ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# Automatic Personal Identification and Verification Using Fingerprints Associated with Multimode Biometrics Approach.

Syed Mohsin Saif*, Sani Asnain Wani, M Maheswran, Ms. Jayashree
Department Of Computer Science,
Hindustan College Of Arts And Science,
Padur, Chennai,Tamil Nadu, India.
Syed.Hcas@Gmail.Com

***Abstract:*** This paper provides a background to fingerprint recognition, describes the biometric use of fingerprints, biometric standards and related security issues .and also discusses several Biometric scan technologies: finger-scan, facials can and retinal-scan. As accurate automatic personal identification is critical in a wide range of application domain such as ID cards, electronic commerce and automated banking and several other information repositories . Biometrics , which refers to automatic identification of persons based on his/her physiological or behavioral characteristics ,in inherently more reliable and more capable in differentiating between an authorized person and fraudulent imposter than traditional methods such as passwords and pin numbers. Automatic fingerprinting and other biometric aspects like face, voice, iris , etc are more reliable and secure and ways for identification and verification of person to claim the access to the information system. We have explored the fingerprint technique and also mentioned some other techniques which when accompanied with the fingerprint provides more powerful security to the system by granting identification to correct and verified access to the person by extracting some physical features from these physiological parts of the body to attain respective security traits (minutiae).

***Keywords*:** Biometric, identification, security, fingerprint, fingerprint standards, fingerprint classification, fingerprint enhancement, facial scan., retinal scan.

## I. INTRODUCTION

Personal identification is to associate a particular individual with an identity. It plays a critical role in our society in which questions related to the identity of individuals such as “Is this the person who he or she claims to be?”, ”Does this employee have authorization to perform this transaction ?”,etc. are asked millions of times every day by hundreds of thousand s of organizations in financial services, health care, electronic commerce, telecommunication, government etc. With the rapid evolution of information technology, people are becoming even more and more electronically connected. As a result, the ability to achieve highly accurate automatic personal identification is becoming more critical [1,2,3,4,5,18,6,20].
Traditionally two major types of automatic personal identification approaches have widely used :
i)knowledge- based and
ii)Token –based[5,6,18].
Token-based approach use “something you have” to make a personal identification. Individuals are identified by demonstrating that they are in possession of certain token, such as passport, license, ID card, and keys.

Knowledge-based approach use “something that you know” to make a personal identification. Individuals are identified by demonstrating that they are in possession of information or knowledge which only they themselves are expected to know such as password and PIN. The major advantage of these traditional personal identification approaches are that They are simple and They can be easily integrated into different systems with a low cost.

However , since these traditional approach are not based on any inherent attributes of an individual to make a personal identification , they have a number of disadvantages like tokens may be lost, stolen , forgotten, or misplaced ;PIN may be forgotten or guessed by the impostors. All of these approach are also unable to differentiate between an authorized person and an impostor who fraudulently acquires the “token” or “knowledge” of the authorized person [ 2,3,5,18].Therefore they are unable

to satisfy the security requirements of our electronically inter-connected information society.

## II. BIOMETRICS

Biometrics which refers to identifying an individual based on his physiological or behavioral characteristics (identifiers)[4,2,3,5,18],relies on “something which you are or you do” to make a positive personal identification. It is inherently more reliable and more capable than knowledge based and token-based techniques in differentiating between authorized person and a fraudulent impostor , because the physiological and behavioral Characteristics are unique to every person. Also the person to be
identified is required to be physically present at the point-of- identification .Biometrics provides a solution for the security requirements of our electronically interconnected information society has the potential to become the dominant automatic personal identification in the near future[4,5,18].

## III. BIOMETRIC SYSTEM

A biometric system is essentially a pattern recognition system which make a personal identification by determining the authenticity of a specific physiological or behavioral characteristics possessed by the user. The block diagram of

© 2010, IJARCS All Rights Reserved

a generic biometric system is depicted in figure1 Logically ,it can be divide into two modules:

i) Enrollment module and Identification module.

The enrollment module is responsible for enrolling individuals into the biometric system. During the enrollment phase , the biometric characteristics of an individual is first scanned by a biometric reader to produce a raw digital representation of the characteristics .In order to facilitate the matching ,the raw digital representation is usually further processed by a feature extractor to generate a compact but expressive representation , called a template. Depending on the application , the template may be stored in the central database of the biometric system or be recorded on a magnetic card issued to the individual . The identification module is responsible for identifying the individuals at the point of access . During the operation phase , the biometric reader captures the characteristic of the individual to be identified and converts it to a digital format, which is further processed by the feature extractor to produce the same representation. The resulting representation is fed to the feature matcher which compare it against the template (s)to establish the identity.

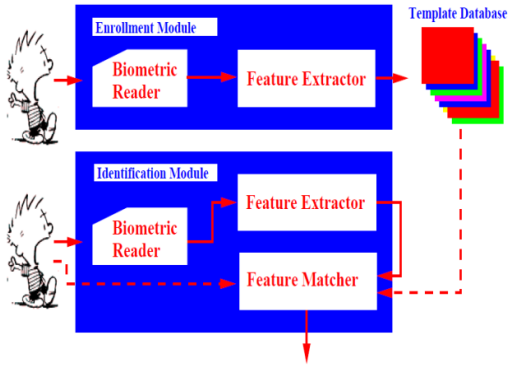


Figure.1The generic biometric system.

## IV. REQUIREMENT OF BIOMETRIC IDENTIFIERS

Any human physiology or behavioral characteristics can be used as a biometric characteristic or identifier to make a personal identification as long as it satisfies the following the requirements[2,18]:

i) **Universality,** which means that each person should have the characteristics.

ii) **Uniqueness,** which indicate that the no two persons should have the same characteristics.

iii) **Permanence,** which means that the characteristics should not be changeable, and

**iv) collectability ,** which indicates that the characteristics can be measured quantitatively.

However in practice , a biometric characteristic that satisfies all the above requirements may not always be feasible for a practical biometric system .In a biometric system there are a number of other issues which should be considered , including performance, acceptability, circumvention etc.

## V. OPERATION MODE

An important issue in designing a practical biometric system is to determine how an individual is identified. Depending on the application context, a biometric system may be either a verification (authentication)system or an identification system. A verification system authenticates a person's identity by comparing the captured biometric characteristic with its own biometric templates pre-stored in the system.

An identification system recognizes an individual by searching the entire template database for a match. It conducts one-to-many comparisons to establish the identity of the individual. In an identification system , the system establish a subject's identity(or fails if the subject is not enrolled in the system database).

## VI. APPLICATIONS

Biometrics is a rapidly evolving technology which has been widely used in forensics such as criminal identification and prison security, and has a very strong potential to be widely adopted in a broad range of civilian applications like banking, electronic commence , access control, welfare and immigration etc.

## VII. BIOMETRIC TECHNOLOGIES

It is believed that a physiological biometric characteristics is more reliable than a behavioral biometric characteristics, since a physiological biometric characteristics tends to have smaller interclass variation than behavioral biometric characteristics[18].

A biometric characteristic could be as we know either

i) a physiological characteristic or

ii) a behavioral characteristic .

Currently, there are mainly nine different biometric techniques that are widely used and some of them are under intensive investigation , including face , fingerprint, hand geometry, hand vein , iris, facial thermo gram, retinal pattern, signature and voice-print. signature and voice-print[8,2,9,4,5,17,10,16,11,12,15]

## VII. FINGERPRINT CLASSIFICATION

Global patterns of ridges and furrows in the central region of fingerprints from special configurations, which have certain amount of interclass variability . But these variations are sufficiently small which allows for a systematic classification of fingerprints. From the overall fingerprint only a portion of a fingerprint, called *pattern area* is of interest[13]. The pattern area of the fingerprint consists of those ridges encircled by typelines , which is defined as the two innermost ridges that form a divergence tending to circle portion of the fingerprint (fig.2)[13 ]. The pattern area of the loop or whorl types of fingerprints contain two types of singular points (i) *delta* and (ii)*core*. The *delta*, outer terminus, defined as the point of ridge at or in front of and nearest to the center of divergence of the typelines. The *core* , sometimes called the inner terminus ,is defined as the specific point located on or within the innermost sufficiently curved ridges.

Typelines

© 2010, IJARCS All Rights Reserved

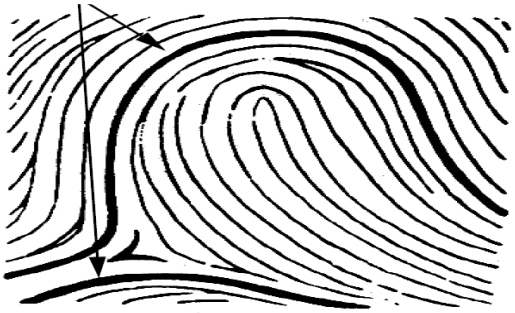

Figure.2 Pattern area and typelines

Another important point or concept in both fingerprint classification and fingerprint matching is ridge count, which may be roughly defined as the number of ridges that touch or cross an imaginary line drawn between the core and delta.[ 1 ]

## VIII. HENRY CLASSIFICATION

The Henry Classification System organizes ten-print fingerprint records by pattern type.Finger ridges and patterns can be continuous, interrupted, forked, and other formations. Fingerprints are classified and identified by the relationship of these formations, described as minutiae. These patterns are divided into five basic groups, with various subgroup[34];

Arch: a ridge that runs across the fingertip and curves up in the middle. Tented arches have a spiked effect.

Whorl: an oval formation, often making a spiral pattern around a central point. Principal types are a plain whorl and a central pocket loop whorl.

Loops: These have a stronger curve than arches, and they exit and enter the print on the same side. Radil loops slant toward the thumb and ulnar loops away from the thumb.

"Composites" are a mix of other patterns;

"Accidentals" form an irregular pattern that's not classifiable as an Arch, Loop or Whorl.

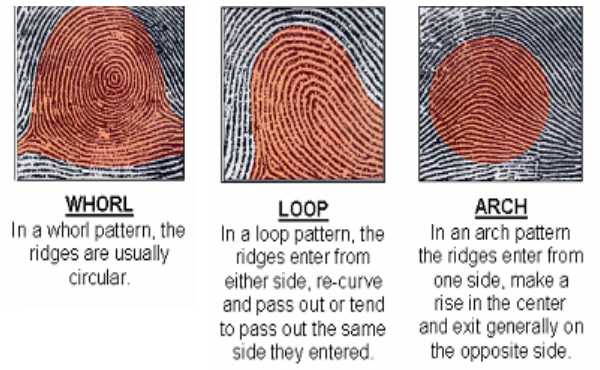


Figure.3

In addition to the above patterns there are many other types as well like shown in fig. below


Figure.4

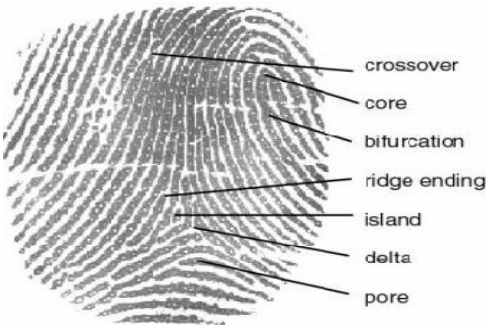


Figure.5

## IX. FINGERPRINT MATCHING

The fingerprint matching depends on the comparison of local ridge characteristics and their relationships to determine the individuality of fingerprint. These local ridge characteristics are not evenly distributed. Most of them depend heavily on the impression conditions and quality of the fingerprints. The two most prominent ridge characteristics called minutiae ,are (i) *ridge ending* and(ii) *ridge bifurcation* .

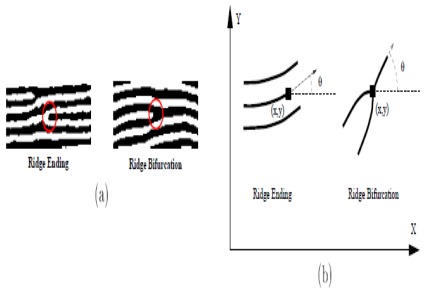


Figure.6

Minutiae: (a) example of minutiae ; (b) characterization of minutiae If two fingerprints belong to the same category and have a sufficient number of minute details that are identical ,then it can be concluded confidently that they are of same finger. But, generally in order to determine whether the two fingerprints are same ,four factors must be evaluated[ 1 ],(i)general pattern configuration(ii)qualitative concordance means corresponding minute details must be same ,(iii) quantitative factor and (iv) relationship of minute details.

© 2010, IJARCS All Rights Reserved

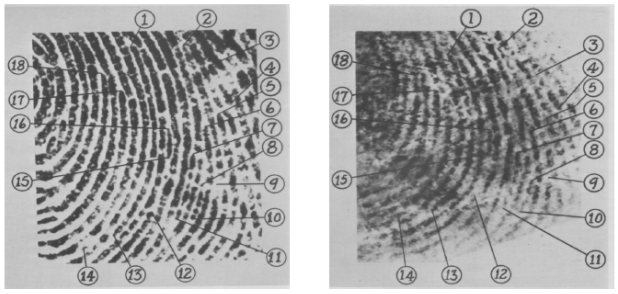

Figure.7 Fingerprint matching result in which 18 identical minute details are identical[ 21 ]

Different biometric characteristics possess different discrimination capability in terms of system accuracy .At the one extreme ,we have a biometric characteristics such as face and dynamic signature to prove the genuine access but and individual mat be easily mistaken due to change in makeup, hairstyle, lightning conditions, background etc , But to combat this we have fingerprint scan and retinal-scan. That are inherently better to prove the individuality of the person . somewhere in between these two extremes are those biometric characteristics such as hand geometry and hand vein which perform the same in deterring imposters and accepting genuine individuals.[ 18 ].

A biometric system may operate either in(i) verification mode or (ii) identification mode. it is more difficult to design an identification system than to design a verification system[ 18 ]. For verification systems , the major challenge is the system accuracy .It is usually not difficult to meet the response time requirements in a verification system, because only one-to-one comparison is conducted .however ,for identification system, both accuracy and speed are critical .An identification system needs to explore the entire template database to establish an identity .Thus more requirements are imposed on the feature extraction**[ 1 ]**.Fingerprint classification may provide a partial to index a fingerprint database. Although a significant progress has been made in the fingerprint identification, still it is not possible to conduct a real time search even on small size fingerprint database is several thousand images without dedicated hardware matches and an efficient indexing mechanism .On the other hand ,it Is feasible to design to a face recognition system operating in the identification mode ,because (i) face comparison is a relatively less expensive operation, and (ii) efficient indexing techniques are available and the recognition performance is admissible**[14]**.

Choosing the operational mode for a biometric system depends mainly on the practical requirements. Identification system usually requires more resources ,hence most expenditures .

Data acquisition in one of the critical process in the biometric system. The quality of the required data determines the performance of the entire system. However the selection of a data acquisition device depends on the practical requirements such as availability, cost and size. There in no thumb rule to determine which device should be used**[ 1 ]**.

## X. ALGORITHM LEVEL DESIGN

The major tasks in the algorithm level design are(i) feature extraction and(ii) matching. Feature extracting is responsible for extraction of representative features from the raw input data. Matching is responsible for determining whether two sets of representative features are extracted from the same resource .The Algorithm level design also consists of other modules such as database management quality control, encryption, and user interface.

The fingerprint representation(feature) constitutes the essence of the algorithm level design and determines almost all aspects of the recognition mechanism. A representation should have the following two properties.(i) Saliency and(ii) suitability. Saliency means that a representation should contain enough class-specific (individual) information about the input data. Suitability mean that the representation can easily be extracted ,stored in a compact fashion, and is useful for matching.

Below in the designed prototype verification system which uses only fingerprints in identity authentication – conducts only one-to-one comparison to authenticate whether identity clamed by and individual is true or not[ 1 ]. This prototype is designed for the applications like ATM card security ,smart card security , information system security, and various access control mechanisms. Logically this system consists of four major parts or components (i) user interface (ii)system database (iii) enrollment module and (iv) verification module. The user interface provides interface provides the user the way to indicate his identity and present his fingerprint or other biometric feature to system, usually for accepting the fingerprint live-scan fingerprint images are used .The database consists of a collection of records associated with each user who has access to the system(fig)

The task of verification module is to authenticate the identity of an individual who intends to access the system. The individual to be authenticated indicates his identity and places her finger on the fingerprint scanner: a digital image of his fingerprint is captured : minutiae is extracted from the captured fingerprint image and fed to a minutiae matching algorithm which matches it with the individual's stored minutiae template in the database to authenticate whether his identity is clamed or not.

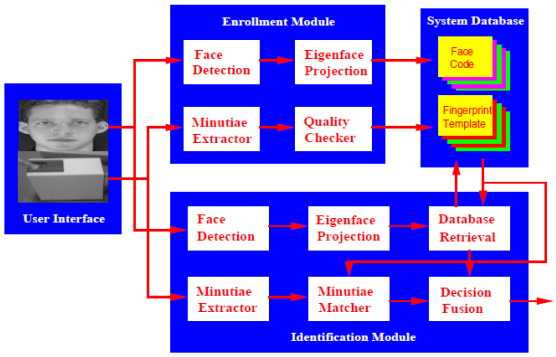


Figure.8. system structure of the prototype integrated biometric identification system

## XI. DIFFICULT PROBLEMS

While a significant progress has been made in automatic fingerprint identification, there are still a number of research issues which need to be addressed to improve the

© 2010, IJARCS All Rights Reserved

performance and maintenance of the secured system with great ease, following are few issues:

- Robust live-scan fingerprint scanner
- Fingerprint feature extractor
- Minutiae matching.
- Fingerprint enhancement.
- Fingerprint classification.
- Fingerprint compression.
- Computational complexity of matching.
- Integration of multiple biometrics characteristics .
- Performance evaluation.

These all the above mentioned issues are correlated with each other **[ 1 ]**.

## XII. MINUTIAE EXTRACTION

Minutiae extraction is to extract representative features, called minutiae, from the input fingerprint images. For automatic fingerprint matching ,a silent and suitable representation of the input fingerprint images is critical. Generally this representation should have the following properties[19] (i) retain discriminating power of raw digital fingerprint images, (ii) compactness, (iii) amendable to matching algorithms ,(iv) robust to noise and distortions and (v) ease to compute.[ 19].

The pattern of the minutiae of the fingerprint forms a valid representation of the fingerprint. In an automatic fingerprint matching, only the two most prominent types of minute details are used for stability and robustness: (i) ridge ending and (ii) ridge bifurcation . So typically in a live-scanning fingerprint image of good quality there are about 50-100 minutiae**[ 1 ]**.

Several other Fingerprint readers can employ several techniques. The principal methods are:

(i) Capacitive and, (ii) Optical

### *A. Capacitive*

Capacitive readers measure the differences in electrical signals generated by the valleys and ridges of fingerprints when presented to the reader. Capacitive readers use a sensor that measures conductivity of a large number of points over the surface of the sensor. Limited by the size of the human finger, sensors measure approximately 15 x 20mm. Grids embedded in the sensors create discrete points of measurement, sometimes described as pixels. For example, in a sensor 12.8 x 18.0 mm in size contains a grid of 256 x 360 pixels[32]

Active capacitive sensing is considered to have a high tolerance for parasitic effects compared to passive capacitive sensing, thus improving accuracy.

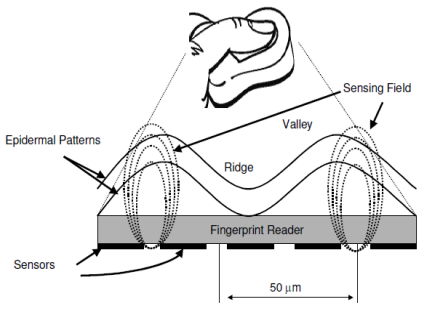


Figure.9 . Capacitive reader

A key advantage of a capacitive reader is the requirement for a fingerprint-type shape, rather than an image. This can be a defense to spoofing. Based on semiconductor chips, capacitive readers can have a price advantage and be more compact than optical devices.

### *B. Optical*

Optical readers use either a complementary metal oxide semiconductor (CMOS) device or, more commonly, a charge coupled device (CCD), similar to the devices used in digital cameras. A fingerprint scanner typically has its own light source, usually a light-emitting diode (LED) array.

Currently, CMOS image sensors offer lower power consumption (up to a factor of 100) and more on-chip functionality. They are also often found in high volume, portable applications such as camera cellular phones, PDAs and some digital cameras[30]**.**

## XIII. OTHER TECHNOLOGIES

### *A. Other sensing technologies include[31]:*

*a. Radio Frequency (RF):* which seeks a live skin layer thus incorporating a "liveness" test; · Thermal; measuring temperature differences between the ridges and valleys on the fingerprint.

*b. Piezo-Resistive:* also known as piezo-electric and which detect finger pressure. More commonly used to detect tapping or key entry patterns.

*·c. Ultrasonic:* or acoustic sensors measuring differences in reflected sound when the fingertip is presented to the sensor. This is usually very high frequency such as 50 MHz; and

*· d. Micro-Electrical Mechanical Systems (MEMS):* These are devices that integrate electronic and mechanical components, usually onto a single substrate.

Examples also include ink-jet printer heads, blood pressure sensors, accelerometers and pressure sensors. MEMS can include a variety of sensor technologies, including those outlined above. The sensing technologies described above are being continually developed and may, in the future, take a place alongside capacitive and optical designs.

## XIV. FINGERPRINT ENHANCEMENT

The performance of the currently available minutiae extraction algorithm depends heavily on the quality of the inputs images. In an ideal fingerprint image, ridges can be easily detected and minutiae can be precisely located from the thinned ridges[ 1 ]. However in practice ,due to the factors mentioned earlier, a significant percentage of acquired fingerprint images(approx. 10% ) is of power quality[ 1 ]. The ridge structure which is in poor-quality fingerprint images are not always detected easily and correctly. This leads the following problems:(i) a significant number of surplus minutiae may be created,(ii) large percentage of genuine minutiae may be ignored and, (iii) large errors in there localization(position and orientation) may be introduced.

Fingerprint enhancement can be conducted on either(i) *binary images* or *grey images*. The improvement in clarity of the ridges of fingerprint is recoverable by the implementation of the algorithm which intern makes the fingerprint suitable for minutiae extraction algorithm[ 1 ].

© 2010, IJARCS All Rights Reserved

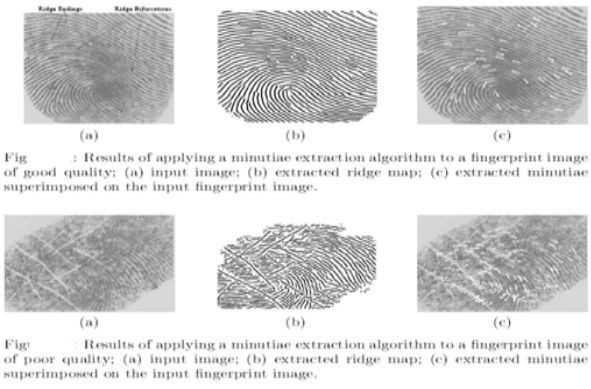


Fig : Results of applying a minutiae extraction algorithm to a fingerprint image of good quality; (a) input image; (b) extracted ridge map; (c) extracted minutiae superimposed on the input fingerprint image.

Fig : Results of applying a minutiae extraction algorithm to a fingerprint image of poor quality; (a) input image; (b) extracted ridge map; (c) extracted minutiae superimposed on the input fingerprint image.

Figure.10

## XV. DECISION FUSION

A biometric system can be either based on the single characteristics or and multiple biometric characteristics in order to increase accuracy in both verification and identification of the individual while calming access to the secure system. The multimode biometrics increases only the accuracy in verification and not the verification speed**[ 1 ]**.

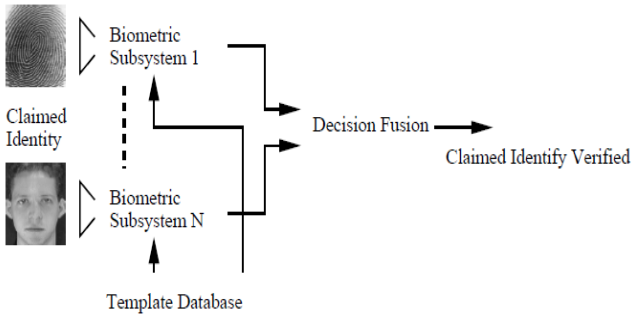


Figure.11. A generic multimodal variation system

The implementation of biometric modes whether single orintegrated depends only on the application domain.

## VVI. OTHER BIOMETRIC APPLICATIONS

### *A. Facial-Scan Technology*

With facial recognition technology, a digital video camera image is used to analyze facial characteristics such as the distance between eyes, mouth or nose. These measurements are stored in a database and used to compare with a subject standing before a camera[22]. Facial recognition systems are usually divided into two primary groups. First there is what is referred to as the '*controlled scene'* group whereby the subject being tested is located in a known environment with a minimal amount of scene variation. In this case, a user might face the camera, standing about two feet from it. The system locates the user's face and perform matches against the claimed identity or the facial database. The system usually comes to a decision in less than 5 seconds[23]. The other group is known as the "*random scene*" group where the subject to be tested might appear anywhere within the camera scene. This situation might be encountered within a system attempting to identify the presence of an individual within a group or crowd. Facial-scan technology is based on the standard biometric sequence of image acquisition, image processing, distinctive characteristic location, template creation, and matching[24]. An optimal image is captured through a high-resolution camera, with moderate lighting and users directly facing a camera. [25]Lighting conditions, which cause an image to be underexposed or underexposed, can cause challenges. Additionally, users with a darker skin tone can be difficult to acquire. Color images are normally reduced to a black and white and images cropped to emphasize facial characteristics [26]. Changes in hairstyle, makeup or the wearing of a hat or sunglasses may pose a problem during the verification process. Facial-scanning technology has a poor record in verifying a subject who has had plastic surgery to alter their appearance.

### *B. Retinal-Scan Technology*

The last biometric technology to discuss is retinal scanning. Retina-scan technology makes use of the retina, which is the surface on the back of the eye that processes light entering through the pupil. *Retinal Scan technology is based on the blood vessel pattern in the retina of the eye*. The principle behind the technology is that the blood vessels at the retina provide a unique pattern, which may be used as a tamper-proof personal identifier[27]. Since infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue, it is used to illuminate the eye retina. Retina-scan devices are used exclusively for physical access applications and are usually used in environments that require high degrees of security such as high-level government military needs.

Retina-scan technology image acquisition is difficult in that the retina is small and embedded, requiring specific hardware and software. The user positions his eye close to the unit's embedded lens, with the eye socket resting on the sight. In order for a retinal image to be acquired, the user must gaze directly into the lens and remain still, movement defeats the acquisition process requiring another attempt.[28] A low intensity light source is utilized in order to scan the vascular pattern at the retina[29]. Normally it takes 3 to 5 acceptable images to ensure enrollment. Because of this, the enrollments process can be lengthy. Enrollments can take over 1 minute with some users not being able to be enrolled at all[27]. Retina-scan technology has its advantages and disadvantages. Among its advantages are its resistance to false matching or false positives and the fact that the pupil, like the fingerprint remains a stable physiological trait throughout ones life.. Well-trained users find retina scan capable of reliable identification. Like fingerprints, retina traits remain stable throughout life.Retina-scan enrollments take longer than both iris-scan and fingerprinting [32]. Users claim discomfort with the fact that they must position their eye very close to the device.

## VII. IN CONCLUSION

Fingerprints have been widely used as a form of identification for many years and are well established in many cultures, countries and jurisdictions. The biometric use of fingerprints continues to grow as sensor technology improves, prices fall and supporting systems are enhanced. But sometimes it is not the only solution to secure the system alone other biometric application are also accompanied like face recognition , retinal , voice ,irs etc. to

© 2010, IJARCS All Rights Reserved

prove the worthiness of the system. While much publicity has been afforded to the spoofing of fingerprint sensors, this is only one of the security concerns with biometric identification and authentication systems. Biometrics allow for increased security, convenience and accountability while detecting and deterring fraud. Biometrics, however, are not suitable for every application and is some situations biometric identification may be the wrong solution. One of the continuing challenges for the biometric industry is to define the environment in which the technology provides the strongest benefit to individuals and institutions. For the security officer, the challenge will be to demonstrate to upper management that the costs associated with deployment outweigh the risks and costs.

**Endnotes**


1. Lin Hong, Automatic personal identification implementing fingerprint,1998
2. R. Clarke. Human Identification systems: Management challenges and public policy issues. Information technology & People,7(4):6-37,1994
3. S. G. Davies. Touching big brother :How Biometric technology will fuse flesh and machine. Information Technology & People,7(4):60-69,1994
4. J Campbell Jr.,L. Alyea, and J. Dunn, Biometric Security : Government application and operations. http:/www.vitro.bloomington.in.us:8080/~BC/,1996.
5. B Miller. Vital signs of identity .IEEE Spectrum,31(2):22-30,1994
6. National Institute of Standards and Technology. Guideline for The use of Advanced Technology Alternatives ,Federal Information Processing Standards Publication 190,1994
7. Biometrics Consortium homepage.INS Passenger Accelerated Service System (INSPASS).http://www.accentdesign.com/bc/publication.html,1998.
8. J. Atick,P. Griffin, and A.Redlich. Statistical approach to shape from shading: Reconstruction of 3D face surfaces from single 2D images. Neural Computation,1998. To appear.
9. J. G. Daugman . High confidence visual recognition of person by a test of statistical independence .IEEE Trans Pattern Anal. And Machine Intell.,15(11):1148-1161,1993.
10. J. Ferrante,J Maier,J. Nelson , and J Woodard .Automated entry control: Radc technology development results and future plans. In proc. Int. Carnahan Conf. on Electronic Crime Countermeasures, Pages 77-82,University of Kentucky,Lexington,Kentucky,1981.
11. Jr. j. Campell Speaker recognition :A tutorial .Proceedings of IEEE, 85(9):1437-1462,1997.
12. V. Nalwa. Automatic on-line signature verification. Proceedings of IEEE,85(2):213-239,1997.
13. Fereral Bereau Of Investigation. The Science Of Fingerprints: Classification and uses. U.S. Govt. Printing office, Washington,D.C.,1984.
14. D. L. Swets and J. Weng. Using discrimint egenfeatures for images retrival. IEEE Trans. PAMI, 18(8):831-836,1996.
15. R. Wildes. Iris recognition: An emerging biometric technology. Proceedings of IEEE,85(9):1348-1363,1997.
16. J Zhang,Y Yan, and M. lades. Face recognition :Eignface, elastic matching, and neural nets. Proceedings of IEEE,85(9):1423-1436,1997.
17. TRS. Technology Recognition Systems Homopage. http:/www.betac.com/trs/,1998.
18. E. Newham. The Biometric Report. SJB Services ,New York, 1995.
19. N. Ratha S. Chen and A K Jain. Adoptive flow orientation based feature extraction in fingerprint images. Pattern Recognition,28(11):1657,1995.
20. J. Woodward. Biometrics: Privacy's foe or privacy's friend? Proceedings of IEEE,85(9):480-1492,1997.
21. A. Moenssens. Fingerprint Techniques. Chilton Book Company1971.
22. Manoj Gupta, Biometric Technologies Overview, SANS Reading Room, http://rr.sans.org/authentic/biometric2.php.
23. Manoj Gupta, Biometric Technologies Overview, SANS Reading Room, http://rr.sans.org/authentic/biometric2.php.
24. Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 65.
25. Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 69.
26. Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 74
27. Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag, p. 108.
28. Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 74
29. Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag, p. 60.
30. Capturing an Image, Eastman Kodak Company, http://wwwdk.kodak.com/global/en/corp/historyOfKodak/capturingAnImage.jhtml , accessed 12 February 2006.
31. Solid State Fingerprint Scanners - A Survey of Technologies, Philip D. Wasserman, NIST, 26 December 2005, http://www.itl.nist.gov/iad/894.03/pact/SSFS_113005.pdf.
32. Sensors, UPEK, Inc., http://www.upek.com/products/sensors.asp #Table2, accessed 19 February 2005.
33. K Karu and A K Jain. Fingerprint patterns. Compute Vision Graphics Image Process.37(4):362-385,1987.
34. All About Fingerprints, Chapter 4 - The Techniques, http://www.crimelibrary.com/criminal_mind/forensics/fingerprints/4.html, accessed 02 December 2005.


© 2010, IJARCS All Rights Reserved