International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
Vol. 48, Issue 01, Quarter 01 (January-February-March 2019)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Biometric System: Implementation of Fingerprint Matching System

Neeru Mago

Department of Computer Science and Applications,
Panjab University SSG Regional Centre, Hoshiarpur
neerumago@pu.ac.in, neerumago80@gmail.com

Publishing Date: January 31, 2019

Abstract

There are many classical ways to identify a person's authentication such as password, identity card, etc. but nowadays, the popular approach is Biometric which is used to authenticate a person. In this approach, we use different identification approaches such as face recognition, voice recognition, fingerprint recognition and retina recognition etc. So that, there is no need to carry an Identity card or to remember password. The most important thing is that it cannot be shared or misplaced. This approach can be used in the field of uniqueness, universality, acceptability, performance etc Biometric identification process has gained popularity with the recent advancement of computing capability. The uniqueness of the Biometrics and the processing power has gained popularity in various walks of our life for the purpose of authentication and verification. This paper describes the process of Biometrics system, its various types and a fingerprint identification system and its implementation to establish the identity of a person.

Keywords: *Biometrics, Face recognition, Fingerprint recognition, Hand geometry, IRIS recognition, Signature recognition, Voice recognition.*

1. Introduction

Biometrics allows a person to be identified and authenticated based on a set of recognizable and verifiable data, which are unique and specific to them. Biometrics is the science of analyzing physical or behavioral characteristics specific to each individual in order to be able to authenticate their identity. If we were to define biometry or biometrics in the simplest sense, we would say the "measurement of the human body". Biometric authentication is the process of comparing data for the person's characteristics to that person's biometric "template" in order to determine resemblance. The reference model is first store in a database or a secure portable element like a smart card. The data stored is then compared to the person's biometric data to be authenticated. Here it is the person's identity which is being verified. In this mode, the question being asked is: "Are you indeed Mr or Mrs X?" Biometric identification consists of determining the identity of a person. The aim is to capture an item of biometric data from this person, for example by taking a photo of their face, by recording their voice, or by capturing an image of their fingerprint. This data is then compared to the biometric data of several other persons kept in a database.

Biometric systems as shown in Fig 1 use three steps:

- Enrolment: The first time you use a biometric system, it records basic information about you, like your name or an identification number. It then captures an image or recording of your specific trait.
- Storage: Contrary to what you may see in movies, most systems don't store the complete image or recording. They instead analyze your trait and translate it into a code or graph. Some systems also record this data onto a smart card that you carry with you.
- Comparison: The next time you use the system, it compares the trait you present to the information on file. Then, it either accepts or rejects that you are who you claim to be.

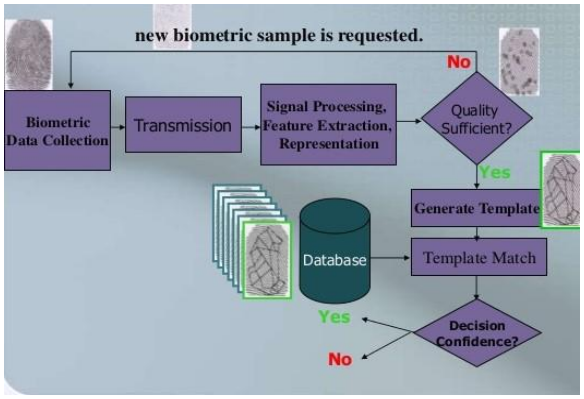


Figure 1: Biometric system

Systems also use the same three components: A sensor that detects the characteristic being used for identification. A computer that reads and stores the information. Software that analyzes the characteristic, translates it into a graph or code and performs the actual comparisons. Biometric Process has three steps:

Step 1: Acquire Biometric Sample.

This step is where you are going to present your desired characteristic trait to be scanned by the biometric device (we will use fingerprints as an example.) Once the device captures this information it creates an electronic representation of that characteristic, which will be used later on in the verification process.

Step 2: Feature Extraction

During this step you are going to present your fingerprint onto the scanning device so that it captures an image of your unique fingerprint.

Step 3: Matching

This is the most important step in the verification process of a biometric system. The image that was captured during the feature extraction is now going to be compared to the electronic template you had provided when it took a sample of your fingerprint. It pulls the template from the database from where it was stored and then either grants you access if there is a match, or denies you entry if it can't recognize your fingerprint.

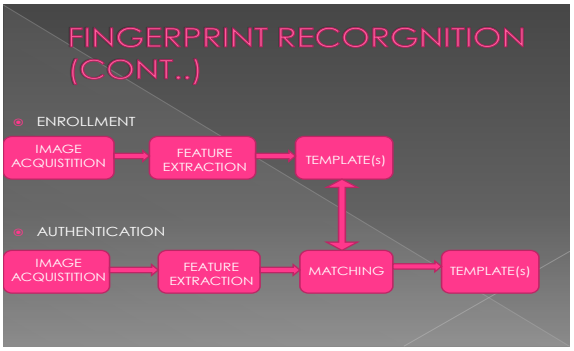


Figure 2: Biometric Process using Fingerprint Recognition

2. Biometrics

Biometrics makes the use of biological terms that deals with data statistically. It verifies a person's uniqueness by analyzing his physical features or behaviors (e.g. face, fingerprint, voice, signature, keystroke rhythms). The systems record data from the user and compare it each time the user is claimed. A biometric system is a computer system that implements biometric recognition algorithms. A typical biometric system consists of sensing, feature extraction, and matching modules. The technique used in biometric system has been broadly classified into two major categories namely:

• *Physiological based techniques* include facial analysis, fingerprint, hand geometry, retinal analysis, DNA and measure the physiological characteristics of a person.

• *Behavior based techniques* include signature, key stroke, voice, smell, sweat pores analysis and measure behavioral characteristics.

Biometric recognition systems based on the above methods can work in two modes: *identification* mode, where the system identifies a person searching a large data base of enrolled for a match; and *authentication* mode where the system verifies a person's claimed identity from his earlier enrolled pattern.

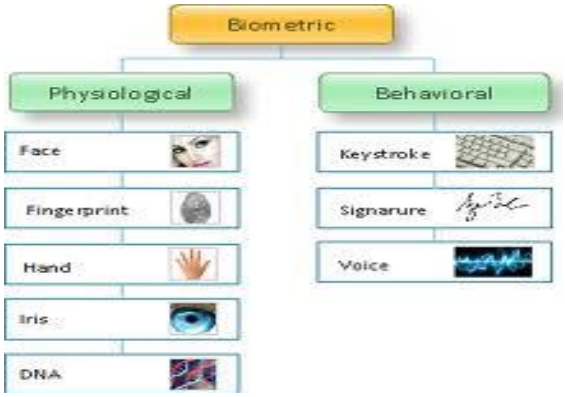
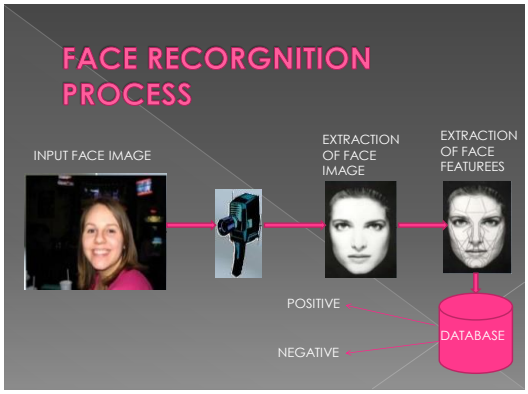


Figure 3: Categories of Biometric

3. Types of Biometrics

3.1 Face recognition

A face recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a face database. It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Recently, it has also become popular as a commercial identification and marketing tool.



3.2 Fingerprint recognition

Fingerprint recognition is one of the most well known biometrics, and it is by far the most used biometric solution for authentication on computerized systems.

Fingerprint Patterns:

-> Basic Patterns
1. Arch
2. Loop
3. Whorl

-> Minutiae Features
1. The Ridge Ending
2. The Bifurcation
3. The Sport

Advantages:
- Improved security
- Improved customer experience
- Cannot be forgotten or lost
- Reduced operational costs

Disadvantages:
- Environment and usage can affect measurements
- Systems are not 100% accurate.
- Require integration and/or additional hardware
- Cannot be reset once compromised

3.3 Hand geometry

Hand geometry is a biometric that identifies users by the shape of their hands. Hand geometry readers measure a user's hand along many dimensions and compare those measurements to measurements stored in a file.

Advantages:
- Simple, relatively easy to use and inexpensive
- Hand geometry data is easier to collect, unlike the fingerprints where a good frictional skin is required by imaging systems, and retinal data where special lighting is required
- Environmental factors, such as, dry weather that causes the drying of the skin is not an issue

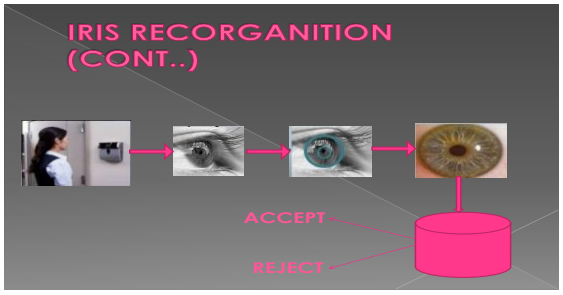
- Usually considered less intrusive than fingerprints, retinal, etc

Disadvantages:

- The hand geometry is not unique and cannot be used in identification systems
- Not ideal for growing children
- Jewellery (rings, etc), limited dexterity (arthritis, etc) etc may pose a challenge in extracting the hand geometry information
- The data size of hand geometry biometrics is large and is not ideal for using it in embedded systems.

3.4 IRIS Recognition

Ocular-based biometric technology that uses the unique patterns on a person's retina blood vessels and is often confused with iris recognition. IRIS recognition uses video camera technology with subtle near infrared illumination to acquire images of the detail-rich, intricate structures of the iris which are visible externally. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual. Databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second per (single-core) CPU, and with remarkably low false match rates.



Advantages:

- Iris pattern and structure exhibit long-term stability
- Ideal for Handling Large Databases
- Unmatched Search Speed
- Safety and Security Measures In Place

Disadvantages:

- Small target (1 cm) to acquire from a distance (1 m)
- Located behind a curved, wet, reflecting surface
- Obscured by eyelashes, lenses, reflections
- Partially occluded by eyelids, often drooping
- Deforms non-elastically as pupil changes size
- Illumination should not be visible or bright

3.5 Signature Recognition

Signature recognition is a behavioural biometric. It can be operated in two different ways:

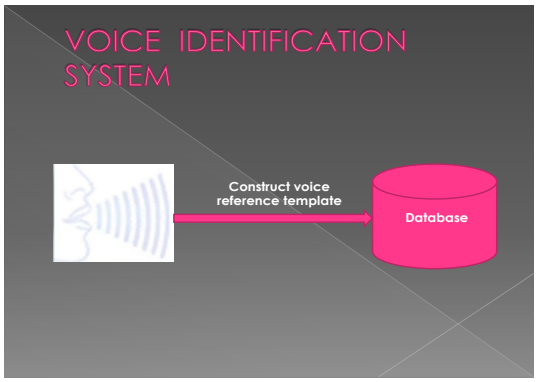
- Static: In this mode, users write their signature on paper, digitize it through an optical scanner or a camera, and the biometric system recognizes the signature analyzing its shape. This group is also known as “off-line”.
- Dynamic: n this mode, users write their signature in a digitizing tablet, which acquires the signature in real time. Another possibility is the acquisition by means of stylus-operated PDAs. Some systems also operate on smart-phones or tablets with a capacitive screen, where users can sign using a finger or an appropriate pen. Dynamic recognition is also known as “on-line”.

Verification process:

- the angle at which the pen is held,
- the number of time the pen is lifted,
- the time it take to write the entire signature,
- the pressure exerted by the person while signing,
- the variations in the speed with which different parts of the signature are written.

3.6 Voice Recognition

Voice recognition is the identification using the acoustic features of speech that have been found to differ between individuals.



4. Implementation of Fingerprint Biometric System

In this program it is shown how to compare two images in asp.net c# like finger print biometric system. In this system base64String method is used to convert the stream object into string.

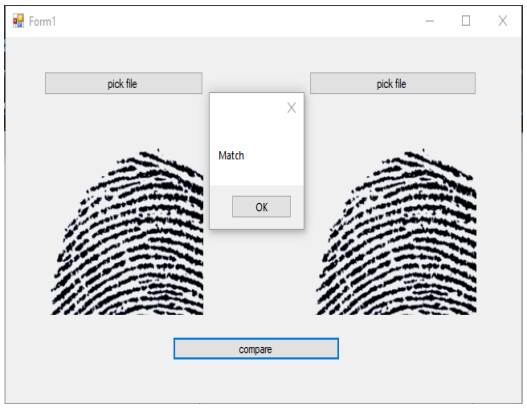
```
using System;
usingSystem.Collections.Generic;
usingSystem.ComponentModel;
usingSystem.Data;
usingSystem.Drawing;
usingSystem.Drawing.Imaging;
using System.IO;
usingSystem.Linq;
usingSystem.Text;
usingSystem.Threading.Tasks;
usingSystem.Windows.Forms;

namespace WindowsFormsApplication1
{
MessageBox.Show("Match");
        }
else
        {
MessageBox.Show("Not Match");
        }
    }
privateboolImageCompareString(Bitmap
bitmap1,Bitmap bitmap2)
    {
//throw new NotImplementedException();
MemoryStreamms = newMemoryStream();
bitmap1.Save(ms,ImageFormat.Png);
publicpartialclassForm1 : Form
  {
Bitmap bitmap1, bitmap2;
public Form1()
    {
InitializeComponent();
    }

privatevoid button1_Click(object sender,
EventArgs e)
    {
OpenFileDialogopenflg = newOpenFileDialog();
if(openflg.ShowDialog()==DialogResult.OK)
        {
          pictureBox1.ImageLocation =
openflg.FileName;
          bitmap1 =
newBitmap(openflg.FileName);
        }
    }
privatevoid button2_Click(object sender,
EventArgs e)
    {
OpenFileDialog openflg1 = newOpenFileDialog();
if (openflg1.ShowDialog() == DialogResult.OK)
        {
          pictureBox2.ImageLocation =
openflg1.FileName;
          bitmap2 =
newBitmap(openflg1.FileName);
        }
    }
privatevoid button3_Click(object sender,
EventArgs e)
    {
bool compare = ImageCompareString(bitmap1,
bitmap2);
if (compare == true)
        {

stringfirstbitmap =
Convert.ToBase64String(ms.ToArray());
ms.Position = 0;
bitmap2.Save(ms,ImageFormat.Png);
stringsecondbitmap =
Convert.ToBase64String(ms.ToArray());
if (firstbitmap.Equals(secondbitmap))
{
returntrue;
        }
else
        {
returnfalse;
        }   }  }}
```

4.1 Designing



5. Conclusion

In this paper, a brief introduction to Biometrics, its process and various types are discussed. There are several types of biometrics, and each has its advantages and drawbacks. Depending on what level of security and what do you want to provide, you have to make the good choice. Further, the given implementation was an effort to understand how fingerprint recognition is used as a form of biometric to recognize identities of human beings.

References

[1] A. Ahmed and I. Traore. Anomaly intrusion detection based on biometrics. In 6th IEEE Information Assurance Workshop, 2005.
[2] A. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. In Transactions on Dependable and Secure Computing, pages 165–179, 2007.
[3] D. Gunetti and C. Picardi. Keystroke analysis of free text. ACM transactions on information and System Security, 8(3), 2005.
[4] E. Lau, X. LI, C. Xiao, and X. Yu. Enhanced user authentication through keystroke biometrics.
[5] Computer and Network Security, Massachusetts Institute of technology, 2004.
[6] Link:http://www.gemalto.com/govt/inspired/biometrics1
[7] J. McHugh. Intrusion and intrusion detection. International Journal of Information Security, 1:14–135, 2001.
[8] Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross. Biometrics: a grand challenge. In Proceedings of the 17th International Conference on Pattern recoginition, pages 935–942, 2004.
[9] Khalil Challita, Hikmat Farhat, Khaldoun Khaldi. Biometric Authentication for Intrusion Detection Systems. First International Conference on Integrated Intelligent Computing, 2010
[10] Tiwari et.al, Biometric authentication using fingerprint, J. Acad. Indus. Res. Vol. 1(8) January 2013.
[11] Mudholkar et.al, Biometrics Authentication Technique for Intrusion Detection Systems using Fingerprint Recognition, International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012.