



JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ANALYZATION OF BIOMETRIC SYSTEMS

¹Dr D.M PATEL, ²PROF. KACHHIYA DHURVAL, ³JEEGAR AJAYKUMAR CHAUHAN, ⁴DIPEN JATINBHAI BHATT, ⁵IQBAL FORID SHAIKH, ⁶ KISHAN MAHENDRBHAI PATEL

¹PRINCIPAL, ² INTERNAL GUIDE, ³B.E STUDENT, ⁴ B.E STUDENT, ⁵ B.E STUDENT, ⁶B.E STUDENT

¹COMPUTER DEPARTMENT,

¹²³⁴⁵⁶ D.A. DEGREE ENGINEERING AND TECHNOLOGY, MAHEMDAVAD-387170, GUJRAT, INDIA.

Abstract :

Over the last few years, a new area of engineering science has been established whose products are likely to create a large market in the near future. It has been called "biometrics". The pioneers of this new domain intend to construct devices which would allow identification of a person on the basis of his/her "biological" characteristics: voice, dynamics of movements, features of face and other parts of the body, retina or iris pattern. Nature has made human beings with different characteristics which may vary from one person to another. This property is made use of by Biometric technology to distinctly identify each person.

INDEX-TERMS : uniqueness, universality, permanence, collectability, performance, acceptability and circumvention.

I. INTRODUCTION

What is Biometric System?

Biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Several important issues must be considered in designing a practical biometric system. First, a user must be enrolled in the system so that his biometric template can be captured. This template is securely stored in a central database or a smart card issued to the user. The template is retrieved when an individual needs to be identified. Depending on the context, a biometric system can operate either in a verification (authentication) or an identification mode.

WHY WE NEED BIOMETRICS?

In order to avoid the problems of forgetting passwords and ID codes, Biometrics based authentication helps us in verifying your fingerprints, iris pattern and voice for your identity at A.T.M's, Airports, etc., you can unlock your houses, withdrawing money from a bank with just a blink of an eye, a tap of your finger or by just showing your face.

WHAT IS IT?

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. Identification based on biometric techniques obviates the need to remember a password or carry a token. By replacing PIN's, biometric techniques can potentially prevent unauthorized access to or fraudulent use of A.T.M's, Smart cards, computer networks.

PIN's passwords may be forgotten, and token-based methods of identification like passwords and driver's licenses may be forged, stolen or lost. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user.

2.DESIGN ISSUES OF BIOMETRIC SYSTEMS:

An important issue in designing a practical system is to determine how an individual is identified and are designed by keeping two characteristics in mind, they are:

PHYSICAL CHARACTERISTICS:

- Fingerprint, Handprint
- Face
- Scent
- Thermal image
- Iris Pattern
- Personal traits
- Voice pattern
- Handwriting
- Acoustic Signature

3.IDENTIFICATION VS VERIFICATION:

There are two different ways to resolve a person's identity: verification and identification. Verification (Am I whom I claim I am?) involves confirming or denying a person's claimed identity. In identification, one has to establish a person's identity (Who am I?). Each one of these approaches has its own complexities and could probably be solved best by a certain biometric system.

4.TYPES OF BIOMETRIC DEVICES AND THEIR SERVICES:

Now let's see some of the biometric devices being widely used in many areas like computer/network security, government organizations, prisons, etc.

They are:

- Fingerprint identification
- Face recognition
- Iris recognition
- Hand geometry
- Signature recognition
- Retinal scanning
- Voice verification

5.APPLICATION AREAS:

The uses for biometric security are varied and growing. It was developed in response to a need to associate human action with identity – whether conducting a transaction, accessing a computer or a critical information system, or entering secure physical area.

6.ADVANTAGES:

- High accuracy rate.
- Imitation is almost impossible

7.DISADVANTAGES:

- Perceived to be intrusive and invasive. Can be done from a short distance.
- Optical readers are difficult to operate requiring advanced training for employees.

8. CONCLUSION:

The advances in accuracy and usability and decreasing cost have made the biometric technology a secure, affordable and cost-effective way of identifying individuals. Biometric parameters such as fingerprint scanning, iris scanning, retinal scanning, hand geometry, signature verification, voice verification and others are all well established with their own particular characteristics. The limiting factors of speed and bandwidth are now a thing of the past and their practical performance might in many instances be better than expected. Today, it is an efficient and effective method of replacing passwords, tokens and smart cards.

In the absence of standards and direction, the rapid and wide spread deployment of biometric authentication system could easily facilitate the problematic proliferation of authentication and tracking of the people.

9.REFERENCES:

- [1] Neha Dahiya, Chander Kant, "Biometrics Security Concerns" IEEE TRANSACTION ON 2012 Second International Conference on Advanced Computing & Communication Technologies.
- [2] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp 21-38, June 2005.
- [3] Anil. K.Jain, Arun Ross, Salil Prabhakar, "An introduction to biometric recognition", IEEE Transactions on circuits and systems for video technology, vol. 14, no. 1, pp 67-80, Jan 2004.
- [4] 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
- [5] Phillips et al., "An Introduction to Evaluating Biometric Systems, Guide to Biometrics", IEEE Computer, February 2000, pp 56-63.