ISSN:0975-9646
Sanjay Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1595-1597

# Analysis of various Biometric Techniques

Mr. Sanjay Kumar[1], Dr. Ekta Walia [2]

[1] *Department of Computer Science & Engineering, Maharishi Markandeshwar University Mullana, Ambala, Haryana, India*

[2] *Department of Information Technology, Maharishi Markandeshwar University Mullana, Ambala, Haryana, India*

***Abstract*— Biometrics is automated methods for identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic has the capability to reliably distinguish between an authorized person and an imposter. Since biometric characteristics are distinctive, can not be forgotten or lost, and the person to be authenticated needs to be physically present at the point of identification, biometrics is inherently more reliable and more capable than traditional knowledge-based and token-based techniques. Using biometrics for identifying human beings offers some unique advantages. Biometrics can be used to identify you as you. Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications. This paper provides an overview of the different biometric technique with some advantages and disadvantages. Than we will try to find out which technique is more reliable and secure.**

***Keywords*— Biometric, False Reject Rate (FRR), False Acceptance Rate (FAR).**

## I. INTRODUCTION

Biometrics, which refers to identifying an individual based on his or her physiological or behavioral characteristics.

Physiological characteristics include hand or finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, voice verification, and keystroke dynamics.

There is no one "perfect" biometric that fits all needs. All biometric systems have their own advantages and disadvantages. There are, however, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. There is a great deal of scientific data supporting the idea that "no two fingerprints are alike." Technologies such as hand geometry have been used for many years and technologies such as face or iris recognition have come into widespread use. Some newer biometric methods may be just as accurate, but may require more research to establish their uniqueness. Another key aspect is how "user-friendly" a system is. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner. Low cost is important, but most implementers understand that it is not only the initial cost of the sensor or the matching software that is involved. Often, the life-cycle support cost of providing system administration and an enrollment operator can overtake the initial cost of the biometric hardware. The advantage biometric authentication provides is the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users.

Biometrics has been widely used in forensics applications such as criminal identification and prison security. The biometric technology is rapidly evolving and has a very strong potential to be widely adopted in civilian applications such as electronic banking, e-commerce, and access control. Due to a rapid increase in the number and use of electronic transactions, electronic banking and electronic commerce are becoming one of the most important emerging applications of biometrics. These applications include credit card and smart card security, ATM security, check cashing and fund transfers, online transactions and web access. The physical access control applications have traditionally used token-based authentication. With the progress in biometric technology, these applications will increasingly use biometrics for authentication [2].

Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). During Enrollment, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison. Biometric recognition can be used in Identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. A system can also be used in Verification mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching [6].

## II. TYPES OF BIOMETRICS

### *A. Face Recognition*

The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Several approaches to modeling facial images in the visible spectrum are Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis.

Some of the challenges of facial recognition in the visual spectrum include reducing the impact of variable lighting and detecting a mask or photograph. Some facial recognition systems may require a stationary or posed user in order to capture the image, though many systems use a real-time process to detect a person's head and locate the face automatically. Major benefits of facial recognition are that it is non-intrusive, hands-free, continuous and accepted by most users [1].

### *B. Voice Recognition*

Voice recognition has a history dating back some four decades, where the output of several analog filters were averaged over time for matching. Voice recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). This incorporation of learned patterns into the voice templates (the latter called "voiceprints") has earned speaker recognition its classification as a "behavioral biometric." Voice recognition systems employ three styles of spoken input: text-dependent, text-prompted and text independent. Most voice verification applications use text-dependent input, which involves selection and enrollment of one or more voice passwords. Text-prompted input is used whenever there is concern of imposters. The various technologies used to process and store voiceprints includes hidden Markov models, pattern matching algorithms, neural networks, matrix representation and decision trees. Performance degradation can result from changes in behavioral attributes of the voice and from enrollment using one telephone and verification on another telephone. Voice changes due to aging also need to be addressed by recognition systems. Many companies market voice recognition engines, often as part of large voice processing, control and switching systems. Capture of the biometric is seen as non-invasive. The technology needs little additional hardware by using existing microphones and voice-transmission technology allowing recognition over long distances via ordinary telephones (wire line or wireless) [4].

### *C. Iris Recognition*

This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought unique. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes (in systems performing one-to-many searches in a database). Current systems can be used even in the presence of eyeglasses and contact lenses. The technology is not intrusive. It does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities [4].

### *D. Hand and Finger Geometry*

These methods of personal authentication are well established. Hand recognition has been available for over twenty years. To achieve personal authentication, a system may measure either physical characteristics of the fingers or the hands. These include length, width, thickness and surface area of the hand. One interesting characteristic is that some systems require a small biometric sample (a few bytes). Hand geometry has gained acceptance in a range of applications. It can frequently be found in physical access control in commercial and residential applications, in time and attendance systems and in general personal authentication applications [3].

### *E. Signature Verification*

This technology uses the dynamic analysis of a signature to authenticate a person. The technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e-business applications and other applications where signature is an accepted method of personal authentication [4].

### *F. Fingerprints*

The patterns of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement has been classifying and determining identity by matching key points of ridge endings and bifurcations. Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available, users no longer need to type passwords – instead, only a touch provides instant access. Fingerprint systems can also be used in identification mode. Several states check fingerprints for new applicants to social services benefits to ensure recipients do not fraudulently obtain benefits under fake names [5].

Fingerprints are the ridge and furrow patterns on the tip of the finger and have been used extensively for personal identification of people. The biological properties of fingerprint formation are well understood and fingerprints have been used for identification purposes for centuries. Since the beginning of the 20th century, fingerprints have been extensively used for identification of criminals by the various forensic departments around the world. Due to its criminal connotations, some people feel uncomfortable in providing their fingerprints for identification in civilian applications. However, since fingerprint-based biometric systems offer positive identification with a very high degree of confidence, and compact solid state fingerprint sensors can be embedded in various systems (e.g., cellular phones), fingerprint-based authentication is becoming more and more popular in a number of civilian and commercial applications such as, welfare disbursement, cellular phone access, and laptop computer log-in. The availability of cheap and compact solid state scanners as well as robust fingerprint matchers are two important factors in the popularity of fingerprint-based identification systems. Fingerprints also have a number of disadvantages as compared to other biometrics [7].

## III. Comparative Study of Different Biometric Techniques

TABLE I

ADVANTAGE AND DISADVANTAGE OF BIOMETRIC TECHNIQUES

| Method | Advantage | Disadvantage |
|---|---|---|
| Finger print Verification | • High Reliability<br>• Robust<br>• Highly Distinctive<br>• Proven Accuracy<br>• Advanced Technology<br>• User Convenience<br>• Uniqueness<br>• Stable over time | • Injury can affect<br>• Dry skin can cause difficulties<br>• Poor environment |
| Hand Geometry | • Small Template<br>• Unaffected by skin condition | • Size of Scanner<br>• Injury can affect<br>• Low Distinctiveness |
| Face Recognition | • Efficient Process<br>• High Acceptance | • Face change over time<br>• Can be manipulated by surgery<br>• Cannot be distinguish between twins<br>• Religious or Cultural inhibitions<br>• Poor environment |
| Iris Scanning | • Uniqueness<br>• Robust<br>• Highly Distinctive | • Complex Processor<br>• High Cost<br>• Poor environment<br>• Relatively new technology<br>• Affected with diabetes |
| Voice Recognition | • High level of user acceptance<br>• High Acceptance<br>• Low training requirement | • Voice and language change over time<br>• Easy to manipulate<br>• Low Accuracy<br>• Poor environment<br>• Flu or Throat infection |
| Signature Recognition | • High user acceptance<br>• Low training requirement | • Unstable over time<br>• Changes over time<br>• Low distinctiveness |

TABLE III

IMPLICATION OF ERROR RATES [2]

| Method | False Reject Rate | False Acceptance Rate |
|---|---|---|
| Finger print | 3 to 7 in 100 (3-7%) | 1 to 10 in 100,000 (.001-.01%) |
| Face Recognition | 10 to 20 in 100 (10-20%) | 100 to 1000 in 100,000 (.1-1%) |
| Voice Recognition | 10 to 20 in 100 (10-20%) | 2000 to 5000 in 100,000 (2-5%) |
| Iris | 2 to 10 in 100 (2-10%) | >=.001% |
| Hand Geometry | 1 to 2 in 100 (1-2%) | 10 to 20 in 1000 (1-2%) |
| Signature | 10 to 20 in 100 (10-20%) | 2-5% |

## IV. Conclusion

Above mentioned difference and implication of error rates of different biometric techniques conclude that the finger print is fast and accurate biometric technique for more reliable and secure system.

## References

[1] George Chellin Chandran. J, Dr. Rajesh. R. S., "Performance Analysis of Multimodal Biometric System Authentication". IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009

[2] Phillips et al., "An Introduction to Evaluating Biometric Systems, Guide to Biometrics", IEEE Computer, February 2000,pp 56-63.

[3] A. K. Jain, A. Ross, and S. Pankanti, "A Prototype Hand Geometry-Based Verification System", 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication, Washington D.C., pp. 166-171, March 22-24, 1999.

[4] Salil Prabhakar, "Fingerprint classification and matching with filterbank", Ph.D Thesis, University of Michigan State, 2001.

[5] Robert Carrigan, Ron Milton, Dan Morrow, "Automated fingerprint identification systems", Technical Report by Computer world honors case study, 2005.

[6] K. Zebbiche, F. Khelifi, and A. Bouridane1, "An Efficient Watermarking Technique for the Protection of Fingerprint Images", Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2008, Article ID 918601, 20 pages.

[7] Tabassam Nawaz, Saim Pervaiz, Arash Korrani, Azhar-Ud-Din, "Development of Academic Attendence Monitoring System Using Fingerprint Identification", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.5, May 2009.