Cyber Security in Biometrics Using Fingerprints

Priyanka Rattan*
Ritika Kapoor**

Abstract

Nowadays, industries are experiencing technological advancement. With the rise of globalization, it is essential to have an easier and more effective system. Security is a major concern for organizations nowadays as security related risks may affect the organization's information assets badly. One method of ensuring a secure system is the Biometric System. It is a system that uses information about a person that identifies a person. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometrics is an automated method of recognizing a person based on a physiological or behavioral characteristic. Physiological biometrics works by analysing the human body characteristics such as face recognition, fingerprint, face, retina, and iris and behavioral biometrics is based on the person's behavior, e.g. voice recognition. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. This paper covers the use of fingerprints scanning in biometrics. Fingerprint recognition is one of the most well known biometrics, and it is by far the most used biometric solution for authentication on computerized systems. Fingerprints vary from person to person (even identical twins have different prints) and don't change over time. Finger-scan technology is the most widely deployed biometric technology, with a number of different vendors offering a wide range of solutions. Thus biometrics is a means to protect security of data. This paper also covers biometrics recognisation, types of biometrics and application of biometrics. One primary conclusion is that identification should be considered as a component of development policy.

Keywords: Biometrics, Fingerprint, Security, biometric identification

Introduction

There are two types of systems that help establish the identity of a person: verification systems and identification systems. In a verification system, a person desired to be identified submits an identity claim to the system, usually via a magnetic card, login name, smart card, etc., and the system either rejects or accepts on the basis of identity of a person (Am I who I claim I am?). In an identification system, the system establishes a person's identity (or fails if the person is not enrolled in the system database) without the person having to claim an identity (Who am I?). The topic of this paper is a verification system based on fingerprints, and the terms verification, authentication, and identification are used synonymously.

Priyanka Rattan*
Trinity Institute of Professional Studies
Ritika Kapoor**
Trinity Institute of Professional Studies

Among the most remarkable strengths of fingerprint recognition, few are the following:

- Its maturity, providing a high level of recognition accuracy.
- The growing market of low-cost small-size acquisition devices, allowing its use in a broad range of applications, e.g., electronic commerce, physical access, PC logon, etc.
- The use of easy-to-use devices, not requiring complex user-system interaction.

Accurate automatic personal identification is becoming more and more important to the operation of our increasingly electronically interconnected information society. Traditional automatic personal identification technologies to verify the identity of a person, which use"something that you know," such as a personal identification number (PIN), or "something that you have," such as an identification (ID) card, key, etc., are no longer considered reliable enough to satisfy the

security requirements of electronic transactions. All of these techniques suffer from a common problem of inability to differentiate between an authorized person and an unauthorized who fraudulently acquires the access privilege of the authorized person.

History of Fingerprints

There are records of fingerprints being taken many centuries ago, although they weren't nearly as sophisticated as they are today. In ancient era people pressed the tips of their fingertips into clay to record business transactions. The Chinese used ink-on-paper finger impressions for business and to help identify their children. Until the 19th century fingerprints weren't used as a method for identifying criminals. A few years later, Scottish doctor Henry Faulds was working in Japan when he discovered fingerprints left by artists on ancient pieces of clay. This finding inspired him to begin investigating fingerprints. In 1880, Faulds and Charles Darwin developed fingerprint classification system. Further Galton collected measurements on people around the world to determine how traits were inherited from one generation to the next. He began collecting fingerprints and eventually gathered 8,000 different samples to analyze. In 1892, he published a book called "Fingerprints," in which he outlined a fingerprint classification system — the first in existence. The system was based on patterns of arches, loops and whorls. Sir Edward Henry, commissioner of the Metropolitan Police of London, became interested in using fingerprints to catch criminals. In 1896, he added to Galton's technique, creating his own classification system based on the direction, flow, pattern and other characteristics of the friction ridges in fingerprints. Examiners would turn these characteristics into equations and classifications that could distinguish one person's print from another's. In 1901, Scotland Yard established its first Fingerprint Bureau. The following year, fingerprints were presented as evidence for the first time in English courts. In 1903, the New York state prisons adopted the use of fingerprints, followed later by the FBI.

State of the Art in Fingerprint Recognition

Fingerprint Recognition is the process in which we find out used whether two sets of fingerprint ridge detail come from the same finger. This paper presents a basic introduction to fingerprint recognition systems and their main parts, including a brief description of the process and applications of fingerprints. The main modules of a fingerprint verification system are: a) fingerprint sensing, in which the fingerprint of an individual is taken by a fingerprint scanner to produce a raw digital representation; b) preprocessing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction; c) feature *extraction*, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors; and d) matching, in which the feature vector of the input fingerprint is compared against one or more existing records. The records of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints.

a) Fingerprint Sensing

The processing of fingerprint images is done by spreading the finger with ink and pressing it against a paper card. The paper card is then scanned,

Fig1. Process of Fingerprint Recognition

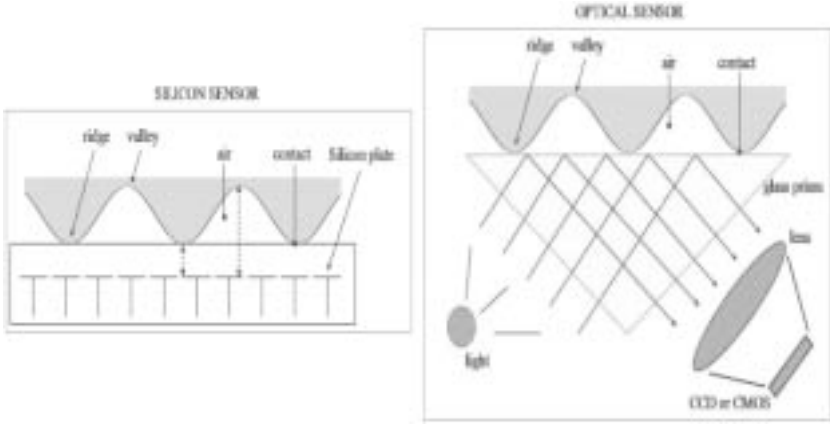

Fig 2. Acquisition principles of silicon and optical sensors

resulting in a digital representation. This process is known as off-line acquisition. Currently, it is possible to acquire fingerprint images by pressing the finger against the flat surface of an electronic fingerprint sensor. This process is known as *online* acquisition. There are three families of electronic fingerprint sensors based on the sensing technology:

I. *Solid-state* or silicon sensors (left part of Fig 2): These contain an array of pixels where each pixel represents a sensor itself. Users place the finger on the surface of the silicon, and four techniques are typically used to convert the ridge/valley information into an electrical signal: capacitive, thermal, electric field and piezoelectric. Since solid-state sensors do not use optical components, their size is considerably smaller and can be easily embedded. On the other hand, silicon sensors are expensive, so the sensing area of solid-state sensors is typically small.

II. *Optical* (right part of Fig.2): The finger touches a glass prism and the prism is illuminated with diffused light. The light is reflected at the valleys and absorbed at the ridges. The reflected light is focused onto a CCD or CMOS sensor. Optical fingerprint sensors provide good image quality and large sensing area but they cannot be miniaturized because as the distance between the prism and the image sensor is reduced, more optical distortion is introduced in the acquired image.

III. *Ultrasound*: Acoustic signals are sent, capturing the echo signals that are reflected at the fingerprint surface. Acoustic signals are able to cross dirt and oil that may be present in the finger, thus giving good quality images. On the other hand, ultrasound scanners are large and expensive, and take some seconds to acquire an image.

b) Preprocessing and Feature Extraction

The process of enhancing the image before the feature extraction is also called pre-processing.A fingerprint is characterized by a pattern of interleaved ridges (dark lines) and valleys(bright lines). Generally, ridges and valleys run in parallel and sometimes they terminate or they bifurcate. At a global level, the fingerprint may present regions with patterns of high curvature, these regions are also called singularity. This pattern sometimes exhibits a number of particular shapes called *singularities*, which can be classified into three types: *loop*, *delta* and *whorl*. At the local level, other important feature called minutia can be found in the fingerprint patterns. Minutia mean small details, and this refers to the behavior of the ridges discontinuities such as termination, bifurcation and trifurcation or other features such as pores (small holes inside the ridges), lake (two closed bifurcations), dot (short ridges), etc. Most system uses only the termination and bifurcations. With the objective of matching the fingerprints we need to extract the fingerprint features such as minutiae and singularity points. From the fingerprint we can also extract other global information such as orientation and frequency of the ridge regions.

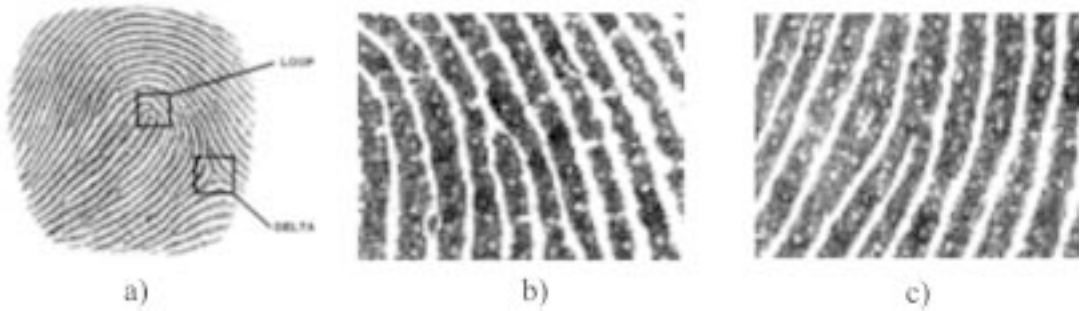

Fig. 3. a) Loop b) Delta c) Whorl

c) Fingerprint Matching

In the matching process, features extracted from the input fingerprint are compared against those in the stored database, which represents a single user (retrieved from the system database based on the claimed identity). The result of such a procedure is either a degree of similarity (also called matching score) or an acceptance/rejection decision. There are fingerprint matching techniques that directly compare gray scale images using correlation-based methods, so that the fingerprint record matches with the gray scale image.

Comparison of Biometric Technologies

Currently, there are mainly nine different biometric techniques that are either widely used Including face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice print, and facial thermograms. A brief comparison of these nine biometric techniques

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Hand Vein	medium	medium	medium	medium	medium	medium	high
Iris	high	high	high	medium	high	low	high
Retinal Scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice Print	medium	low	low	medium	low	high	low
F.Thermograms	high	high	low	high	medium	high	high

Fig. 4: Comparison of Biometric Technologies

is provided in Fig 4.Although each of these techniques satisfies the above requirements and has been used in practical systems or has the potential to become a valid biometric technique not many of them are acceptable as indisputable evidence of identity. For example, despite the fact that extensive studies have been conducted on automatic face recognition and that a number of face-recognition systems are available it has not yet been proven that face can be used reliably to verify identity and a biometric system that uses only face can achieve an acceptable identification accuracy. So far, the only acceptable, automated, and mature biometric technique is the automatic fingerprint identification technique, which has been used and accepted in forensics since the early 1970's.

Applications of biometrics

Biometrics is a rapidly evolving technology that has been widely used in forensics, such as criminal identification, prison security and broad range of civilian applications. The use of fingerprints as a biometric is the oldest mode of computer-aided and personal identification that is most prevalent today.

Following are the various applications of biometrics:-

1) Banking security, such as electronic fund transfers, ATM security, cheque cashing, and credit card transactions
2) Physical access control, such as airport access control
3) Information system security, such as access to databases via login privileges
4) Government benefits distribution, such as welfare disbursement programs
5) Customs and immigration, such as the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry
6) National ID systems, which provide a unique ID to the citizens and integrate different government services
7) Voter and driver registration, providing registration facilities for voters and drivers.

Future Scope

The upcoming techniques of user authentication, which involves the use of passwords and user IDs or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords such as birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric fingerprint authentication technology may solve this problem since a person's biometric data is connected to its owner, is unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card.

Conclusion

Biometrics is a means of verifying personal identity by measuring and analyzing unique physical or behavioral characteristics like fingerprints or voice patterns. The conclusion of this paper is that the manual system should be replaced and there must be easier, reliable, secure, cash free and tension free electronic system, i.e. biometric system in which no one has to take dozens of cards for shopping, traveling, university or bank. So to consider the disadvantages of manual system, the fingerprints system is suggested to be implemented because it is easier, reliable, feasible, secure and authorized to everyone. There is no worry that anyone can stole my finger and anybody can use it. In fingerprint system customer has to place his fingers on the finger scanner and then scanner will recognize the account which belongs to that person and perform the action. Biometric system may be like fingerprints, IRIS, face recognition and blood reading or skin reading and it may be installed at any store, university, library, hostel, bank, office, home door lock, internet online shopping and many kinds where card system is installed. So in this paper we conclude that finger print system is the best biometric for identification of an individual.

References

1. N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", *Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 223-228, 2001.
2. A.K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "FingerCode: A filterbank for fingerprint representation and matching", *Proc. IEEE Conf. on Computer Vision and Pattern Recognition*, vol. 2, pp. 187-193, 1999.
3. L. O'Gorman, "Overview of fingerprint verification technologies", Elsevier Information Security Technical Report, vol. 3, no. 1, 1998.
4. L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021– 2040, Dec. 2003.
5. O' Gorman, L.: Fingerprint Verification, in *Biometrics: Personal Identification in Networked Society*, The Kluwer Academic Publishers, International Series in Engineering and Computer Science, Jain, A. K., Bolle R. and Pankanti, S. eds., Vol. 479, Chapter 2, pp. 43-64 (1999).
6. Uludag, U., Jain, A.: Attacks on biometric systems: a case study in fingerprints. Proc. SPIEEI2004, Security, Seganography and Watermarking of Multimedia Contents VI pp. 622–633 (2004)
7. Putte, T., Keuning, J.: Biometrical fingerprint recognition: dont get your fingers burned. Proc.IFIP TC8/ WG8.8, Fourth Working Conf. Smart Card Research and Adv. App. pp. 289–303 (2000)
8. Jiang, X., Yau, W., Ser, W.: Detecting the fingerprint minutiae by adaptive tracing the gray level ridge. Pattern Recognition 34, 999–1013 (2001)