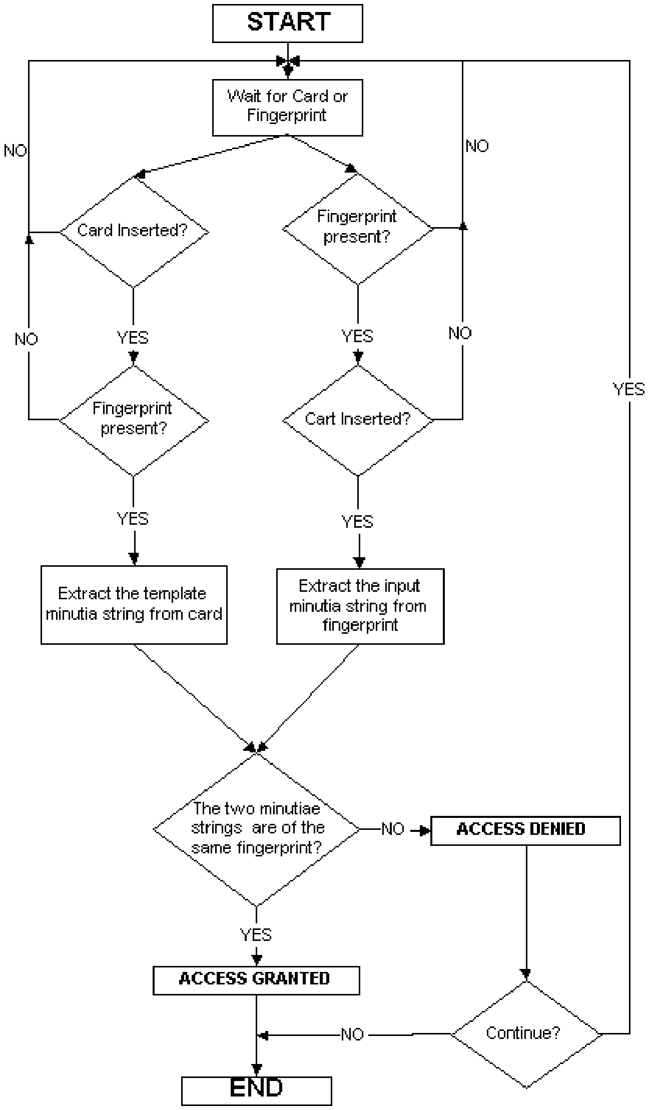

START
Wait for Card or Fingerprint
NO
NO
Card Inserted?
Fingerprint present?
NO
YES
YES
NO
YES
Fingerprint present?
Cart Inserted?
YES
YES
Extract the template minutia string from card
Extract the input minutia string from fingerprint
The two minutiae strings are of the same fingerprint?
NO
ACCESS DENIED
YES
ACCESS GRANTED
NO
Continue?
END

Fig 8. Steps of identifcation system

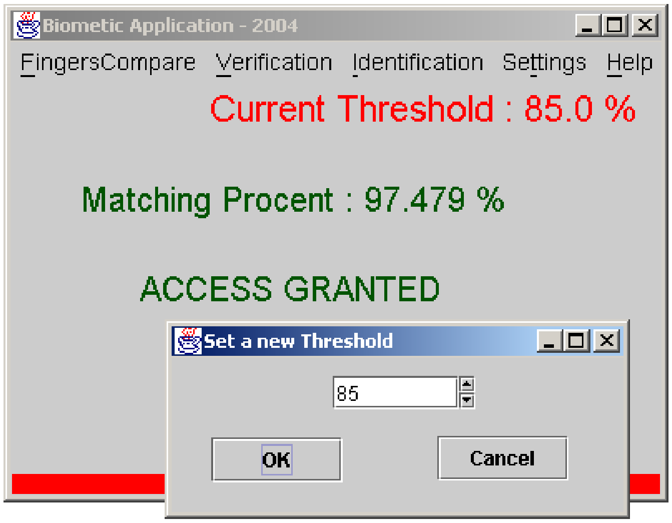
If we want to use the system for a security objective, the typical threshold is 85%, which is the usual in biometric identification system. For improvement of security, a higher threshold can be set, which means that more minutiae must be extracted from the image acquired from the biometric sensor, when a user wants to authenticate. That procedure usually involves many retry of user fingerprint read, because the image is altered by external factors, such as dust, wet, or degrading of the fingerprint, due to a hard work.

A. *Identification*

The identification part of the application performs several steps, in order to find an owner of a card in the database. First of all a verification is done, in order for the user to be authenticated towards his card.

Application is connected to a database, where personal detail of a user are stored. The details include fields like: Name, Address, etc, and also a picture of the user. Upon successful completeness of the user fingerprint verification towards his/her smart card, the channel to the smart card is closed. The minutia sting took from the smart card is already stored in a variable inside the program. This string is searched in a database, and if it found, a window with his/her personal data is shown.

In this way, a external entity can verify easily if a person is who he pretends to be, because the first can see the details of the person and can compare the picture of the user with the "live" one.



Current Threshold : 85.0 %

Matching Procent : 97.479 %

ACCESS GRANTED

85

Fig. 9. The main window of the application. We can see the current threshold rate, the matching percent of the verification and the grant or denial of the access

VIII. 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.

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 10. 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.

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.

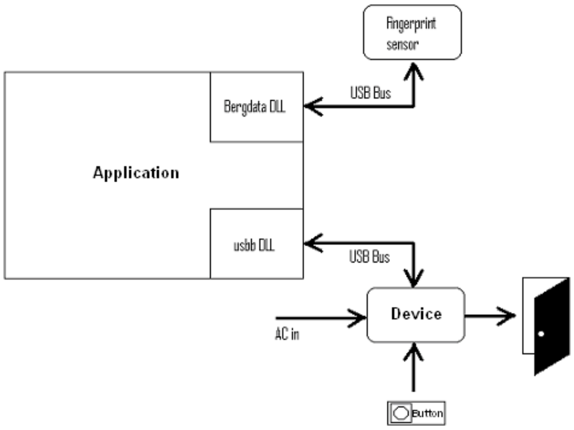


Fig 11. System Architecture

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.

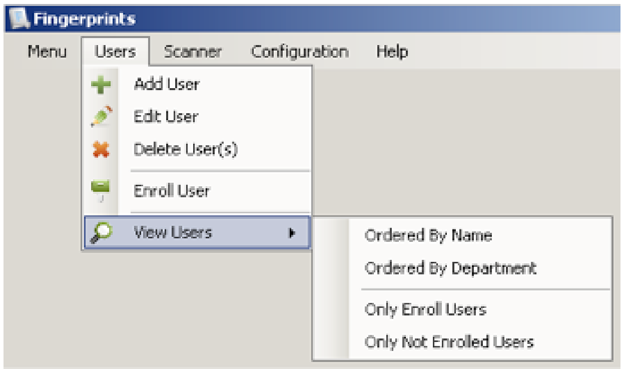


Fig 12. Fingerprints Application (1)

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.

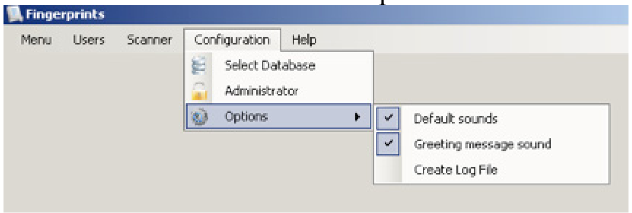


Fig 13. Fingerprints Application (2)

IX. 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.

Biometric identification is preferred over the traditional methods because the person to be identified is required to be physically present at the point of identification and also identification based on biometric techniques obviates the need to remember a password. Along with a smart card, there can be designed access control systems which can have a higher immunity to frauders.

In embedded systems, based on biometrics and smart cards, the personal features can be used in authentication to the smart card. In this way, better security to smart card stored data is provided, compared with the current security, provided by a PIN number, who can be easily subtracted

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.

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

[6] Zanero, S. Smart Card Content Security, 2002

[7] Pankanti, S., Prabhakar, S., and Jain, A. On the individuality of fingerprints. IEEE Transactions on PAMI 24, 2002

[8] Hendry, M. Smart Card Security and Applications, Second Edition, Artech House, 2001

[9] Davida, G., Frankel, Y., and Matt, B. On enabling secure applications through off-line biometric identification, IEEE Symposium on Privacy and Security, 1998.

[10] GSA Government Group, Guideline for placing biometrics in smart cards, 1998

[11] Zhang, W., Wang, S. and Wang, Y. Structure matching algorithm of fingerprint minutiae-based on core point, 2003

[12] Jain, A., Hong, L. and Boole R. On-Line fingerprint verification, IEEE Trans. PAMI, Vol. 19, No. 4, 1997

[13] Zhang, W. and Wang, Y. Core-Based Structure Matching Algorithm of Fingerprint Verification, Proceeding of International Conference on Pattern Recognition, Vol.1, Quebec City, Canada, IEEE Press, 2002

[14] Wang, Y., and Zhang, W. Topology based Fingerprint Minutiae Matching Algorithm, Chinese Patent apply No. 02116254.9, 2002

.