RESEARCH REVIEW JOURNALS
Volume-03
Issue-09
September-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

# Biometrics Security System

Prof. Neena

*Dept. of computer Science S.D. College Hoshiarpur (India)*

**ARTICLE DETAILS**

**Article History**
*Published Online:* 07 September 2018

**Keywords**
Biometrics, authentication, identification, recognition

**ABSTRACT**

In today's networked world the need for security systems are growing due to increase in crimes like computer hacking, illegal access of ATM & cell phone and security breaches in Govt. and private buildings. Criminals take advantage of fundamental flows in the conventional security systems. For this security issues biometrics recognition system are used for personal identification. Biometric system provides automatic recognition of an individual based on a unique feature possessed by the individual.Biomatrics can be used to prevent unauthorized access to ATM's ,cellular phone ,smart cards, desktop PC's workstations and computer networks. This paper proposes a comparison among all kind of biometric system available in the society. The existing computer security systems used at various places like banking ,passport, credit cards ,smart cards, PIN, access control and network security are using username and passports for person identification. Biometric systems also introduce an aspect of user convenience. In this paper, the main focus is on working principal of biometric technique the various biometrics system and their comparisons.

## 1. Introduction

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons, the person to be identified is required to be physically present at the point of identification, and identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive /personal data. By replacing PIN's biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATM's ,cellular phones, smart cards, desktop PC s, workstations and computer networks, PINs and passwords may be forgotten and token based methods of identification like passports and driver's licenses may be forged, stolen or lost. Thus biometric systems of identification are enjoying a renewed interest. Various types of biometric systems are being used for real time identification, the most popular are based on face recognition and fingerprint matching. However there are other biometric systems that utilize iris and reinal scan, speed, facial thermo grams and hand geometry.

## 2. What is Biometrics?

A biometrics system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristics possessed by the user.

Biometric is the science and technology of measuring and analyzing biological data of human body, ,extracting a features set from the acquired data and comparing this set against to the template set in the database and these system are called Biometric system. These systems may operate in the following two modes.

1. **Enrollment mode**

2. **Verification mode**

In the Enrollment mode, the system recognizes an individual by searching the templates of all the users in the database for a match.

In the Verification mode, systems validate identity of person by comparing the captured biometric data with her own biometric templates which are stored system database.

The biometric systems consist of following four modules:

1. **Sensor module**
2. **Feature Extraction**
3. **Matcher**
4. **System Database**

1. **Sensor module:** - It captures the biometric data of individual. Fingerprint sensor is example of sensor module. It captures the ridge and valley structure of user finger.
2. **Feature extraction:** -In this module captured biometric data is processed and set of features are extracted.
3. **Matcher module:-**In this module to generate matching score during recognition features are compared against the stored templates.
4. **System database module:-** This module stores the templates of users. It stores the multiples of user to account for variations observed in biometric data & templates in database are updated over time.

## 3. Types of Biometrics

A. **Physiological Biometrics:-**A biometric related to the human body and difficult to forgery. It remains unaltered without significant issue. This type of biometric includes
   - **IRIS**

- **RETINAL**
- **FINGERPRINT**
- **PALM PRINT**
- **HAND GEOMETRY**
- **FACE**
- **DNA**

The physical characteristics of a person like finger prints, hand geometry, face, voice and iris are known as biometrics. The suitable biometric can be selected depending upon the application in various computer based security systems.

- **Finger points:-**
  The finger points of a person have been used as people have been used as person identification from long time. A finger print is the pattern of rids and valley on the surface of a fingertip. The finger prints of the identical twins are different. It is affordable to scan the finger prints of a person and can be used in computer for number of applications. This method is traditional and it gives accuracy for currently available fingerprint Recognition System is becoming affordable in a large number of applications like banking, passport etc.

- **Hand Geometry:-**
  The hand Geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, length and width of the fingers. This method is very simple and easy to use. As there is no effect of environment factors such as dry weather or dry skin, this does not appear to have dry negative effects on the authentication accuracy.

- **Face:-**
  The voice recognition systems have been currently used in various applications. Voice is a combination of physical and behavioral biometrics. The most popular approaches to face recognition are based on shape of facial attributes, such as eyes, eyebrows, nose, lips, chin and the relationships of these attributes. This face recognitions system automatically detects the correct face image and is able to recognize the person.

- **Voice:-**
  The voice recognition systems have been currently used in various applications. Voice is a combination of physical and behavioral biometrics. The features of person voice are based on the vocal tracts, mouth, nasal activities and lips movement that are used synthesis of sound. The behavioral part of the speech of person changes over time due to age, medical conditions and emotional stage. The speaker dependent voice recognition system is more difficult to design but provides more protection.

- **Iris:-**
  The iris is biological feature of a human. It is a unique structure of human which remains stable over a person lifetime. The iris is the annular region of the eye. The left and right irises of an individual can be treated as separate unique identifier. The iris information can be collected by iris image. The accuracy of iris based recognition system .The iris recognition system has become more users friendly and cost effective. The iris have a very low false accept rate as compared to other biometrics like finger print, face, hand geometry and voice.

**B. Behavioural Biometrics:-** It depends upon the behaviour of humani.e. Psychologically dependent. It depends on the present state of mind and can vary frequently as per situation or environment. For examples voice of human being can be affected by various factors as sadness, happiness, disease as throat infection, environment and so on. This type of biometric includes voice print, signature and typing rhythm recognition.

- **VOICE**
- **SIGNATURE**
- **TYPING RHYTHM**

## 4. Working Principle of Biometric System

All the biometric system use the same basic principle. It consists predefined steps as well as we must know some basic terms related to biometric system as enrollment, biometric data , presentation , template, feature extraction , matching.

- **Enrollment or Registration :-** The process, by which a user's biometric data is initially obtained ,processed and stored in the form of a template for ongoing use in a biometric system. It is called enrolment or registration process. This template will be used for further process as authentication.

- **Biometric Data:-** The data presented by the user during registration is called unprocessed image data which is also referred as raw biometrics data or biometric sample. Raw biometric data cannot be used to performed biometric matches so it is used to generate biometric template with the help of feature extraction process.

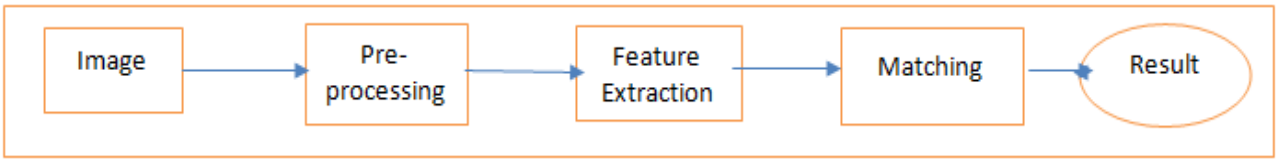
- **Presentation:-** The process by which user presents his/her biometric data to the acquisition devices the hardware which is used to collect data. For Example placing a finger on a plate at finger reader device.

- **Template: -** A mathematical representation of raw biometric data which is obtained after applying a number of feature extraction algorithms. A template size can vary in size as few bytes for hand geometry to several thousand bytes for facial recognition. The template created at the time of registration is called stored template and at the time of authentication is called live template.

- **Feature Extraction: -** The process of locating and encoding distinctive characteristics from biometric data in order to generate a template is called feature extraction. Feature extraction take place during enrolment and verification any time a template is created.

- **Matching**: -A process where stored template is matched with live template at the time of verification and we obtained a score on the basis of this score we conclude that a user is authenticate human or not.




**A Biometric System**

## 5. Advantages of Biometrics System

Biometric technology is gaining more popularity day by day, all around the world. Biometric solutions are highly accepted by many government agencies, multinational organizations, institutions, banks, and hospitals just to name a few industries. It is growing in every sector including finance, banking, workforce, borders and most rapidly for national identity.

- **Security:-**We used to have passwords with numbers, alphabets, symbols, etc. which are becoming easy to hack every day. There are zillions of hacking incidents happening every year and we are losing our money constantly. Biometric technology brings different types of solutions which are nearly impossible to hack unlike passwords. This is a great help for us, specifically for business owners who are fighting with security problems for a long time.
- **Accuracy:-**Traditional security systems mess up regularly costing us a big amount of time, money and resources. The most common security systems are passwords; personal identification numbers (PINs) and smart cards that aren't always accurate. However, biometric works with your physical traits such as fingerprints, palm vein, retina amongst others that will always serve you accurately anywhere, anytime.

- **Accountability:-**In other verification methods, anybody can use your password or security number to hack your personal information, which is highly risky and we are suffering from this problem continuously. But, in case of biometric security, it needs your direct interactions to login or pass the security system which allows 100% accountability for all your activities.

- **Convenient:-**Imagine all the times when you forgot your passwords, quite nerve-wrecking, right? You are not alone. We all have gone through this process where it is hard to memorize or note down each and every password and we are more than likely to forget it at some sticky situations. There are some handy tools to do the job for you, but none of these can beat the convenience of biometric solutions which stands to be the most convenient solution ever. Your credentials are with you forever, so it doesn't require you to memorize or note down anything.

- **Scalability:-**Unlike other solutions, biometrics are highly scalable solutions for all types of projects. Biometric technologies are used in many government projects, banking security systems, workforce management, etc. It is possible because of the scalability of its solutions.

- **ROI:-**Biometric solutions will provide you the best ROI compared to other security systems. You can keep track of thousands of employees of a large company with just one biometric device and software. On the other hand, you would need to manage a huge resource to do the same job costing you more time than the appropriate biometric solution.

- **Flexibility:-**Definitely biometric systems are the most flexible security solution. You have your own security credentials with you so you don't need to bother memorizing awkward alphabets, numbers and symbols required for creating a complex password.

- **Trustable:-**Reports claim that the young generations trust biometric solutions more than other solutions. Banks have already started using biometric security systems to enhance the security and reliability for their customers.

- **Save Time:-**Biometric solutions are highly time conserving. In most cases, you just need to put your finger on a device or look at a retina device to pass the system. On the other hand, traditional methods have layers of hassles and interrogations which become annoying and unbearable.

- **Save Money:-**Governments are putting their money to create a national biometric database so that government services can be provided to the people with more accuracy and less cost. Corporations are adopting biometric system to get accurate information which saves both time and money. With a little money, any company can track their employees and reduce the extra costs they are paying for years.

It is the age of information technology. Our traditional security systems are going to be outdated day by day. We have to adopt the latest technologies to enhance our security and kick off the burglars. The developed countries including USA, UK, Australia, Canada, etc. know the advantages of biometrics and have already adopted the technology in many phases of public services and continue to adapt to create a more biometrically secure future.

## 6. Disadvantages of Biometrics

Technology is built to improve the quality of our life. It brings betterments in the way of our life in every aspect. Biometric technology is also a great invention that brings significant changes in our lifestyle. As said, with great power comes even greater responsibility, biometric technology is a good example of this quote. While the introductions of biometrics bring many benefits, unfortunately, it also came with its own set of problems.

- **Physical traits are not changeable:-**Most of the biometric modalities work with physical traits such as fingerprint, iris, palm vein, etc. We all have only a pair of eyes; a certain number of fingerprints, and other body parts that are unchangeable. We can reset a password, but we never can change our fingerprints or retina, these are fixed. Our biometric data is stored in respective government's databases or companies who enable such services.

- **Error Rate:-** Biometric machines are less than perfect and mistakes can happen. Usually, biometric devices make two types of errors, False Acceptance Rate (FAR) and False Rejection Rate (FRR). When the device accepts an unauthorized person, it is known as FAR and when it rejects an authorized person, it is known as FRR. The error rate in some cases are so high that it creates great chaos for the entire security system. It could happen due to weather, physical condition, age and other issues. A turmoil could happen with an error rate of as low as 1% in a large-scale authentication process.

- **Cost:-**The cost of biometric devices are comparatively higher than other traditional security devices. The costs of biometric software, devices, programmers, server and other relative equipment combined is a large amount of money.

- **Delay:-**Some biometric devices take more than the accepted time and a long queue of workers form waiting to be enrolled in large companies. In these cases, people get hard time while scanning the biometric device every day. It is hard for a person when he/she has to go through a biometric verification system before entering into school, office or other places every day.

- **Complexity:-**One of the biggest disadvantages of biometrics is the highly technical and complex system that makes up the whole process. A non-techy person will be flopping like fish out of water when trying to understand the system. Companies hire highly experienced and skilled programmers to develop the system, so it requires programmers for managing the system as well.

- **Unhygienic:-**There are various types of biometric modalities. Some of them are contact based like fingerprint and palm vein scanner; some are contactless like iris and face recognition, etc. In contact-based modalities, a biometric device is used a zillion times by enormous amount of people. Everyone is actually sharing their germs with each other via the device. You never know what you are taking with you after placing your finger on the device. You wouldn't have any option to change the system.

- **Scanning Difficulty:-**Some biometric modalities like iris scan can go through scanning difficulties. It happens due to several reasons including eyelashes, eyelids, lens and reflections from the cornea. For these reasons, iris scanning may not be as reliable for use.

- **Physical Disability:-**Some people aren't fortunate enough to be able to participate in the enrollment process. They might have lost or damaged body parts such as fingers or eyes. In this type of case, a fingerprint/ Iris recognition device to recognize would be embarrassing and simply offensive. These types of people will surely pass a hard time to cope up with others in the system.

- **Environment and usage Matters:-**Environment and usage can affect the overall measurements taken. Especially in highly cold areas, the error rate is higher which creates unnecessary chaos and disappointments over the whole system.

- **Additional Hardware Integration:-**Some biometric modalities need additional hardware integration which is costly, inconvenient and complex. It is hard to manage these types of modalities.

## 7. Conclusion

The Biometric security systems are the systems which uses the physical characteristics of a person like finger print, hand geometry ,face , voice and iris. These systems overcomes the drawback s of the traditional computer based security systems which are used at the places like ATM, passport, payroll, driver's license , credit cards, access control, smart cards, PIN ,government offices and network security . The biometric security systems have been proved to be accurate and very effective in various applications. The biometric features can be easily acquired and measured for the processing only in the presence of a person. Hence these systems are proved highly confidential computer security systems.

**References**


1. https://www.ukessays.com/dissertation/examples/information-systems/advantages-and-disadvantages-of-biometrics.php
2. https://biometrictoday.com/10-advantages-disadvantages-biometrics-technology/
3. https://www.slideshare.net/prabhjeet946/biometric-security-advantages-and-disadvantages
4. https://www.wikipedia.org
5. https://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/