Applications Designed to Promote a New Way to Ensure Home Security

Mustahid Hossain
Department of Information Systems
The University of Maine
Orono, Maine, USA

Abstract

Fingerprint-based applications hold a promising future in terms of resolving numerous security hazards. In order to offer efficient security systems for the households, we investigate prototypes, technologies, and frameworks that will transcend the current state of practice in household security application systems. In this paper, we first discuss the current practices and trends in the regular door locks. Then, we investigate a number of research issues and future directions in fingerprint-based development for door locks.

Keywords: biometrics, fingerprint-based technology, door lock security, database

1. INTRODUCTION

In the modern society, there is an ever-growing need to positively determine or verify the identity of a person. Where authorization is necessary for an action, be it picking up a child from daycare, or boarding an aircraft, this authorization is usually vested in a single individual or a class of individuals (Immigration and Naturalization Service). There exist a number of methods of verifying identity that have been adopted by society or automated systems. These are summarized in table 1. The existing methods can be grouped into three classes: (i) possessions (what you have); (ii) knowledge (what you know); and (iii) biometrics (unique personal traits).

Method	Example	Comments
What you know	User id, password, pin	Can be forgotten Easily shared Many passwords are easy to guess
What you have	Cards, badges, keys	Can be lost or stolen Easily shared Can be duplicated
What you know and what you have	ATM + PIN	PIN is a weak link Writing PIN on Card Easily shared
What you are	Fingerprint, face, …	Non-repudiable authentication

Table-1 A Categorization of Identification Technologies

Biometrics is the science of identifying or verifying the identity of a person based on physiological or behavioral characteristics. Physiological characteristics include fingerprints and facial appearance. Behavioral characteristics are actions carried out by a person in a unique way. They include signatures and voiceprints though these are naturally dependent on physical characteristics as well. It is important that behavioral characteristics must be insensitive to variations due to the state of the health, mood of the user, or the passage of time. Similarly, the measured physiological characteristics should remain constant overtime (Nalini Ratha, et al).

Often, the three identification methods in Table-1 are used in combination. The possession of a key is physical conveyor of authorization; a password plus a user ID is a purely knowledge based method of identification; an ATM card is a possession that requires knowledge (PIN) to carry out a transaction; a passport is a possession that requires a biometric verification (passport photo).

Early-automated authorization and authentication methods relied only on possessions and knowledge. There are several well-known issues associated with these methods that restrict their use and the extent to which they are trustworthy. The problem is that these methods verify attributes that only indirectly indicate the presence or absence of a given person. Most importantly, the problems are (i) possessions can be lost, forged, or even duplicated; (ii) knowledge can be forgotten; (iii) both knowledge and possession can be lost or stolen. Consequently; repudiation is easy. That is, it is easy to deny that a given person carried out an action because only the possession or knowledge is checked and these are loosely coupled to the person's identity. Clearly, this is unacceptable in applications of high security physical access control, bank account access, etc.

The science of biometrics provides an elegant solution to these problems by positively verifying the identity of the individual. For contemporary applications, biometric authentication is automated to eliminate the need for human verification, and a number of new biometrics have been developed, taking advantage of increasing understanding of the human body and human actions, and advances in sensing techniques. Newer physiological biometric authentication technologies that have been developed include iris patterns, retinal images, and hand geometry. Newer behavioral biometric technologies (still very much in research stage) are gait and keystone patterns. The first step in an automatic biometrics is an enrollment of the user (like the registration of a password). After this, the user can be a verified many times (CIS).

In this paper, we describe the architecture and application of a biometrics-based secure authentication implementation for door-locks. In particular, we address the issues of a fingerprint-based authentication scheme with the existing door-lock security infrastructure. Contrary to what may be the common belief, one cannot just install any commercially available fingerprint verification system and reflect the security features in the application. We will discuss the subtle issues involved in integration and demonstrate our solutions to various problems.

2. CURRENT TREND

There are numerous types of door-lock devices in operation. We describe a top-notch and latest one in the following. The Door-Lock, from SmartHome, a leading secured door-lock service provider, "is a very flexible and secure digital access system that uses Dallas Semiconductor iButtons to identify people, usually to grant them access to a secure area (i.e., your home). iButtons have unique 64-bit serial numbers and are the size of a large watch battery. This unique 64-bit serial number is used to grant or deny access to someone. iButtons can be attached to key chains, wallets, watch bands, and even rings making it very easy to store and carry them with you. iButtons are accessed via a small probe contact the size of a dime. You simply press the iButton onto

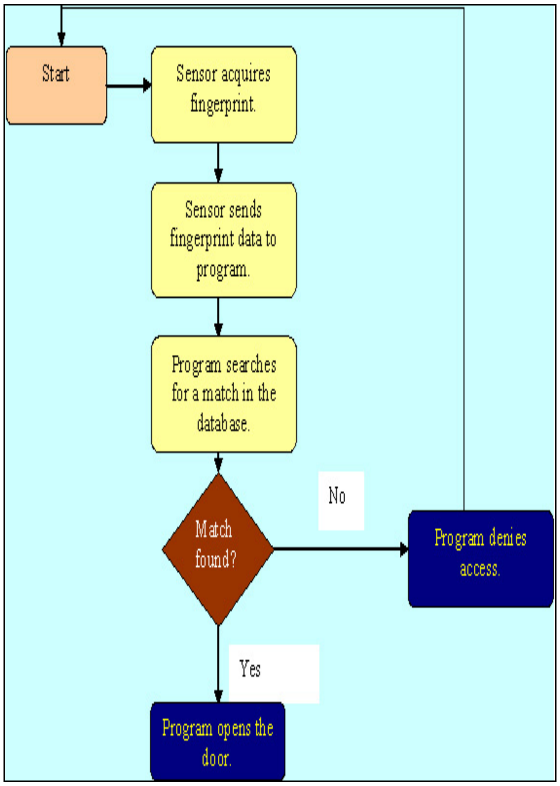
Start
Sensor acquires fingerprint.
Sensor sends fingerprint data to program.
Program searches for a match in the database.
Match found?
No
Program denies access.
Yes
Program opens the door.

Diagram-1: Proposed System Flowchart

the probe and it is instantly read. A multi-color LED shows if access is granted or denied. The DoorLock's relay output can be used to activate electric door strikes or they can inform a Home Automation System to open the door and even log the specific person who opened it (Home Automation Products).

3. COMMENT ON EXISTING SERVICES

We agree to the fact that such device offers 24 hour monitoring services, but they have not been proved to be perfect, unfortunately. We also believe that such device can easily be lost or stolen or even shared (CERT® Coordination Center). Since our proposed application overcomes such limitations, we would like to consider it a better application.

4. OUR AUTOMATED DOOR-LOCK DEVICE

In our system, we will have an image database to store user information (biometric images from the household members) and a program to inquire database and control door lock mechanism. Both our database and the program would be coded into a chip which would ultimately reside inside the door lock device. This is how, when a household member uses the image scanner, the program will try to find a match. As the match is found, the program will execute the procedure to open the door lock. However, if there is a mismatch, the access will be denied and the door will remain closed (Diagram 1 and 2).

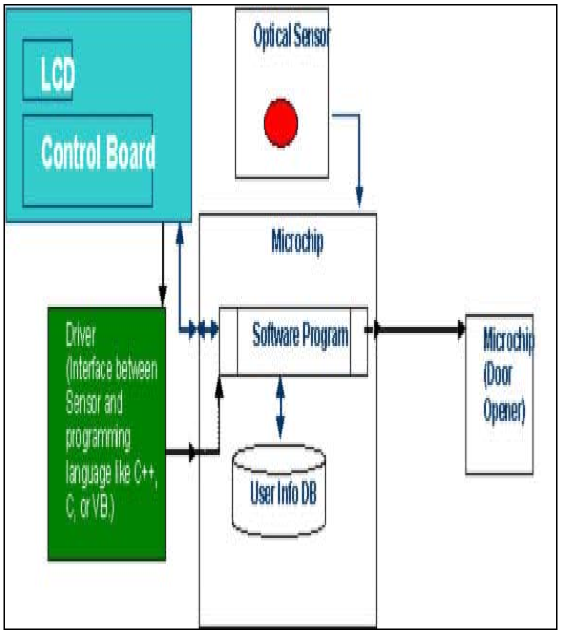

DIAGRAM-2: REGULAR USER INTERFACE

Below, you will find a flowchart that attempts to explain the process of our proposed system.

Things to remember:

1) LCD will just display things like:
   a)"Please place your thumb on the sensor to obtain admission"
   b) If there is a "no match" of the fingerprint, LCD displays the failure message. Successful message if it succeeds.

2) Control Board
   a) Contains buttons like "call administrator", "Help"

- Call Administrator button is used by user when they have trouble getting into the system

- "Help" button upon being pressed displays step-by-step sample procedure of the system Functionality:

As the user puts the finger on the sensor, the image is copied and then translated into a template. The template is in a language that our software cannot understand. So a driver is used that translates the template into a more friendly structure that our software can understand. The converted template is then sent to the microchip, which in turn inquires the database for a match. If there is a no-match, the software sends a message to the control board where a "failure message" is displayed on the LCD. Otherwise, a successful message is displayed (Segee) (Diagrams 2 and 3).

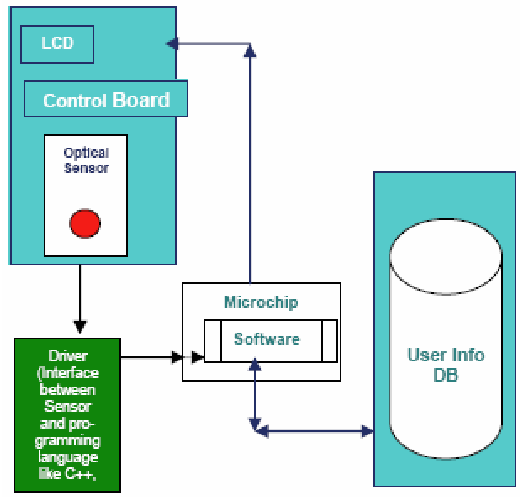
LCD
Control Board
Optical Sensor
Driver (Interface between Sensor and pro-gramming language like C++.
Microchip
Software
User Info DB

DIAGRAM 3: ADMINISTRATIVE INTERFACE

5. SENSOR FUNCTION

The main purpose of the sensor is to sense the ridges on a finger, which are in contact with the surface of the scanner. We assume that our device would overcome the dry and wet skin issues in the optical scanners and can sustain higher static discharge. Once a fingerprint image is acquired by some means, it must be analyzed and invariant properties need to be identified. Such process starts by examining the quality of the input fingerprint impression. After there is a match between the image database, the device would start functioning (Diagram 4).

6. INTEGRATION ISSUES

Several issues need to be addressed while integrating an emerging technology like biometrics into a more established technology like door-locks. The main issues involved in the integration of a fingerprint based authentication method are:

<u>Development issue</u>: commercial, off-the-shelf products are often designed as standalone systems, not including a development toolkit. This makes them difficult to integrate into an existing application like door-locks.

<u>Auto detect and snap</u>: during the input process, the sensor should require very little intervention from the user.

<u>Quality</u>: the system should attempt tot ensure, or at least measure, the quality of the input automatically. Users typically have no feel for the factors that contribute to good or poor signals, and cannot make suitable adjustments on their own.

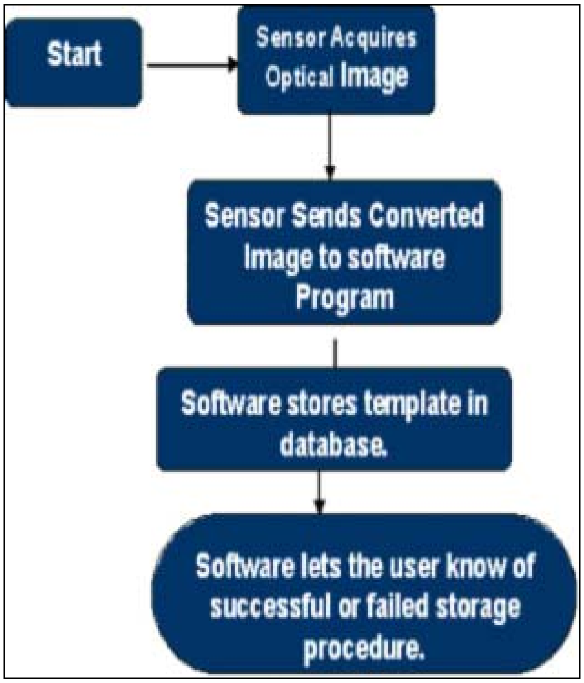
Start
Sensor Acquires Optical Image
Sensor Sends Converted Image to software Program
Software stores template in database.
Software lets the user know of successful or failed storage procedure.

DIAGRAM 4: Sensor Function within the System

<u>Enrollment Issues</u>: any authentication system requires two steps: one time enrollment and multiple authentication. Enrollment is the single most important step that can affect the performance of the system.

Having stated the design issues, we would implement the solution using Visual Basic or C++ programming language.

7. ENCRYPTION

The use of standard encryption enhances the overall security of the system. The templates extracted during enrollment have to be stored in a secure location as they are keys to the secure authentication. They also are encrypted using a standard key-based encryption method. The decryption keys are known only to application which decodes the templates as required during authentication.

8. FINGERPRINT BASED TECHNOLOGY AND PRIVACY

Biometric solutions are getting increasingly popular, as costs have fallen dramatically in the last few years, making them affordable even to small business. Further, new technological innovations have settled the sensitive privacy issue: modern fingerprint systems do not store fingerprint images but create an encrypted mathematical template recording their unique details. It also could be added in this connection that the actual fingerprint image cannot be recreated from this data (biofirst.com).

9. CONCLUDING REMARKS

Existing methods of automated door-lock authentication have a number of limitations, particularly, they can be transferred to one person from another. Automatic biometric door-lock devices can address this problem while also overcoming the other problems like loss and forgery. Such device, by measuring hard-to-forge characteristics inherent to a person provides a reliable, non-duplicable guarantee of identity. This is how, our proposed application ensures maximum security, and that is why we believe such an application would be better than the existing ones.

Recent innovations in algorithms and hardware have meant that the field of biometrics has expanded tremendously, and many applications, not just in security, are being implemented with the use of biometric technology.

Finally, we would like to say that here we have detailed one such application that has commercial potential. We believe that such applications or inherent techniques could also be used in at the immigration port of entries for traveler verification, for quickly obtaining student records on campus or even for ordering meals at a busy restaurant, etc. Educators could play a vital role here in terms of teaching students and people about the fundamentals of database, data security as well as the merits of fingerprint-based technology.

10. REFERENCES

Biofirst.com (2003). "Biometrics, Ideas, and Solutions!" Retrieved on August 22nd, 2003.

Center for Immigration Studies (CIS) (2003). "Immigration: Security and Threat." Retrieved on August 14, 2003.

CERT® Coordination Center: Home Network Security (2003). "Home Network Security." Retrieved on July 28, 2003.

Home Automation Products (2003). "New Ideas!" Retrieved on June 30, 2003.

Immigration and Naturalization Service (2003). "Machine-Readable Passports in Visa Waiver Program." Retrieved on August 5th, 2003.

Nalini Ratha, et al. (1999). "Secure Fingerprint Based User Authentication For Lotus Notes." IBM Research Journal, vol-17, No. 04, pp. 1-11.

Segee, Bruce (no date). Personal communication. Associate Professor, Department of Computer Engineering. The University of Maine.