ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

Multimodal Biometric System: An Overview

D.Gayathri[1], Dr.R.Uma Rani[2]

Assistant Professor, Dept. of Computer Science, Periyar University College of Arts and Science, Salem, India[1]

Associate Professor, Dept. of Computer Science, Sri Saradha College For Women, Salem, India[2]

ABSTRACT: Information Security is the process by which an organization protects and secures data communications and storage. Biometrics is a field of science which deals with the positive identification of unique individuals based on their physiological or behavioural characteristics. Each biometric has its strength and weakness. No single biometric is expected to effectively meet the requirements of all applications. Biometric products provide improved security over traditional electronic access controls. While some technologies have gained more acceptance then others, it is beyond doubt that the field of access control biometrics has gained a measure of acceptance. In certain situations, the user might find one form of biometric identification is not exact enough for identification. Unimodal biometric system have to contend with a variety of problems such as noisy data, spoof attacks, non-universality, intra-class variations etc. These limitations can be overcome by Multimodal biometric system. Multimodal biometric technology uses more then one biometric identifier to compare the identity of the person for better security. This article describes about Multimodal Biometric technologies, modules and levels of fusions, design issues and modes of operations etc.

Keywords: **Fusion, PCA, LDA, Patterns, Minutia, Feature extraction**

I. INTRODUCTION

With a growing concern regarding security, interest in biometrics is increasing. Since biometrics utilizes a user's physiological or behavioral characteristic, which is unique and immutable, the compromise of biometric templates is a serious problem. Fingerprint authentication system is one of the most widely used biometric authentication systems. In general, in the enrollment procedure, the features are extracted from the enrollment image and are stored as a template. The template is compared to the features extracted from the verification image. Unlike passwords, however, biometrics has no or little substitutions. For example, if one's fingerprint template is compromised, he or she cannot use that fingerprint for any other fingerprint authentication system from then on.

The deployment of automatic biometrics-based personal recognition systems and their acceptance by the society depends on several factors such as the ease of use, the non-intrusive methods of operation and their related privacy concerns; as well as their recognition accuracy, reliability and security levels, response time and system costs. All these factors will determine the successful spread of the biometric security in a wide range of daily use applications such as electronic payment, access systems, border control, health monitoring, etc. all over the world.

A biometric system involves two steps like Enrollment and Authentication. In enrollment step Biometric data (fingerprint, face, iris) are captured, transformed into a template linked to the individual and stored as a reference. In Authentication step, a new template is issued from a new capture, and compared to the stored reference template as shown in fig.1.

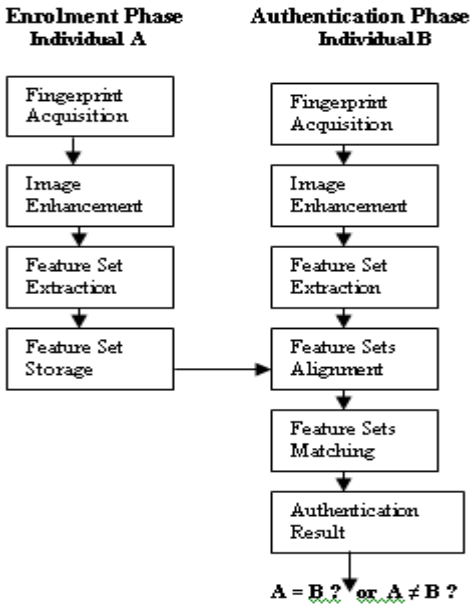

Fig.1 Processing phases of an Automatic Fingerprint-based Authentication System

Unimodal biometric systems have to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates. Some of these limitations can be addressed by deploying multimodal biometric systems that integrate the evidence presented by multiple sources of information [3].

II. MULTIMODAL BIOMETRIC TECHNOLOGIES

In order for the biometrics to be ultra-secure and to provide more-than-average accuracy, more then one form of biometric identification is required. Hence

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

the need arises for the use of multimodal biometrics. This uses a combination of different biometric recognition technologies [5].

A pattern / template that is going to be identified is going to be matched against every known template, yielding either a score or distance describing the similarity between the pattern and the template. The system assigns the pattern to the person with the most similar biometric template. To prevent impostor patterns (in this case all patterns of persons not known by the system) from being correctly identified, the similarity has to exceed a certain level. If this level is not reached, the pattern is rejected [4].

With verification, a person's identity is known and therefore claimed a priority to search against. The pattern that is being verified is compared with the person's individual template only. Similar to identification, it is checked whether the similarity between pattern and template is sufficient enough to provide access to the secured system or area.

III. MULTIMODAL BIOMETRICS IN TERMS OF FAR & FRR

In biometric systems, a biometric identifier is personal and sensitive. Two types of errors are present at the verification step:

• *false match*: the verification process outcome is that biometric measurements from two different persons are from the same person

• *false non-match*: the verification process outcome is that two biometric measurements from the same person are from two different persons

These two types of errors are quantified by the *false acceptance* rate and the *false rejection* rate respectively [7].

A biometric recognition system can be used in two different modes: identification or verification. Identification is the process of trying to find out a person's identity by comparing the person who is present against a biometric pattern/template database[4]. The system would have been pre-programmed with biometric pattern or template of multiple individuals. During the enrolment stage, a biometric would have been processed, stored and encrypted, for each individual.

Biometric systems use scores (also called weights) to express the similarity between a pattern and a biometric template. The higher the score, the higher the similarity is between them. As described in the previous section, access to the system is granted only, if the score for an authorized individual (identification) or the person that the pattern is verified against (verification) is higher then a certain threshold.

In theory, authorized user scores (scores of patterns from persons known by the system) should always be higher than the scores of impostors. If this was true, a single threshold, that separates the two groups of scores, could be used to differ between clients and impostors. This unfortunately is not the reality for real world biometric systems. In some cases, impostor patterns can generate scores that are higher than the scores of an authorized user's patterns (FAR or false acceptance rate). For this reason when the classification threshold is chosen some classification errors may occur.

For example you may configure the threshold with a high setting, which will reject all impostor patterns that exceed this limit. As a result no patterns are falsely accepted by the system. But on the other hand the authorised user patterns with scores lower than the highest impostor scores are also falsely rejected. The opposite scenario would be to configure a low threshold that ensures no client patterns are falsely rejected. However, this would than allow a certain percentage of impostor patterns to be falsely accepted. If you choose the threshold somewhere between those two points, both false rejections and rejections false acceptances occur. This creates an access control environment which is obviously not ideal for high security installations.

IV. FINGERPRINT VERIFICATION OR AUTHENTICATION

Fingerprint verification or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These includes

- Patterns(aggregate characteristics of ridges)
- Minutia (unique features found within the patterns)

A. *Patterns*:

The three basic patterns of fingerprint ridges are the arch, loop and whorl:

- Arch: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
- Loop: The ridges enter from one side of a finger and then exit on that same side.
- Whorl: Ridges form circularly around a central point on the finger.

B. *Minutia Features*:

The major Minutia features of fingerprint ridges are

- Ridge ending- the abrupt end of ridge or the point at which a ridge terminates.
- Ridge Bifurcations are points at which a single ridge splits into two ridges.
- Short ridges(or dots)/independent ridge- are ridges which are significantly shorter than the average ridge length on the fingerprint.
- Island – a single small ridge inside a short ridge or ridge ending that is not connected to all other ridges

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

- Ridge enclosure – a single ridge that bifurcates and reunites shortly afterward to continue as a single ridge
- Spur – a bifurcation with a short ridge branching off a longer ridge
- Crossover or bridge – a short ridge that runs between two parallel ridges
- Delta – a Y – shaped ridge meeting
- Core – a U – turn in the ridge pattern

Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

V. FINGERPRINT SENSORS

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan[3]. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching.

Finger print Technologies:

- Optical
- Ultrasonic
- Capacitance
  - ✓ Passive Capacitance
  - ✓ Active Capacitance

A. *Optical*:

Optical fingerprint imaging involves capturing a digital image of the print using visible light. This type of sensor is, in essence, a specialized digital camera. The top layer of the sensor, where the finger is placed, is known as the touch surface. Beneath this layer is a light-emitting phosphor layer which illuminates the surface of the finger. The light reflected from the finger passes through the phosphor layer to an array of solid state pixels(a charged-coupled device) which captures a visual image of the fingerprint.

A scratched or dirty touch surface can cause a bad image of the fingerprint. A disadvantage of this type of sensor is the fact that the imaging capabilities are affected by the quality of skin on the finger. For instance, a dirty or marked finger is difficult to image properly. Also, it is possible for an individual to erode the outer layer of skin on the fingertips to the point where the fingerprint is no longer visible. It can also be easily fooled by an image of a fingerprint if not coupled with a "live finger" detector. However, unlike capacitive sensors, this sensor technology is not susceptible to electrostatic discharge damage.

B.*Ultrasonic*:

Ultrasonic sensors make use of the principles of medical ultrasonography in order to create visual images of the fingerprint. Unlike optical imaging, ultrasonic sensors use very high frequency sound waves to penetrate the epidermal layer of skin. The sound waves are generated using piezoelectric transducers and reflected energy is also measured using piezoelectric materials. Since the dermal skin layer exhibits the same characteristic pattern of the fingerprint, the reflected wave measurements can be used to form an image of the fingerprint. This eliminates the need for clean, undamaged epidermal skin and a clean sensing surface.

C. *Capacitance*:

Capacitance sensors utilize the principles associated with capacitance in order to form fingerprint images. In this method of imaging, the sensor array pixels each act as one plate of a parallel-plate capacitor, the dermal layer(which is electrically conductive) acts as the other plate, and the non-conductive epidermal layer acts as a dielectric.

1) Passive Capacitance:

A passive capacitance sensor uses the principle outlined above to form an image of the fingerprint patterns on the dermal layer of skin. Each sensor pixel is used to measure the capacitance at that point of array. The capacitance varies between the ridges and valleys of the fingerprint due to the fact that the volume between the dermal layer and sensing element in valleys contains an air gap. The dielectric constant of the epidermis and the area of the sensing element are known values. The measure capacitance values are then used to distinguish between fingerprint ridges and valleys.

2) Active Capacitance:

Active capacitance sensors use a charging cycle to apply a voltage to the skin before measurement takes place. The application of voltage charges the effective capacitor. The electric field between the finger and sensor follows the pattern of the ridges in the dermal skin layer. On the discharge cycle, the voltage across the dermal layer and sensing element is compared against a reference voltage in order to calculate the capacitance. The distance values are then calculated mathematically, and used to form an image of the fingerprint. Active capacitance sensors measure the ridge patterns of the dermal layer like the ultrasonic method. Again, this eliminates the need for clean, undamaged epidermal skin and a clean sensing surface.

VI. DIFFERENT MODULES AND LEVELS OF FUSION

A generic biometric system has 4 important modules:

- ✓ the sensor module which captures the trait in the form of raw biometric data
- ✓ the feature extraction module which process the data to extract a feature set that is a compact representation of the trait
- ✓ the matching module which employs a classifier to compare the extracted feature set with the templates residing in the database to generate matching scores
- ✓ the decision module which uses the matching scores to either determine an identity or validate a claimed identity.

In multimodal biometric system information reconciliation can occur in any of the aforementioned modules as in fig.2.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

- ✓ Fusion at the data or feature level: Either the data itself or the feature sets originating from multiple sensors/sources are fused.
- ✓ Fusion at the match score level: The scores generated by multiple classifiers pertaining to different modalities are combined.
- ✓ Fusion at the decision level: The final outputs of multiple classifiers are consolidated via techniques such as majority voting.
- ✓ Biometric systems that integrate information at an early stage of processing are believed to be more effective than those systems which perform integration at later stage[1].

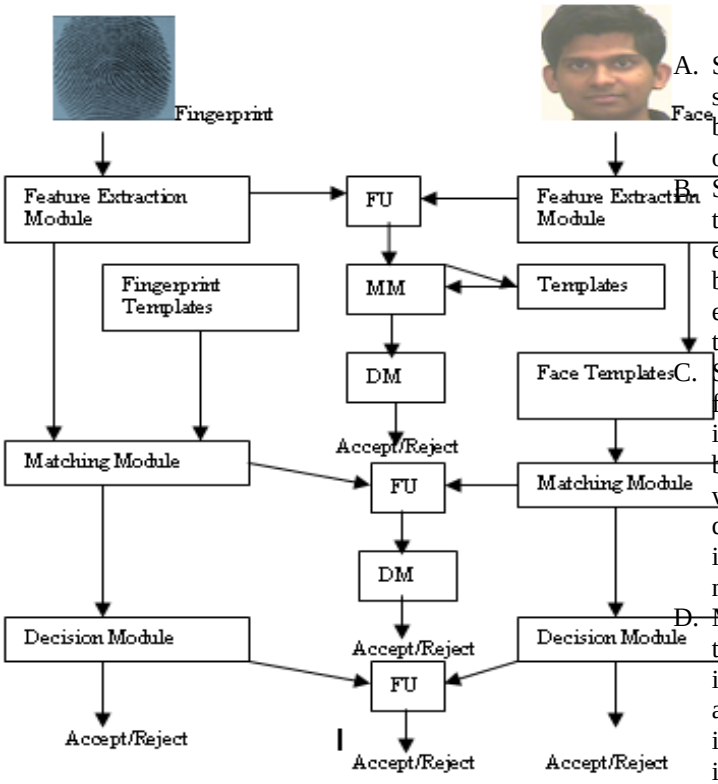

Fig.2. Levels of fusion in a Multimodal biometric system
FU: Fusion Module, MM: Matching Module, DM: Decision Module

VII. FUSION SCENARIOS OF MULTIMODAL BIOMETRIC SYSTEM

Depending on the number of traits, sensors, and features set used, a variety of scenarios are possible in a multimodal biometric system as shown in fig.3.

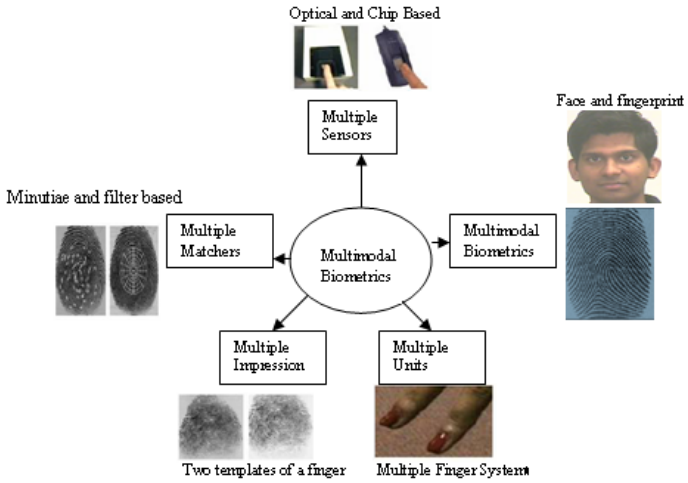

Fig.3. Scenarios in a Multimodal Biometric System

A. Single biometric trait, multiple sensors: Multiple sensors record the same biometric trait. Thus, raw biometric data pertaining to different sensors are obtained[1].

B. Single biometric trait, multiple classifiers: Unlike the previous scenario, only a single sensor is employed to obtain raw data; this data is then used by multiple classifiers[1]. Each of these classifiers either operate on the same feature set extracted from the data or generate their own feature sets.

C. Single biometric trait, multiple units: In the case of fingerprints(or iris), it is possible to integrate information presented by two or more fingers(or both the irises) of a single user. This is an expensive way of improving system performance since this does not entail deploying multiple sensors nor incorporating additional feature extraction and /or matching modules[1].

D. Multiple biometric traits: Here, multiple biometric traits of an individual are used to establish the identity. Such systems employ multiple sensors to acquire data pertaining to different traits. The independence of the traits ensures that a significant improvement in performance is obtained[1].

VIII. MODES OF OPERATION

A multimodal system can operate in one of three different modes:

- ✓ Serial Mode
- ✓ Parallel mode
- ✓ Hierarchical mode

In the *serial* mode of operation, the output of one modality is typically used to narrow down the number of possible identities before the next modality is used. Therefore multiple sources of information (e.g., multiple traits) do not have to be acquired simultaneously. Further, a decision could be made before acquiring all the traits. This can reduce the overall recognition time[4].

In *parallel* mode of operation, the information from multiple modalities are used simultaneously in order to perform recognition.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

In the *hierarchical* scheme, individual classifiers are combined in a treelike structure. This mode is relevant when the number of classifiers is large.

IX. DESIGN ISSUES

A variety of factors should be considered when designing a multimodal biometric system. These include

- ✓ The choice and number of biometric traits
- ✓ The level in the biometric system at which information provided by multiple traits should be integrated
- ✓ The methodology adopted to integrate the information
- ✓ The cost versus matching performance trade off.

The choice and number of biometric traits is largely driven by the nature of the application, the overhead introduced by multiple traits (computational demand and cost, for example), and the correlation between traits considered.

X. CONCLUSION

By using more then 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. Multimodal biometric systems elegantly address several of the problems present in unimodal systems [6]. By combining multiple sources of information, this system improves matching performance, increase population coverage, determines spoofing and facilitates indexing. Various fusion levels and scenarios are possible in multimodal systems. Incorporating user-specific parameters can further improve performance of these systems.

REFERENCES

[1] K. Jain, A. Ross, and S. Prabhakar, "*An Introduction to biometric recognition*, "IEEE trans on Circuits and Systems for Video Technology, vol.14, pp. 4-20, Jan 2004.

[2] X. Lu, Y. Wang, and A. K. Jain, *"Combining classifiers for face recognition,"* in Proc. IEEE Int'l Conf. on Multimedia and Expo(ICME), vol. 3, (Baltimore, MD),pp. 13-16,Jul 2003.

[3] [3] Arun Ross and Anil K. Jain," *Multimodal Biometrics: An Overview",* Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp 1221-1224, September 2004.

[4] http://en.wikipedia.org/w/index.php?title=Iris_recognition &oldid= 455497359.

[5] http://en.wikipedia.org/w/index.php?title=Iris_recognition &oldid= 451687504.

[6] Binsu C.Kovoor, Supriya M. H, and K. Poulose Jacob, "*A Prototype for a Multimodal Biometric Security system based on Face and Audio Signatures",* International Journal of Computer Science and Communication, June 2011.

[7] Rima Belguechi, Estelle Cherrier, Vincent Alimi, Patrick Lacharme and Christophe Rosenberger, "*An Overview on Privacy Preserving Biometrics, Recent Application in Biometrics",* Dr. Jucheng Yang (Ed.), ISBN: 978-953-307-488-7, 2011.

D. Gayathri has completed her M.C.A from J.K.K Nataraja College of Arts and Science, Komarapalayam, affiliated with Periyar University. She received her M.Phil Degree from Periyar University in June 2005. Now pursuing her Part time Ph.D., research in Periyar University, Salem. Now she is working as Assistant Professor, Department of Computer Science in Periyar University College of Arts and Science, Mettur Dam, Salem Dt. Her research area is of Information security.

Dr. R. Uma Rani has completed her M.C.A. from NIT, Trichy in 1989. She did her M.Phil. From Mother Teresa University, Kodaikanal. She received her Ph.D., from Periyar University, Salem in the year 2006. She has published around 50 papers in reputed journals and National and International Conferences. She has received the best paper award from VIT, Vellore, Tamil Nadu in an International conference. She was the PI for MRP funded by UGC. She has acted as resource person in various National and International conferences. Her area of interest includes Information Security, Data Mining, Fuzzy Logic and Mobile Computing. She is working as Associate Professor in Department of Computer Science, Sri Sarada College for women, Salem.