International Journal of Advanced Research in Engineering and Applied Sciences
ISSN: 2278-6252

BIOMETRICS IN MODERN ERA

Himanshu Sekhar Acharya*

Abstract: *Biometrics is seen by many as a solution to a lot of the user identification and security problems in today's networks. Password abuse and misuse, intentional and inadvertent is a gaping hole in network security. This results mainly from human error, carelessness and in some cases maliciousness. Biometrics removes human error from the security equation. Our aim will examine all the technological and feasibility aspects as well as the practical applications. We will look at many different biometric methods of identifying the user.*

Keywords: *Biometrics, Network Security, Biometric authentication*

*Asst. Prof., Comp. Sc, KIIMS,CUTTACK

1.0 INTRODUCTION

The meaning of Biometrics comes from the Greeks. The Greek hybrid of the words is bio meaning life and metry meaning to measure. The webster's definition is the statistical measurement and analysis of biological observations and phenomena. In a more simpler terms biometrics means using the body as a password.

Now-a-days, Security is no longer a secure word, because of the recent evolutions in the IT field such as e-commerce, Internet etc., gone are the days where passwords, authentication were considered as measures for security. To help the security on the Net, there comes a new era of security namely BIOMETRICS.Biometric identification is, simply, the technique of verifying a person by a physical characteristic or personal characteristics.Biometrics is personal identification based on "who are you" rather than

" what you have " or " what you know "

2.0 BEFORE AND AFTER BIOMETRICS

Before the establishment of the biometric system ,We have traditional methods like PIN(Personal Identification Numbers) Passwords and token based methods like passports and licenses For personal identification.

The major drawbacks with these are:

- These can be stolen , These may be forgotten ,
- Token based methods like passports , licenses can be forged
- Biometrics set a stage to overcome the above problems

Biometrics is preferred than traditional methods for two reasons

1. The person to be identified is required to be physically present at the point-of-identification
2. Identification based on biometric techniques obviates the need to remember a password or carry a token.

3.0 APPLICATIONS OF BIOMETRICS

Applications that currently uses keys, ID cards, ATM cards, or passwords for verification purposes has the potential to be converted to a biometrics application. Also, in an age where highly sensitive personal information can be accessed through several different remote channels, the need for more accurate and fraud-proof verification methods

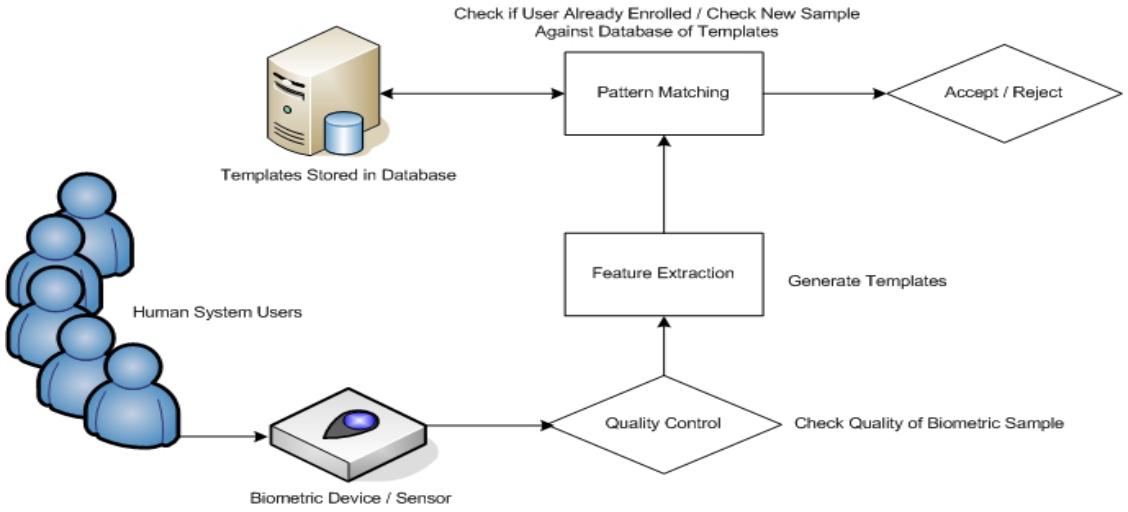
becomes large. Below are some of the potential and commercial applications of biometrics:

- Some of the biggest potential applications include word or PIN, a biometric trait cannot be lost, stolen, or recreated. This makes biometrics an obvious antidote to identity theft, a problem that is mushrooming alongside databases of personal information.
- Banks and others who have tested biometric-based security on their clientele, however, say consumers overwhelmingly have a pragmatic response to the technology. Anything that saves the information-overloaded citizen from having to remember another password or personal identification number comes as a welcome respite.
- There are also commercial applications for computer access control, access to web site servers, access through firewalls, and physical access control to protect sensitive information.
- Finger scan has the world's largest application of biometrics in the servicing of automated teller machines. There are many law enforcement applications, mostly for fingerprint recognition, at the Federal, State, and local levels.

The **future applications** of biometrics are very promising. Biometrics will play a crucial role in serving the identification needs of our future. Listed below are some potential future verification applications of biometrics:

- Voter Registration-verify identity at the polls to prevent fraudulent voting.
- In-store and Online purchases- eliminate the need for credit cards to make in-store purchases.

4.0 BASIC ARCHITECTURE OF A BIOMETRIC SYSTEM



The working procedure of any biometric system includes the following three phases.

ENROLLMENT

- Capturing biometric trait using sensor device
- Extracting relevant features to generate template
- Store template in database

VERIFICATION

- Generate template as in enrollment
- Match the template against a specific template“one-to-one”search(1:1)
- Used for physical or computer access

IDENTIFICATION

- Match done against a set of templates “one-to-many”search(1:N)
- Used in identifying criminals

5.0 DIFFERENT BIOMETRIC TECHNOLOGIES

There are two types of biometric technologies.

1. Based on PHYSICAL characteristics of a person

2. Based on BEHAVIORAL characteristics of a person

These are listed below

PHYSICAL	BEHAVIORAL
• Fingerprints identification	1. Voice recognition
• Iris recognition	2. key strokes
• Face recognition	3. signature scan
• Retinal scan	
• Hand geometry	

6.0 VOICE RECOGNITION

Automatic speaker recognition (ASR) system identifies people based on their speech. It may use different forms of speech like words or phrases or sentences.

The steps in this process include

1. The user speaks in front of the microphone ,that converts voice into electrical signals.
2. These electrical signals are then applied to analog to digital converter(ADC) and to Filters that convert this signal into binary form
3. This is then compared with the list of templates in the database and grants authentication if any match occurs.

Requirements

- More the no of filters more the accuracy of the code .
- Large capacity RAM is required to store much no of templates.
- High speed processor is required to handle comparisions fastly.

7.0 PROS AND CONS OF BIOMETRIC METHODS

Here are some of the advantages and disadvantages of fully developed biometric systems that are fairly accurate:

RETINAL SCAN (electronic scan of the innermost layer of the eyeball's wall):

Advantages: Retina generally remains stable through life, ensuring accuracy.

Disadvantages: Requires close physical contact MW scanning device; may not be generally accepted by public.

IRIS RECOGNITION (recording of iris using standard video technology):

Advantages: Non-invasive procedure (close physical contact not required).

Disadvantages: Relatively expensive; requires large amount of computer storage; may not be generally accepted by public.

FINGER IMAGING (recording of fingerprint using optical scanner):

Advantages: Widely accepted by public and law enforcement communities as reliable identification.

Disadvantages: Requires close physical contact with scanning device; residue on finger may cause recognition problems; has criminal overtones.

HAND GEOMETRY (three-dimensional recording of length, width and height of hand and fingers, using optical scanner):

Advantages: User-friendly; requires small amount of computer storage space. Disadvantages: Isn't as unique as other biometric methods; hand injury can cause recognition problems.

FACIAL RECOGNITION (photograph of face converted into digital code): Advantages: Non-invasive procedure.

Disadvantages: People who look alike can fool scanner; people can alter their appearance and facial hair can fool device.

VOICE RECOGNITION (acoustic signal of voice converted into digital code):

Advantages: Works well over the telephone.

Disadvantages: Requires large amount of computer storage; people's voices can change; background noises can interfere.

SIGNATURE RECOGNITION (computer record of pen/stylus speed, pressure, direction and other characteristics of signature):

Advantages: People are used to providing a signature.

Disadvantages: Poor long-term reliability; accuracy difficult to ensure.

8.0 FUTURE OF BIOMETRICS

a) DNA SCANNING All testing and fastest possible analysis of the human DNA takes at least 10 minutes to complete and it needs human assistance. Thus, it cannot be considered as biometric technology in its sense of being fast and automatic. Additionally current DNA capture mechanisms, taking a blood sample or a test swab inside of the mouth, are extremely intrusive compared to other biometric systems. Apart from these problems DNA, as a concept, has a lot of potential.

b) EAR SHAPE

Ear shape biometrics research is based on law enforcement needs to collect ear markings and shape information from crime scenes. It has some potential in some access control applications in similar use as hand geometry. There are not excessive research activities going on with the subject.

c) Keystroke Dynamic Scanning

Keystroke dynamics is a strongly behavioral, learnt biometric. As being behavioral, it evolves significantly as the user gets older. One of the many problems includes that highly sophisticated measuring software and statistical calculations have to be made real time if

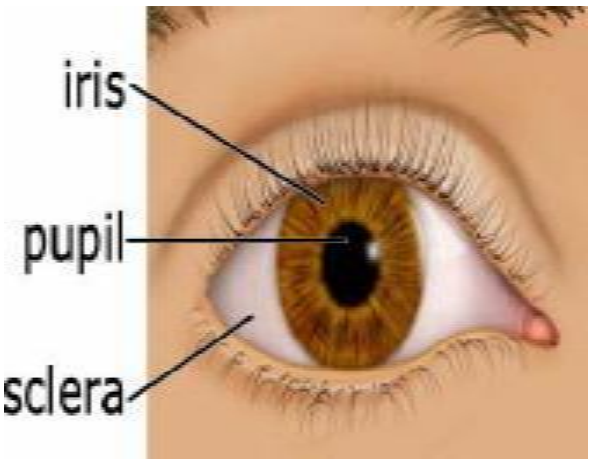
the user actions should be constantly Verified .

9.0 FUTURE APPLICATIONS OF BIOMETRIC

Biometrics will play a crucial role in serving the identification needs of our future. Listed below are some potential future verification applications of biometrics:

- Voter Registration-verify identity at the polls to prevent fraudulent voting.
- In-store and Online purchases- eliminate the need for credit cards to make in-store purchases.
- Academics/Certifications- verify person's identity prior to taking an exam.
- Personal transportation- eliminates the need for keys for cars, boats, motorcycles, planes, etc.

10.0 IRIS RECOGNITION



- Iris recognition analyzes the features that exist in the colored tissue surrounding the pupil, which has 250 points used for comparison, including rings, furrows, and freckles.
- Iris recognition uses a regular video camera system and can be done from further away than a retinal scan.
- It has the ability to create an accurate enough measurement that can be used for Identificationpurposes, not just verification.
- The probability of finding two people with identical iris patternsis considered to be approximately 1 in 10^52 (Population of theearth is of the order 10^10).
- Not even one-egged twins or afuture clone of a person will have the same iris patterns.

- The iris is considered to bean internal organ because it is time even though the person ages.
- Iris recognition is the most precise and fastest of the biometric authentication methods

11.0 FINGERPRINT RECOGNITION

Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows.

The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.

12.0 ETHICS OF BIOMETRICS

First of all we have to distinguish between authentication and identification. Identification is the process of checking whether the particular entry is there in the list of entries or not. Where as authentication is the process of verifying the person is eligible or not. Surely identification is an internal process of authentication. The problem is that a biometric such as a fingerprint can be used as a unique surrogate of one's identity which, as a unique identifier, can be used to trace people's transactions and link massive amounts of personal data about them. If my fingerprints are stored in a database, then my transactions, whereabouts and personal information can easily be tracked. It doesn't really matter for what purpose the biometric information was assembled whether it was for welfare registration or bank machine access, the same point applies unauthorized access to the database. The temptation for secondary or unauthorized uses of such a database beyond its primary purpose will be very great, especially if crime, tax fraud, and terrorism increase in our society.

Some vendors of biometric technology are proposing that a solution is to have unique hardware and software algorithms for different organizations and government agencies so that the police cannot generate the same template.

A step in the right direction is to encrypt the digital templates stored in the database. These encrypted biometrics improve privacy protection since matching efforts could not be accomplished without access to the encryption key. In this case, key management would be the weak link. Who is going to have control over the encryption keys? With key management, as with key escrow in a security system, privacy is based on a trust model.

13.0 CONCLUSION

Thus Biometrics plays a very important role in present technology. In a short span of time this concept gained much importance in the world. Also, in an age where highly sensitive personal information can be accessed through several different remote channels, the need for more accurate and fraud-proof verification methods becomes large. Already many organizations are currently using some old Biometric methods, in the coming years almost each and every organization will use this modern biometric security options. Biometrics itself is not solution to this problem. It just provides means to treat the possible user candidates uniquely. When doing so biometric system handles the unique data scanned from the user. Secrecy of this information has to be ensured by strong cryptographic methods. The best case could still be that the biometric templates would never leave the scanner device, with or without encryption. The result should only be granting the scanning device, which could be special smart card carried by user itself, to complete the challenge-response sequence needed. In that case your fingerprint may be the password, but the problem with management of public and secret cryptographic keys stays the same.

14.0 REFERENCES

1. “Biometrics for Network Security” - Paul Reid
2. “Biometrics” - Anil K Jain, John Woodward
3. Www.sciencedaily.com
4. www.zdnet.com
5. www.iscit.surfnet.nl
6. www.iriscan.com
7. www.biometric.cse.msu.edu
8. www.biometrics.org