An Overview of Biometrics Methods'

Akshatha M A[1], Athitha M A[2], Ashwini B[3]

[1, 2] Computer Science Engineer, Mysuru, Karnataka, India

[3]Assistant Professor, Department of CS&E, MIT Mysuru, Karnataka, India

Abstract: ***Biometrics refer to metrics related to human characteristics and traits. It is a science of measuring and statistically analysing data. It is one of the most widely used authentication technique that rely on the measurable physical characteristics. Usually collected biometric data will be encrypted to prevent misuse of data. In this paper we are going discuss some of methods used in Biometrics. Also we are going to study advantages and issues of Biometrics.***

Keywords: Biometrics, Authentication, Security, Technology.

1. Introduction

Biometrics is an authentication mechanism that relies on the automated identification or verification of an individual based on unique physiological or behavioural characteristics. Physiological characteristics refer to inherited traits that are formed in the early embryonic stages of human development. Typical physiological features measured include an individual's fingerprints, face, retina, iris and hand. Behavioural characteristics are not inherited, but learned. Typical behavioural features that can be measured include voice patterns, handwriting and keystroke dynamics. Biometric technologies offer two means to determine an individual's identity: verification and identification. Verification confirms or denies a person's claimed identity by asking, "Is this person whom he/she claims to be?" Identification, also known as recognition, attempts to establish a person's identity by asking, "Who is the person?" Verification is a one-to-one comparison of the biometric sample with the reference template on file. A reference template is the enrolled and encoded biometric sample of record for a user. Identification makes a one-to-many comparison to determine a user's identity. It checks a biometric sample against all the reference templates on file. If any of the templates on file match the biometric sample, there is a good probability the individual has been identified. [1]

A. Need for Biometrics

In the present times, when most transactions - financial or otherwise-are automated and many of them networked, security has emerged as a most important issue. Security is usually in the form of possessions (like ID cards, keys) or secret knowledge (like password, PIN). This type of security is not failsafe as for example, ID cards may be lost; passwords may be forgotten or compromised. A strong need was thus felt for more robust authentication methods and extensive research ensued in this area. This led to the concept of using human body parts or human mannerism itself as security and authentication measure, and finally to the emergence of biometrics as a field by itself. It is now widely accepted that any positive identification of a person must include biometric identification [2]

B. Basic Characteristics of Biometrics

Any aspect of human physiology or behavior that can be accepted as a biometric should satisfy seven properties described as follows:

- Uniqueness is considered as the priority one requirement for biometric data. It will indicate how differently and uniquely the biometric system will be able to recognize each user among groups of users. For instance, the DNA of each person is unique and it is impossible to replicate.
- Universality is the secondary criteria for the biometric security. This parameter indicates requirements for unique characteristics of each person in the world, which cannot be replicated. For example, retinal and iris are characteristics will satisfy this requirement.
- Permanence parameter is required for every single characteristic or trait which is recorded in the database of the system and needs to be constant for a certain period of time period. This parameter will mostly be affected by the age of the user.
- Collectability.The collectability parameter requires the collection of each characteristic and trait by the system in order to verify their identification
- Performance is the next parameter for the system which outlines how well the security system works.
- The accuracy and robustness are main factors for the biometric security system. These factors will decide the performance of the biometric security system. The acceptability parameter will choose fields in which biometric technologies are acceptable.
- Circumvention will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process. DNA is believed to be the most difficult characteristic leading to the failure of the verification process.[3]

2. Types of Biometrics

Methods used in biometrics can be classified based on physiological or behavioural traits being used by system for validation. The methods involved in physiological method are Finger print technology, Face recognition, hand recognition, Retinal scan and Iris scan. The methods used in Behavioural method are Keystroke recognition, signature validation and voice recognition. We are going to discuss each method in the following.

a) Finger Print Technology

Our fingerprint is made of a number of ridges and valley on the surface of finger that are unique to each human. "Ridges are the upper skin layer segments of the finger and valleys are the lower segments". The ridges form two minutiae points: ridge endings-where the ridges end, and ridge bifurcations-where the ridges split in two. The uniqueness of a fingerprint can be determined by the different patterns of ridges and furrows as well as the minutiae points. There are basic patterns (Fig 1) which make up the fingerprint: the arch such as tented and plain arch covers 5% of fingerprint; left and right loop covers 60% of fingerprints; whorl covers 34% of fingerprints and accidental whorls covers 1% of fingerprints. To capture the surface of the fingerprint for verification during the identification of users, new technologies are designed with tools such as: optical and ultrasound

Figure 1: Fingerprint scanner

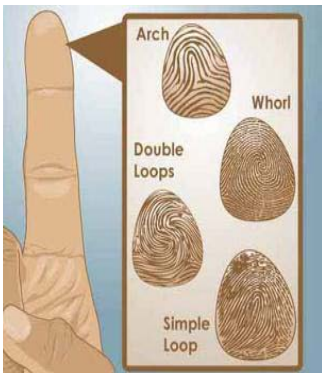

Figure 2: Basic patterns in Fingerprint

There are two main algorithms which are used to recognize fingerprints: minutiae matching and pattern matching. Minutiae matching will compare the details of the extract minutiae to identify the difference between one users fingerprint as compared to others. When users register with the system, they will record images of minutiae location and direction on finger surface. When users use fingerprint recognition system to verify their identification, a minutiae image is brought out and compared with the one which provided at the time of access. Pattern matching will compare all the surfaces of the finger instead of one particular point. It will concentrate more in thickness, curvature and density of finger's surface. The image of the fingers surface for this method will contain the area around a minutiae point, areas with low curvature radius or areas with unusual combinations of ridges. [3]

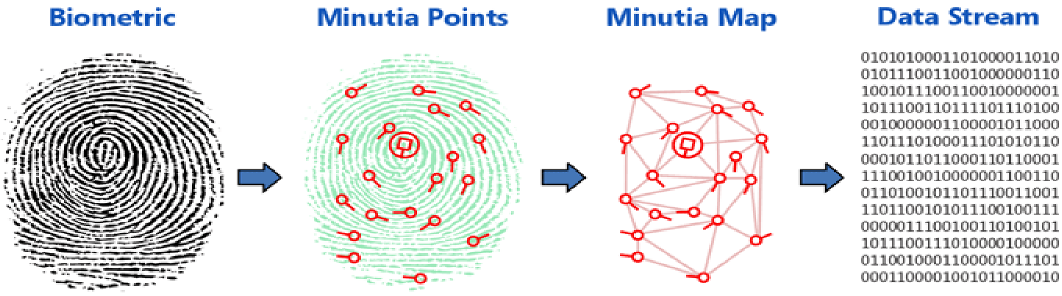

Figure 3: Minutiae matching in Fingerprint Technology

Figure 4: Pattern matching in Fingerprint Technology

b) Hand Geometry

In hand recognition, the geometric features of the hand such as the lengths of fingers and the width of the hand are measured using a charged couple device camera (CCD) and various reflectors and mirrors.

Black and white pictures of

i) An image of the top of the hand
ii) An image of the side of the hand are captured.

Unique features in the structure of the hand such as finger thickness, length and width, the distances between finger joints, the hand's overall bone structure, etc. are also recorded. To enroll, the user places his or her hand onto a platen three different times; three images are captured and averaged. The resulting image forms the basis for the enrolment template, which is then stored in the database of the hand geometry scanner. The enrolment phase can be completed within five seconds. In the verification phase, the user is prompted to place his/her hand only once on the platen. An image is captured, and forms the basis for the verification template. The verification template is compared against the enrolment template, in the same fashion as fingerprint recognition. The verification phase can be accomplished in just under one second .This technology is mostly used in physical access entry applications. [2]

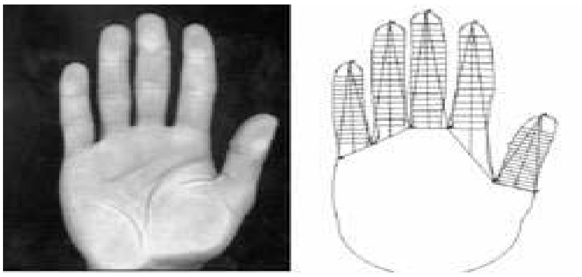

Figure 5: Hand Geometry pattern

Figure 6: Hand Geometry Scanner

c) Voice Recognition

There are two main factors which makes a person's voice unique. Firstly, it is the physiological component which is known as the voice tract. Secondly, it is a behavioral component which is known as the voice accent. By combining both of these factors, it is almost impossible to imitate another person's voice exactly. Taking advantages of these characteristics, biometrics technology created voice recognition systems in order to verify each person's identification using only their voice. Mainly, voice recognition will focus on the vocal tract because it is a unique characteristic of a physiological trait. It works perfectly in physical access Control for users. Voice recognition systems are easy to install and it requires a minimal amount of equipment. This equipment includes microphones, telephone and/or even PC microphones. However, there are still some factors which can affect the quality of the system. Firstly, performance of users when they record their voice to database is important. For that reason, users are asked to repeat a short passphrase or a sequence of numbers and/or sentences so that the system can analyze the users' voice more accurately. On the other hand, unauthorized users can record authorized users' voices and run it through the verification process in order to get user access control to system. To prevent the risk of unauthorized access via recording devices, voice recognition systems will ask users to repeat random phases which are provided by the system during verification state. [3]

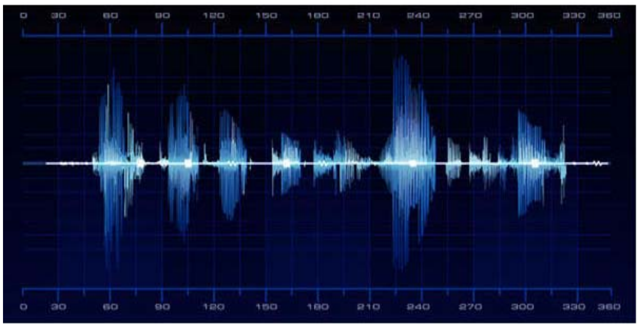

Figure 7: Voice Recognition

d) Face Recognition

The human face is one of the easiest characteristic which can be used in biometric security system to identify a user. Face recognition technology, is very popular and is used more widely because it does not require any kind of physical contact between the users and device. Cameras scan the user face and match it to a database for verification. Furthermore, it is easy to install and does not require any expensive hardware. Facial recognition technology is used widely in a variety of security systems such as physical access control or computer user accounts. However, it is still not as unique as its counterparts such as retinal, iris or DNA. Therefore, it is normally used with other characteristics in the system. On the other hand, time is the most negative affective factor with face recognition technology because as the user ages will change over time. Biometric face recognition systems will collect data from the users' face and store them in a database for future use. It will measure the overall structure, shape and proportion of features on the user's face such as: distance between eyes, nose, mouths, ears, jaw, size of eyes, mouth and others expressions. Facial expression is also counted as one of the factors to change during a user's facial recognition process. Examples include, smiling, crying, and wrinkles on the face [3]

e) Face Recognition

The human face is one of the easiest characteristic which can be used in biometric security system to identify a user. Face recognition technology, is very popular and is used more widely because it does not require any kind of physical contact between the users and device. Cameras scan the user face and match it to a database for verification. Furthermore, it is easy to install and does not require any expensive hardware. Facial recognition technology is used widely in a variety of security systems such as physical access control or computer user accounts. However, it is still not as unique as its counterparts such as retinal, iris or DNA. Therefore, it is normally used with other characteristics in the system. On the other hand, time is the most negative affective factor with face recognition technology because as the user ages will change over time. Biometric face recognition systems will collect data from the users' face and store them in a database for future use. It will measure the overall structure, shape and proportion of features on the user's face such as: distance between eyes, nose, mouths, ears, jaw, size of eyes, mouth and others expressions. Facial expression is also counted as one of the factors to change during a user's facial recognition process. Examples include, smiling, crying, and wrinkles on the face [3]

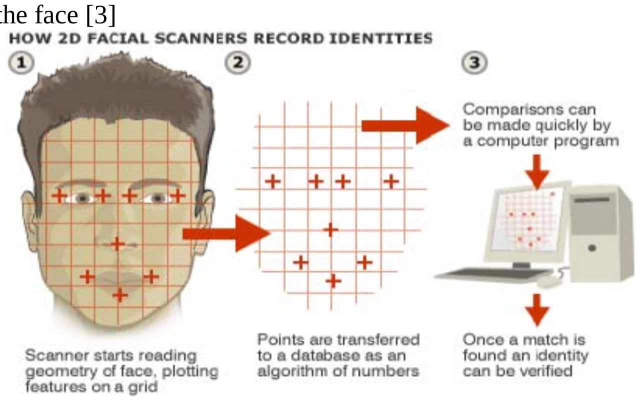

Figure 8: Face Recognition System

f) Iris Scan

The human iris is a thin circular structure in the eyes which is responsible for controlling the diameter and size of the pupils. It also controls the amount of light which is allowed through to retinal in order to protect the eye's retina. Iris colour is also a variable different to each person depending upon their genes. Iris colour will decide eye colour for each individual. There are several colours for iris such as: brown (most popular colour for the iris), green, blue, grey, hazel (the combination of brown, green and gold), violet, pink (in really rare cases). The iris also has its own patterns from eye to eye and person to person, this will make up to uniqueness for each individual.

Iris recognition systems will scan the iris in different ways. It will analyse over 200 points of the iris including: rings, furrows, freckles, the corona and others characteristics. After recording data from each individual, it will save the information in a database for future use in comparing it every time a user want to access to the system. Iris recognition security systems are considered as one of the most accurate security system nowadays. It is unique and easy to identify a user. Even though the system requires installation equipment and expensive fees, it is still the easiest and fastest method to identify a user. There should be no physical contact between the user and the system during the verification process. During the verification process, if the users are wearing accessories such as glasses and contact lenses, the system will work as normal because it does not change any characteristics of the user's iris. Theoretically, even if users have eye surgery, it will have no effect on the iris characteristics of that individual. [3]

Figure 9: Iris of a person

Figure 10: Iris recognition device

g) Retina Scan

Retina recognition technology captures and analyzes the patterns of blood vessels on the thin nerve on the back of the eyeball that processes light entering through the pupil. Retinal patterns are highly distinctive traits. Every eye has its own totally unique pattern of blood vessels; even the eyes of identical twins are distinct. Although each pattern normally remains stable over a person's lifetime, it can be affected by disease such as glaucoma, diabetes, high blood pressure, and autoimmune deficiency syndrome. The fact that the retina is small, internal, and difficult to measure makes capturing its image more difficult than most biometric technologies. An individual must position the eye very close to the lens of the retina-scan device, gaze directly into the lens, and remain perfectly still while focusing on a revolving light while a small camera scans the retina through the pupil. Any movement can interfere with the process and can require restarting. Enrollment can easily take more than a minute. The generated template is only 96 bytes, one of the smallest of the biometric technologies. [4]

Figure 11: Retina Scan

h) Keystroke Authentication

This is biometric authentication in which access is granted to users based on biological signatures such as a fingerprint, iris scan or biometrics based on keystroke behaviour. ID Control brings you Keystroke ID which is the best way to authenticate a person while minimizing the impact on privacy. This keystroke behaviour is used to recognize or verify the identity of a person. Not only unique physiological biometrics such as the iris and finger bring us unique biometrics. Physiological biometrics defines biological aspects of a person that determine identity. Behavioural biometrics verifies users based on how they conduct a given activity. Behavioural biometrics such as the way we sign our name or type in our password are unique as well and have much lower impact on privacy and costs. The way and the manner in which we type on our computer keyboard varies from individual to individual and is considered to be a unique behavioural biometric. Keystroke Dynamics or Recognition is probably one of the easiest biometrics forms to implement and manage. This is so because at the present time, Keystroke Recognition is completely a software based solution. There is no need to install any new hardware and even software. All that is needed is the existing computer and keyboard that is already in place and use. [5]

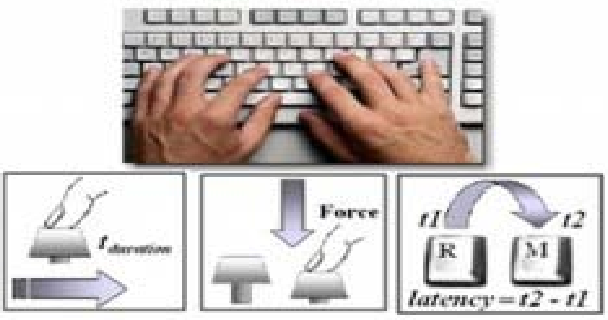

Figure 12: Illustration of Keystroke Dynamics

i) Vein Recognition

Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger. Vein recognition is a fairly recent technological advance in the field of biometrics. It is used in hospitals, law enforcement, military facilities and other applications that require very high levels of security. Vein recognition biometric devices can also be used for PC login, bank ATM identification verification, and many other applications such as opening car doors. Vein recognition biometrics is a particularly impressive and promising technology because it requires only a single-chip design, meaning that the units are relatively small and cheap. The ID verification process is very fast and contact-less. Using a light-transmission technique, the structure of the vein pattern can be detected, captured and subsequently verified. The user's vein pattern structure is image processed by the device and stored in a relevant data repository in the form of digital data. Many feel that vein recognition biometrics can produce higher accuracy rates than finger print recognition and finger vein patterns are virtually impossible to forge. [6]

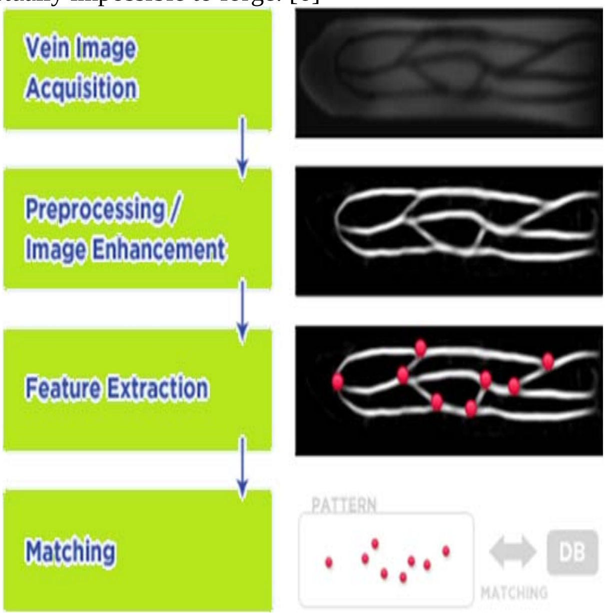

Figure 13: Steps in vein recognition

Figure 14: Vein recognition

j) Signature Recognition

The authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication, Static and Dynamic. Static is most often a visual comparison between one scanned signature and another scanned signature, or a scanned signature against an ink signature. Technology is available to check two scanned signatures using advances algorithms. Dynamic is becoming more popular as ceremony data is captured along with the X,Y,T and P Coordinates of the signor from the signing device. This data can be utilized in a court of law using digital forensic examination tools, and to create a biometric template from which dynamic signatures can be authenticated either at time of signing or post signing, and as triggers in workflow processes. [7]

Figure 15: Signature Recognition

3. Advantages of Biometrics

As biometrics technology gets more advanced and sophisticated, a greater number of advantages of biometrics used for security purposes and data protection in the workplace are being identified. Basically, biometrics technology is an automated method of monitoring access based on physiological or behavioural characteristics used for recognition and verification. Many different versions of biometric security have been developed, including identification by fingerprints, face, iris/retina, hand geometry, and voice verification. Here are some of the advantages that biometrics offer over more traditional security practices. [8]

- Identification is accurate. Unlike other security systems that rely on passwords or smart cards, one of the greatest advantages of biometrics is the accuracy it provides. When the system is set up correctly, biological characteristics like fingerprints and retinal scans provide completely unique data sets that cannot be replicated easily. This makes it very difficult for anyone but an authorized user to gain access without permission.
- Employee tracking. Since biometrics systems are essentially automatic and therefore data tracking is simple to implement, they offer employers and managers great opportunities for oversight concerning daily activities and operations. Certain events, transactions, and other activities are linked to a specific person, making it possible for employers to track chains of events. Biometrics can also significantly cut down on certain dishonest employee practices that can really eat away at a company's bottom line, such as buddy punching and other forms of fraud.
- Biometrics methods offer convenience. Some other advantages of biometrics products concern the efficiency and convenience they lend to access control. Passwords and pins are easily forgotten, can be written down and subsequently stolen, and are sometime hacked. Once obtained, they can be easily used by someone other than the authorized person. Smart cards and keys can similarly be lost or stolen, and can also be used by an imposter without detection. But with biometrics, something like fingerprints won't be lost and can't be easily obtained and replicated by someone trying to illicitly gain access.
- Systems are user friendly. Once they've been installed and implemented, biometrics systems are able to identify people very rapidly, uniformly, and reliably. Typically, only minimum training is needed to get the system operational, and there's no need for expensive password administrators. In addition, high-quality systems don't tend to need a large amount of maintenance, further cutting costs.

Table 1: Strengths of each methods.

Technique	strengths
Fingerprint	Mature technology; highly accurate; low cost; small size, becoming widely acceptable
Hand Geometry	accurate and flexible; widely acceptable to users
Voice Recognition	Usable over existing telephone system; good for remote access and monitoring;
Face Recognition	Widely acceptable to users; low cost; no direct contact; passive monitoring possible
Iris Scan	Highly accurate; works with eyeglasses; more acceptable to users than retina scan
Retina Scan	Highly accurate
Keystroke Authentication	Widely acceptable to users; low cost; uses existing hardware
Vein Recognition	More precise than fingerprint and accurate also
Signature Recognition	Widely acceptable to users

4. Issues in Biometrics

The use of biometrics is centuries old as the need for unique identification of individuals has existed throughout history. The more recent examples of its use are of Frenchman Alphonse Bertillon who developed "Anthropometrics" in 1888 and the Englishman Edward Henry who in 1900 used fingerprints for the first time to classify and identify criminals. However, since the tragic events of 9/11 biometric technology has been gaining popularity as the public now expects greater security. Additionally, there are some tangible benefits in the use of biometrics. For example, it is unique, convenient and fulfils the need for strong authentication. The main applications so far are governmental, e.g. ID Cards, e-passports, e-borders, air and port security and policing systems. Among the commercial enterprise the leading users are the travel industry, transport and financial services. However, there are serious ethical issues in the use of biometric technology. The main issues concern the personal privacy, the conflict with one's beliefs and values and the collection, protection and use of personal biometric data. The civil liberty organisations argue that the technology undermines the human rights for privacy and anonymity. It is intrusive and has the capability to make serious impact on personal freedom and democratic rights. The technology is prone to failure and is not fake proof as it can be spoofed. But due to many issues and threats around the world, e.g. threat of terrorism, identity theft and fraud, security, illegal immigration, benefit fraud and crime prevention and detection issues, it has become important to have the capability to freeze someone identity for later identification and verification. At the same time since 9/11 the biometric technology has advanced tremendously. The hardware has improved in design and accuracy, the prices have come down and, therefore, biometrics has firmed its place in the security world. The public concern regarding the issues mentioned above cannot be ignored. There is a compelling need to find "Workable and Deployable" solutions to these issues. The academics have a very important role to play through consultations, workshops and student education. [9]

5. Conclusion

Biometrics is a new advance technology which has improved time to time to meet the changing requirements. It is having major impact in security, authentication systems and also privacy. From fingerprint to signature the technology has augmented by its own features. Though there are some ethical and social issues being faced, no one can reject the statement that the technology has helped the human kind a lot.

References

[1] http://www.isaca.org/Journal/Past-Issues/2004/Volume 4/Documents/jpdf044-Biometrics-AnOverview.pdf
[2] Jammi Ashok et. al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 07, 2010, 2402-2408, AN OVERVIEW OF BIOMETRICS
[3] http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet.pdf
[4] http://www.globalsecurity.org/security/systems/biometrics-eye_scan.htm
[5] http://www.idcontrol.com/keystroke-biometrics
[6] http://findbiometrics.com/solutions/vein-recognition/

[7] http://www.biometricsinstitute.org/pages/types-of-biometrics.html
[8] http://enlightenme.com/advantages-of-biometrics/

Author Profile

Akshatha M A, Graduate in Computer science and Engineering from ATME College of Engineering under Visveshvaraya Technological University (VTU).