Volume 2, Issue 4, April 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Fingerprint Biometric System

Sravya. V, Radha Krishna Murthy,Ravindra Babu Kallam, Srujana B
Aizza College of Engineering & Technology, Mancherial
India
sravya47@gmail.com

Abstract—Fingerprint is the most popular biometric system that is widely used in various authentication applications, PC logon, gate access control systems, and so on. The reason can be considered that fingerprint can achieve the best balance among authentication performance, cost, size of device, and ease of use. However, most of fingerprint authentication devices have some problems to be solved. One is that captured images are easily affected by the condition of finger surface and it can degrade authentication performance. The other is that the problem of impersonation by artificial gummy or fake fingers has been pointed out. And the last but not the least is the loss of privacy and security in all biometric systems which include fingerprint biometric system.This survey paper mainly looks into the methods to overcome the above disadvantages of fingerprint biometric system. It concerned with the multimodal biometric system, fake finger detection methods and also looked into how to achieve privacy and security in biometric systems.

Keywords—Fingerprint biometric system, fake fingers, multimodal biometric system, privacy and security in biometric system, encryption of biometric templates.

I. INTRODUCTION

Biometric verification [6] [7] is an automated method whereby an individual's identity is confirmed by examining a unique physiological trait or behavioral characteristic, such as a fingerprint, retina, or signature. Physiological traits are stable physical characteristics, such as palm prints and iris patterns. This type of measurement is essentially unalterable.

A behavioral characteristic — such as one's signature, voice, or keystroke dynamics — is influenced by both controllable actions and less controllable psychological factors. Because behavioral characteristics can change over time, the enrolled biometric reference template must be updated each time it is used. Although Behavior-based biometrics can be less expensive and less threatening to users; physiological traits tend to offer greater accuracy and security. In any case, both techniques provide a significantly higher level of identification than passwords or cards alone.

Biometric traits are unique to each individual; they can be used to prevent theft or fraud. Unlike a password or personal identification number (pin), a biometric trait cannot be forgotten, lost, or stolen. Today there are over 10,000 computer rooms, vaults, research labs, day care centers, blood banks, ATMs and military installations to which access is controlled using devices that scan an individual's unique physiological or behavioral characteristics. Biometric identifiers currently available or under development include fingerprint, face recognition, keystroke dynamics, palm print, retinal scan, iris pattern, signature, and voice pattern.

II. IDENTIFICATION AND VERIFICATION

Identification and *verification* **(**also known as ***authentication*****)** are both used to declare the identity of a user.

Identification: In an identification system, an individual is recognized by comparing with an entire database of templates to find a match. The system conducts one-to-many comparisons to establish the identity of the individual. The individual to be identified does not have to claim an identity (*Who am I?) [9]*.

Verification (authentication): In a verification system, the individual to be identified has to claim his/her identity (*Am I whom I claim to be?)* and this template is then compared to the individual's biometric characteristics. The system conducts one-to-one comparisons to establish the identity of the individual [9]. Before a system is able to verify/identify the specific biometrics of a person, the system requires something to compare it with. Therefore, a profile or template containing the biometric properties is stored in

the system. Recording the characteristics of a person is called *enrollment* [10].
The processes of enrollment, verification, and identification are depicted graphically in fig. 1.

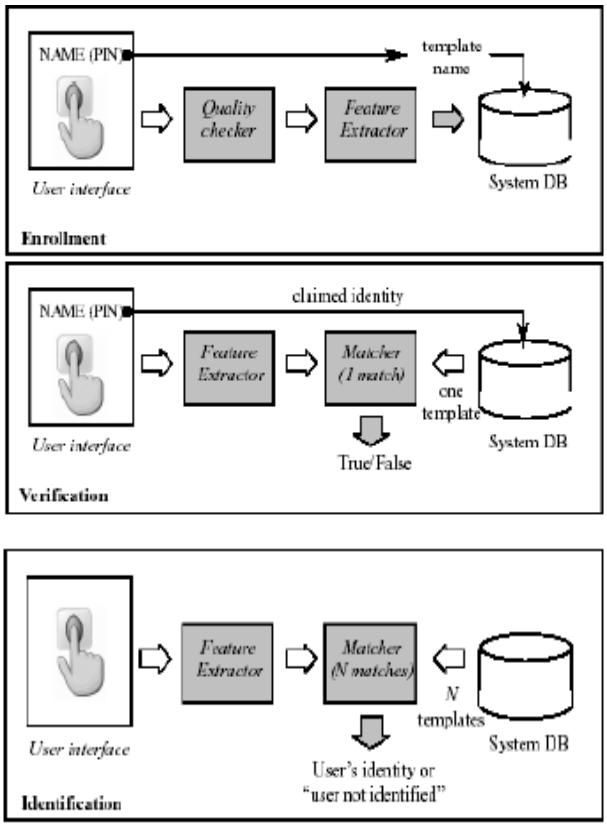

Fig.1. Enrollment, verification, and identification. [9]

A. Results from identification and verification procedures
When results from identification or verification procedures are discussed, the following terms will be used in this report:
Success rate: The rate at which successful verifications or identifications are made compared to the total number of trials [11].
False rejection rate (FRR): The rate at which the system falsely rejects a registered user compared to the total number of trials [11]
False acceptance rate (FAR): The rate at which the system falsely accepts a nonregistered (or another registered) user as a registered one compared to the total number of trials. The FAR is in this report used in the identification version, as a contrast to verification procedures, where it measures if a user is accepted under a false claimed identity [11].
Equal error rate (EER): The common value of the FAR and FRR when the FAR equals the FRR. This is the value where both the FAR and FRR are kept as low as possible at the same time (see fig. 2). A low EER value indicates a high accuracy of the system.

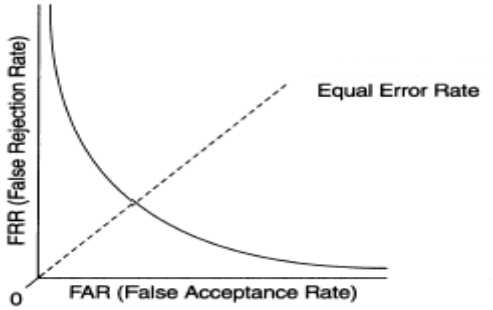

Fig.2. The relationship between FRR, FAR, and EER. A big FRR often means a low FAR, and a big FAR often means a low FRR. The small EER value indicates that the security of the system is better. [12]

III. FINGERPRINT BIOMETRIC SYSTEM

Fingerprint recognition [7] is the technology that verifies the identity of a person based on the fact that everyone has unique fingerprints. It is one of the most heavily used and actively studied biometric technologies.
A. Why Fingerprints?
The cost of a fingerprint based biometric system is quite low in comparison to others like iris and face readers. Fingerprint based systems are quite strong and can be deployed across any kind of environment. This system is less intrusive than iris or retina scans. Most people find it unacceptable to have their pictures taken by video cameras or to speak into a microphone. Finger based systems are more user friendly. Besides, the ability to enroll multiple fingers makes this a very flexible option. It is a proven technology and has been in use for a long time as compared to other nascent technologies.
B. Principles of fingerprint biometrics
A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points[8], ridge endings (where a ridge end) and ridge bifurcations (where a ridge splits in two). Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other)[18].The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. There are five basic fingerprint patterns: arch, tented arch, left loop, right loop and whorl. Loops make up 60% of all fingerprints, whorls account for 30%, and arches for 10%.Fingerprints are usually considered to be unique, with no two fingers having the exact same dermal ridge characteristics**.**
C. How does fingerprint biometrics work
The main technologies used to capture the fingerprint image with sufficient detail are optical, silicon, and

ultrasound. There are two main algorithm families to recognize fingerprints:

1) Patterns: The three basic patterns of fingerprint ridges are the arch, loop, and whorl [15]. An arch is a pattern where the ridges enter from one side of the finger, rise in the centre forming an arc, and then exit the other side of the finger. The loop is a pattern where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter. In the whorl pattern, ridges form circularly around a central point on the finger. Scientists have found that family members often share the same general fingerprint patterns, leading to the belief that these patterns are inherited [16].

Pattern matching compares the overall characteristics of the fingerprints, not only individual points. Fingerprint characteristics can include sub-areas of certain interest including ridge thickness, curvature, or density. During enrollment, small sections of the fingerprint and their relative distances are extracted from the fingerprint. Areas of interest are the area around a minutia point, areas with low curvature radius, and areas with unusual combinations of ridges.

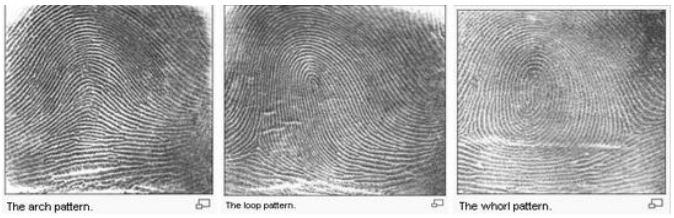

Fig.3 Different patterns arch, loop and whorl pattern respectively [13][15].

2) Minutia features: The major Minutia features [7] of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

Minutia matching compares specific details within the fingerprint ridges. At registration (also called enrollment), the minutia points are located, together with their relative positions to each other and their directions. At the matching stage, the fingerprint image is processed to extract its minutia points, which are then compared with the registered template.

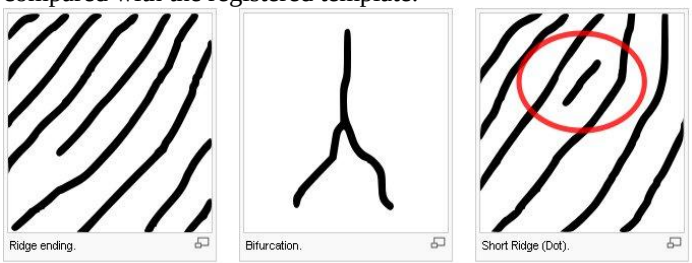

Fig.4. Different Minutia features

D. Issues with fingerprint systems

The tip of the finger is a small area from which to take measurements, and ridge patterns can be affected by cuts, dirt, or even wear and tear. Acquiring high-quality images of distinctive fingerprint ridges and minutiae is complicated task.

People with no or few minutia points (surgeons as they often wash their hands with strong detergents, builders, people with special skin conditions) cannot enroll or use the system. The number of minutia points can be a limiting factor for security of the algorithm. Results can also be confused by false minutia points (areas of obfuscation that appear due to low-quality enrollment, imaging, or fingerprint ridge detail).

Note: There is some controversy over the uniqueness of fingerprints. The quality of partial prints is however the limiting factor. As the number of defining points of the fingerprint becomes smaller, the degree of certainty of identity declines. There have been a few well-documented cases of people being wrongly accused on the basis of partial fingerprints.

E. Benefits of fingerprint biometric systems

- Cheap
- Small size
- Low power
- Non-intrusive
- Easy to use
- Large database already available
-

F. Disadvantages fingerprint biometric systems

- Vulnerable to noise and distortion brought on by dirt and twists.
- Some people have damaged or eliminated fingerprints.
- Using fake fingers by intruders.

G. Applications of fingerprint biometrics

Fingerprint sensors are best for devices such as cell phones, USB flash drives, notebook computers and other applications where price, size, cost and low power are key requirements [17]. Fingerprint biometric systems are also used for law enforcement, Forensics, dermatoglyphics, background searches to screen job applicants, healthcare and welfare.

IV. FINGERPRINT SENSORS

There are two main types of sensors for inputting fingerprints. One is an optical sensor using a prism or hologram, and the other type is a non-optical sensor. Recently, products employing both optical and non-optical methods have been introduced. In the past, a semiconductor sensor was the only non-optical choice, but now equipment with ultrasonic sensors, another type of non-optical sensors, are on the market.

A. Optical fingerprint sensors

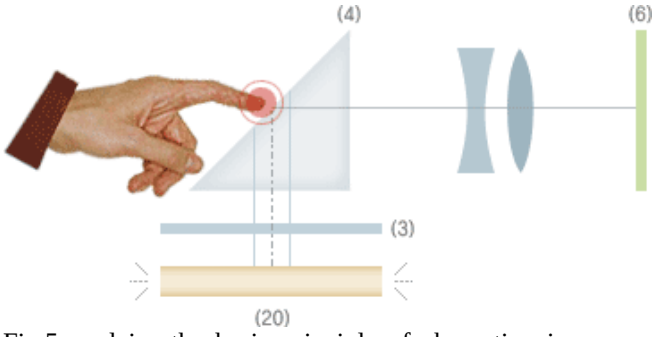

Fig.5 explains the basic principle of absorption in an optical fingerprint sensor.

An absorption optical fingerprint sensor [6] is composed of a right-angled triangle prism (4), light source (20), a diffusion plate (3), a lens group and an image sensor (6).
When a fingerprint is placed on the contact surface, its ridges are closely pressed onto the surface while its valleys are detached from it.
The light radiated from light source becomes uniform after undergoing the diffusion plate. The light reaches the fingerprint contact surface after passing through the prism. If the light touches the valley, total internal reflection happens so that it reaches the image sensor composed of CCD (Carge Coupled Device) element or CMOS (Complementary Metal Oxide Semiconductor) element after going through the lens group. On the other hand, if the light reaches the ridges closely pushed onto the surface, some light goes to the image sensor after the total internal reflection and some light is absorbed in the ridges.
There are changes in luminous intensity between light reflected from valleys and light from ridges and the image sensor obtains the fingerprint image by calculating the changes in the reflected light intensity between the two.
The absorption optical fingerprint sensor needs several LEDs (15-20) since the light should be two-dimensionally uniform after going through the diffusion plate. To capture a fingerprint image without distortion brought on by different optical paths, enough distance is required between the prism and the image sensor.

B. Non -Optical fingerprint sensors

A semiconductor fingerprint sensor is a prime example of non-optical sensors. Fig. 6 shown below describes the basic principle of the semiconductor fingerprint sensor.

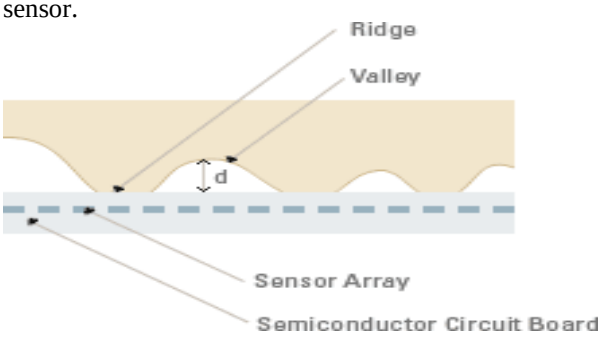

Fig. 6 Basic principle of the semiconductor fingerprint sensor

The semiconductor fingerprint sensor [6] measures the electrostatic capacity between sensor surface and skin, and translates it into an image. If a user places his or her fingerprint on the surface, its ridges are closely pressed on the surface and its valleys have some space from the surface. In the case of the ridges, the distance (d) between ridges and surface is short so that the electrostatic capacity is high. On the other hand, the valleys are distant from the surface compared to the ridges, so the electrostatic capacity is low. The fingerprint image can be captured by composing signals obtained from an array of sensors on the semiconductor surface. The semiconductor fingerprint sensor can be lighter and smaller. But it is vulnerable to external shocks and chemical substances such as sodium chloride from people's skin due to the physical traits of a silicon wafer, which is fundamental to the sensor. To address these disadvantages, the contact surface is being coated. Developing a physically strong coating is one of the major tasks facing semiconductor fingerprint sensors.

V. MULTIMODAL BIOMETRIC SYSTEM

Multimodal biometric technology [5] uses more then one biometric identifier to compare the identity of the person. The main disadvantage is (rejecting the valid user due to scar, cuts, bruises on the finger) overcome by this system. We are having two options in this multimodal biometric system. They are scanning more than one finger and using other biometric systems like face, voice, iris etc.

A. Using more than one finger

As we have ten fingers, we can use more than one finger for high reliability. The number of finger used is our choice. The number is directly proportion to the reliability of the biometric system. The main advantage is no extra hardware is required, but a small disadvantage is memory, however it's not at all a problem now days because cost of storage device is cheap.

B. Using other Biometric factors

In this we integrate face recognition, fingerprint verification, and speaker verification in making a personal identification. This system takes advantage of the capabilities of each individual biometric. It can be used to overcome some of the limitations of a single biometrics. Preliminary experimental results demonstrate that the identity established by such an integrated system is more reliable than the identity established by a face recognition system, a fingerprint verification system, and a speaker verification system
Therefore in the case of a system using say three technologies i.e. face, finger and voice. If one of the technologies is unable to identify, the system can still

use the other two to accurately identify against. The fig.7 depicts the multimodal biometric system.

C. The benefits of multimodal biometrics

By using more than one means of biometric identification, the multimodal biometric identifier can retain high threshold recognition settings. The system administrator can then decide the level of security he/she requires. For a high security site, they might require all three biometric identifiers to recognise the person or for a lower security site, only one or two of the three. With this methodology, the probability of accepting an impostor is greatly reduced.

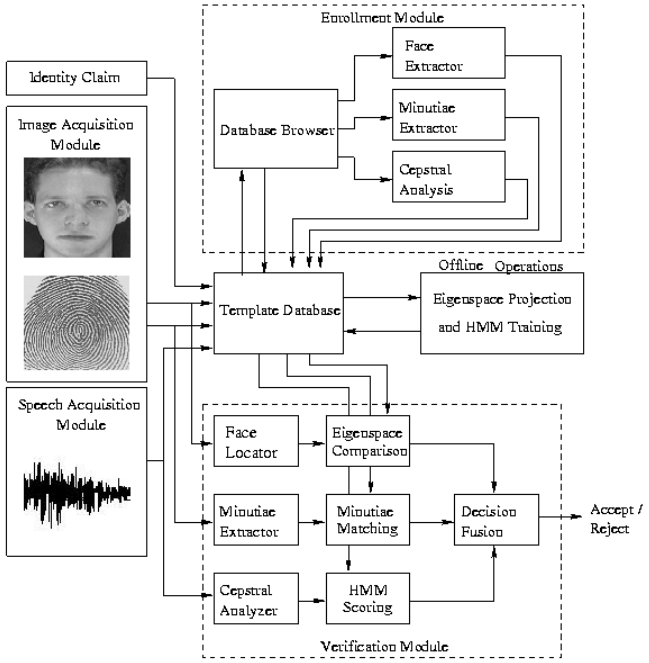

Fig.7 A Multimodal Biometric System Using Fingerprint, Face, and Speech.

VI. FAKE FINGER DETECTION

Liveness detection in a biometric system means the capability for the system to detect, during enrollment and identification/verification, whether or not the biometric sample presented is alive or not. If the system is designed to protect against attacks with artificial fingerprints, it must also check that the presented biometric sample belongs to the live human being who was originally enrolled in the system and not just any live human being.

Fingerprint scanners can be spoofed by artificial fingers using mouldable plastic, clay, Play-Doh, gelatin, silicone rubber materials, etc. Liveness detection [2] is an anti-spoofing method which can detect physiological signs of life from fingerprints to ensure only live fingers can be captured for enrollment or authentication.

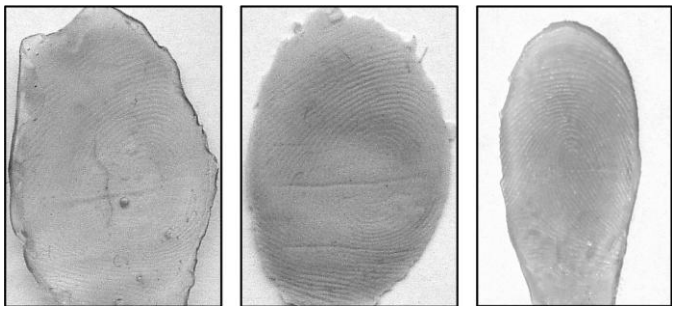

Fig.8. Fake fingertips created with different materials. From left to right: gelatin, silicone, and latex.

A. Fake finger detection approach

There are different methods to detect the liveness of finger scan.

A live finger can have the following properties

- Temperature sensing
- Detection of pulsation on finger trip
- Pulse oximetry
- Electrical conductivity [1]

1) Temperature:

The temperature of the epidermis is about 26{30±C. When using a thin silicone artificial fingerprint, this results in a decrease by a maximum of 2±C of the temperature transfer to the sensor. Obviously, it will not be difficult to have the temperature[14] of the artificial fingerprint within the working margins of the sensor. Sensors that are used outdoors often have a broader working margin, giving the intruder even better prerequisites.

2) Pulsation:

The pulse in the tip of the finger can be detected and used as a liveness detection method. With a wafer-thin artificial fingerprint, the underlying finger's pulse [14] will however be sensed. Also, practical problems arise due to changes in the pulse. A person with a pulse of 40 beats per minute implicates that the finger must be held for at least four seconds on the sensor for the pulse to be detectable. The same person could have a pulse of 80 beats per minute if he or she worked out immediately before the fingerprint scanning. The emotional state of the person also affects the pulse.

3) Pulse oximetry:

Pulse oximetry is used in the medical field to measure the oxygen saturation of haemoglobin in a patient's arterial blood. A pulse oximeter also measure the pulse rate. The technology involved is based on two basic principles. First, haemoglobin absorbs light differently at two different wavelengths depending on the degree of oxygenation. Second, the fluctuating volume of arterial blood for each pulse beat adds a pulsatile component to the absorption. Detection of pulse oximetry [14] can be fooled using a translucent artificial fingerprint which covers only the live finger's fingerprint. The pulse oximetry will measure the saturation of oxygen of haemoglobin in the intruder's finger's blood.

4) Electric resistance

The electric resistance of the skin can range from a couple of kilo-Ohms to several mega-Ohms depending on the humidity of the finger. With some people having dry fingers, and others being sweaty, it is easy to realize that the span of allowed resistance levels will be great enough for an intruder to easily fool the system. For example, by putting some saliva on the silicone artificial fingerprint, the system will be fooled into believing it is the live finger [14].

5) Relative dielectric permittivity

The relative dielectric permittivity (also known as relative dielectric constant or RDC) [14], is a measurement of the degree to which a medium resists the flow of electric charge divided by the degree to which free space resists such charge. The different values of RDC between a live finger and an artificial fingerprint is the basis of this liveness detection method. Just like electric resistance, the RDC is also affected by the humidity of the finger, so to get an acceptable FRR, the range of acceptable RDCs will include the RDC of a gelatin fingerprint. An artificial fingerprint made of silicone on the other hand, has to be prepared with a solution of 90 % alcohol and 10 % water to fool a system. The RDCs of alcohol and water are 24 and 80 respectively, while the RDC of human skin has a value in between these. Since the alcohol will evaporate quicker than water, the RDC will soon be within the acceptance range of the sensor.

By considering these properties we can use sensors to detect the fake fingers. The user is required to place a finger onto the scanner surface and to apply some pressure while rotating the finger in either clockwise or counter-clockwise direction.

VII. PRIVACY AND SECURITY ISSUES ON BIOMETRIC SYSTEMS

Since biometric data are unique and permanent characteristics of individuals, the privacy protection of biometric authentication schemes [3] has become a common concern of the public.

- Growing biometrics deployments and uses pose significant systemic risks to individual privacy and security
- Biometrics a lifetime permanent identifier, worse than a password (access control)
- Indiscriminate or excess collection of biometric data invites misuse.
- Unauthorized secondary use of biometric data.
- Poor accountability will undermine trust, acceptance and use.

To achieve privacy and security we need to follow cryptographic techniques. This is called biometric encryption [4] in this scenario.

A. Biometric Encryption

Rather than comparing the biometric data directly, a key is derived from these data and subsequently knowledge of this key is proved.

The goal of a biometric encryption system is to embed a secret into a biometric template in a way that can only be decrypted with a biometric image from the enrolled person.

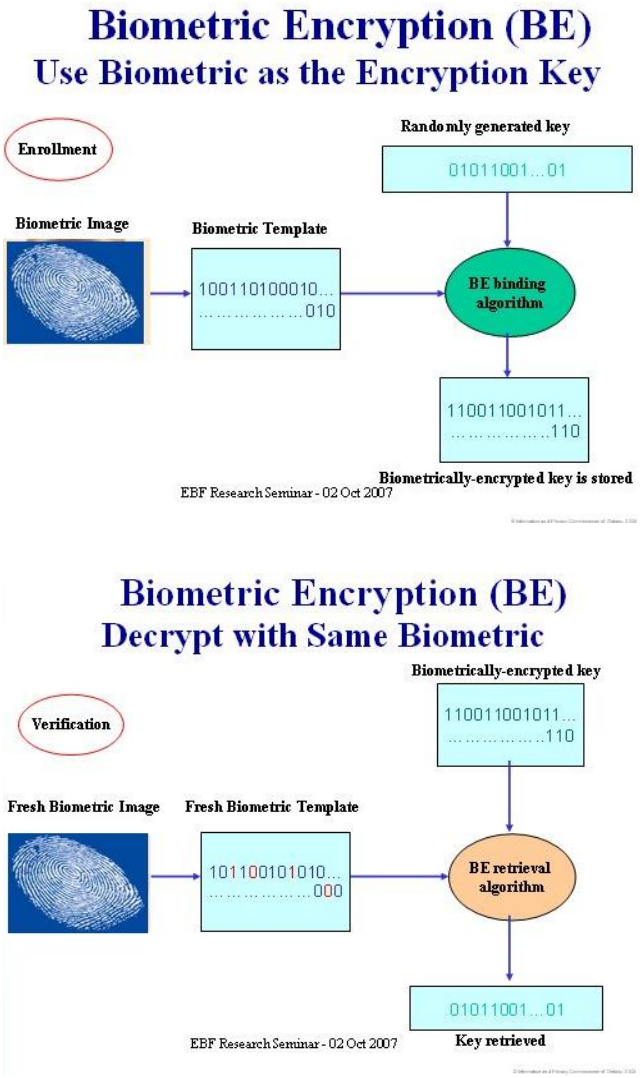

Figure 9 Biometric Encryption

Biometric Encryption is conceptually simple. Make the biometric the actual encryption key. In a sense, this is the ultimate private key, always stored with the person. The technology uses the biometric to encrypt the key or other ID information.

The storage of the biometric remains with the individual and can be used at any time to create a biometrically-encrypted key. The biometrically-encrypted key can be stored in a central database, but no one can access it without the direct involvement of the data subject. This allows a data subject unlimited numbers of keys or identifiers.

The key can only be decrypted with the use of the data subject's biometric. The greatest challenge is to

generate the same key from each reading of the biometric, and to make the system resilient against attacks.

VIII. CONCLUSION

Biometrics is a means of verifying personal identity by measuring and analyzing unique characteristics like fingerprints.This paper presents the detailed information about fingerprint biometrics and specially focussed on methods that overcome the disadvantages of fingerprint biometric system.

Fingerprint biometric system is used in all fields except chemical industries because the finger print of those people working in Chemical industries are often affected. Therefore these companies cannot use the finger print mode of authentication .To overcome this problem multimodal biometrics system can be applied in chemical industries. Still, Fingerprint recognition systems can be very useful if used in the right applications under the right circumstances.

We like to conclude that Finger print biometrics is one of the efficient, secure, cost effective, ease to use technologies for user authentication and according to our survey almost all drawbacks are overcomed in fingerprint biometric system.

ACKNOWLEDGEMENTS

We would like to thank our beloved parents for their overwhelming support all along.

We also thank the management of Aizza College of Engineering & Technology for allowing us to work on this in the college campus

REFERENCES

[1] Utilizing Characteristic Electrical Properties of the Epidermal Skin Layers to Detect Fake Fingers in Biometric Fingerprint Systems—*A Pilot Study*, 16 April 2007.

[2] Fingerprint liveness detection based on quality measures, *IEEE*, 08 July 2009.

[3] Biometric Systems: *Privacy and Secrecy Aspects*, *IEEE*, 17 November 2009.

[4] On biometric encryption using fingerprint and its security evaluation, *IEEE Conferences*, February 2009.

[5] European Biometrics Forum (EBF) Research Seminar, 2007.

[6] www.biometrics.org

[7] www.cse.msu.edu/biometrics

[8] Samir Nanavati, Michael Thieme, Raj Nanavati *Biometrics- identify verification in a networked world*

[9] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of FingerprintRecognition*. Springer Verlag, New York, NY, USA, June 2003.

[10] T. van der Putte and J. Keuning. Biometrical Fingerprint recognition: don't get your fingers burned. In *Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, pages 289-303.Kluwer Academic Publishers, September 2000.

[11] J. Blomm¶e. *Evaluation of biometric security systems against artificial fingers. Master's thesis* LITH-ISY-EX-3514- Department of Electrical Engineering, LinkÄoping University, LinkÄoping, Sweden, October 2003.

[12] Jr. J. D. Woodward, N. M. Orlands, and P. T. Higgins. *Biometrics: Identity assurance in the information age*. McGraw-Hill/Osborne, Berkeley, California, USA, 2003.

[13] International Biometric Group. The henry classification system,2003. Available at http://www.biometricgroup.com/Henry %20Fingerprint%20Classification.pdf [accessed 12/05/04].

[14] Marie SandstrÄom *Liveness Detection in Fingerprint Recognition Systems by, Reg nr*: LITH-ISY-EX-3557-2004.

[15] Dileep Kumar, Yeonseung RyuA *Brief Introduction of Biometrics and Fingerprint Payment Technology* http://www.sersc.org/journals/IJAST/vol4/4.pdf

[16] Anil Jain, Umut Uludag and Arun Ross *Biometric Template Selection: A Case Study in Fingerprints.*

[17] Ross Anderson's: *"Chapter 13th Biometrics of Security Engineering".*

[18] Fernando L. Podio: *"Personal Authentication Through Biometric Technologies"*

