Case study on Design of Biometric Authentication Software

Group Members	Roll no
Shreya Gandhi	21021
Tejaswini Maskare	21038
Parth Gujarathi	21024
Mahesh Jagtap	21027
Shreyas Lolge	21036

Introduction

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control or for identifying individuals who are under surveillance. The basic premise of biometric authentication is that every person can be accurately identified by their intrinsic physical or behavioral traits. The term biometrics is derived from the Greek words bio, meaning life, and metric, meaning to measure.

In this highly advancing digital world the level of security is getting breached and also the transaction fraud has increased. Existing security measures rely on knowledge based approaches like passwords, PIN numbers or token based approaches like passports, swipe cards. Such methods are not very secure. These can be easily accessed through number of ways for example by stealing or by sharing etc. Furthermore it is quite impossible to differentiate between authorized user and the person having access to the tokens or passwords.

Biometric-based authentication is the perfect solution for this problem. Various classifications of Biometric characteristics are shown in Fig.

Biometrics is the science and technology of measuring and analyzing biological data. It refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for uthentication purposes. Biometric characteristics of human beings can be divided in three main classes,

Physiological are related to the shape of the body. The oldest authentication system that have been used for more than 100 years, are fingerprints. Other examples are face recognition, hand geometry and iris recognition.

Behavioral are related to the behavior of a person. The first characteristic to be used, still widely used today, is the signature. Some more modern approaches are the study of keystroke dynamics and of voice.

Chemical /Biological are related to the chemical analysis of different biological Parameters of a person. This is the latest arena in biometric authentication systems. Some examples are DNA structure analysis, blood glucose, skin spectrography etc.

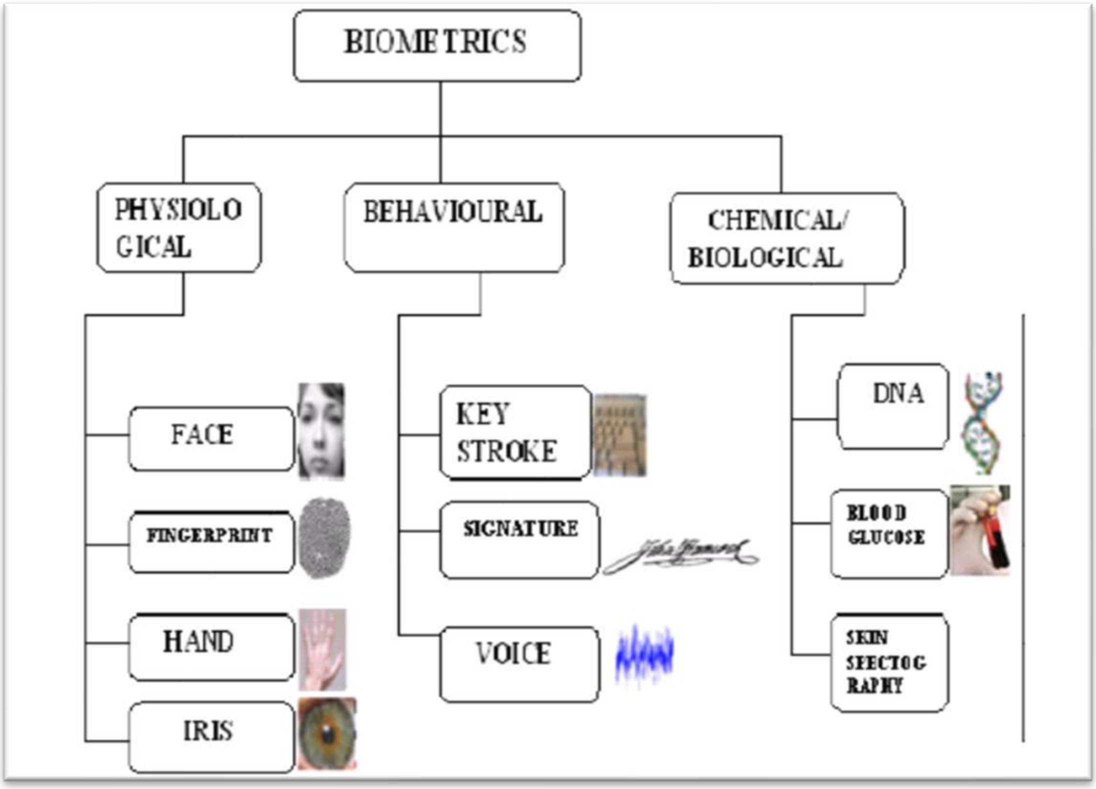


Fig. : Classification of Biometric characteristics

Methodology (How Software Works)

Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point-of-sale (POS) applications. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry. Some biometric methods, such as measuring a person's gait, can operate with no direct contact with the person being authenticated.

Components of biometric devices include the following:

- a reader or scanning device to record the biometric factor being authenticated;
- software to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with stored data; and
- a database to securely store biometric data for comparison.

Biometric data may be held in a centralized database, although modern biometric implementations often depend instead on gathering biometric data locally and then cryptographically hashing it so that authentication or identification can be accomplished without direct access to the biometric data itself.

Types of biometrics

The two main types of biometric identifiers are either physiological characteristics or behavioral characteristics.

Physiological identifiers relate to the composition of the user being authenticated and include the following:

- facial recognition
- fingerprints
- finger geometry (the size and position of fingers)
- iris recognition
- vein recognition
- retina scanning
- voice recognition
- DNA (deoxyribonucleic acid) matching

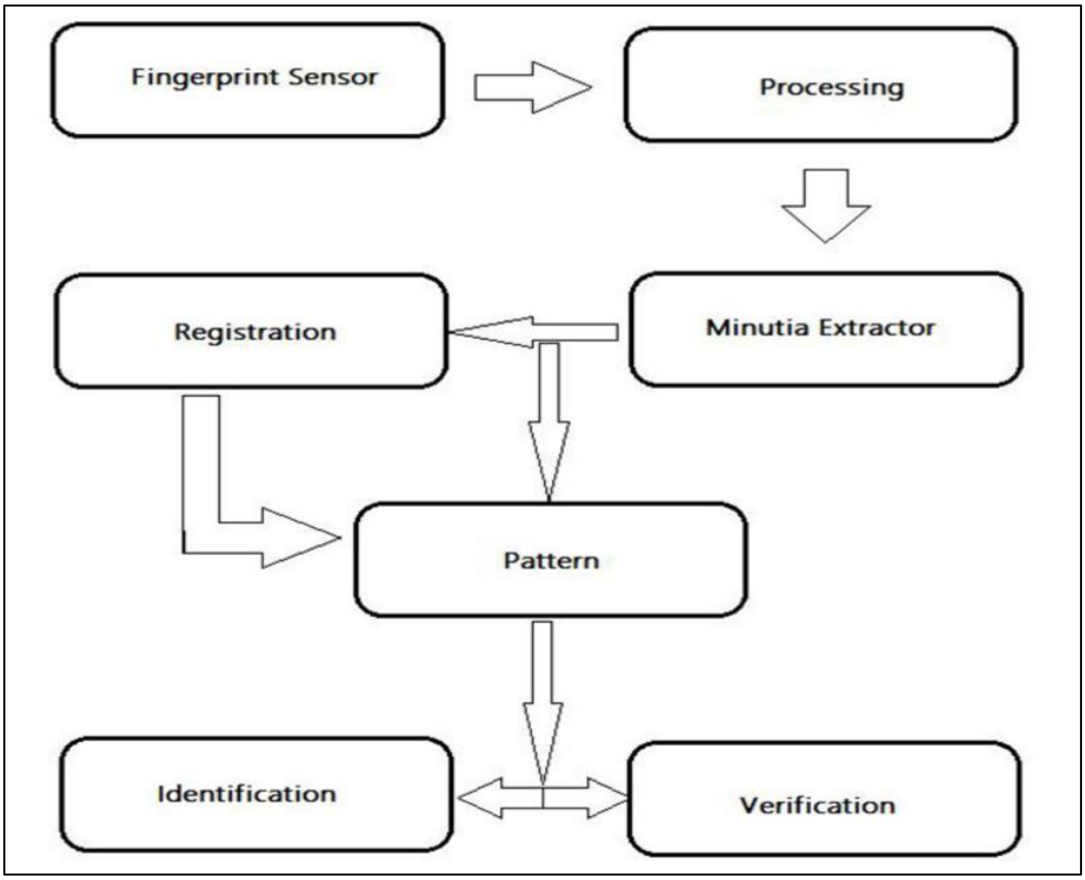
- digital signatures

Architecture of Biometric Authentication Software

A biometric system is designed specifically to map a particular biometric trait, i.e. fingerprint recognition systems cannot process iris or retina patterns. However, all biometric systems work on the principle of mapping patterns with the help of technology. A person’s physiological or behavioural patterns are mapped, stored and compared at a later date to verify or identify the owner of the pattern. Biometric system consists of both hardware and software elements. Hardware generally includes electronic components and sensors to be able to read data out of specific patterns, software portion makes use of algorithms to enhance and recognize this data to generate a template unique to the individual it comes from.

Biometric system architecture is the representation of a system as a whole, including a mapping of functionality onto hardware and software components, a mapping of the software architecture onto the hardware architecture, and human interaction with these components. Different biometric recognition systems may have different set of sensors, sub-systems, algorithms, to achieve the objective of specific pattern recognition and matching. Here we are covering architecture of a biometric access control system for restricted areas based on individual finger print.

Following is the block diagram of basic fingerprint recognition system architecture:



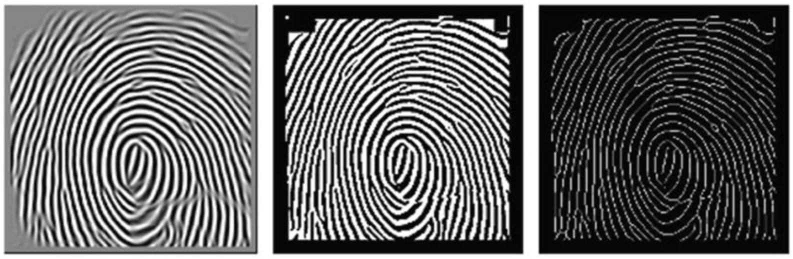
Block diagram of a fingerprint biometric system

Fingerprint sensor

Digital image of fingerprint patterns is captured by an electronic device called a fingerprint sensor. The captured image is called a live scan. This live scan is digitally processed to create a biometric template. A biometric template is a collection of extracted minutiae points, which is stored in a biometric data base and used for identification and verification. Fingerprint scanner is a vital part of a data capture sub-system of a biometric system and other sub-systems depends on the data sampled by it. Fingerprint sensors are improving as technology advances, still there may be certain conditions that can adversely affect the scanned fingerprint image. These image shortcomings are addressed by image processing sub-system.

Image processing

Extraction of minutiae from the scanned fingerprint image is a crucial stage. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In order to ensure that the performance of an automatic fingerprint identification/verification system will be robust with respect to the quality of the fingerprint images, it is essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module.



(a) Enhanced image. (b) Binirization image. (c) Thinned image.

Fingerprint images after applying different enhancements

Image segmentation, Normalization, Orientation Estimation, Ridge Frequency Estimation, etc. are the techniques applied to enhance the image quality in terms of usability for minutia extraction. Most minutiae extraction algorithms operate on binary images where there are only two levels of interest: the black pixels that represent ridges, and the white pixels that represent valleys. Binarization is the process that converts a grey level image into a binary image. The final image enhancement step typically performed prior to minutiae extraction is thinning. Thinning is a morphological operation that successively erodes away the foreground pixels until they are one pixel wide.

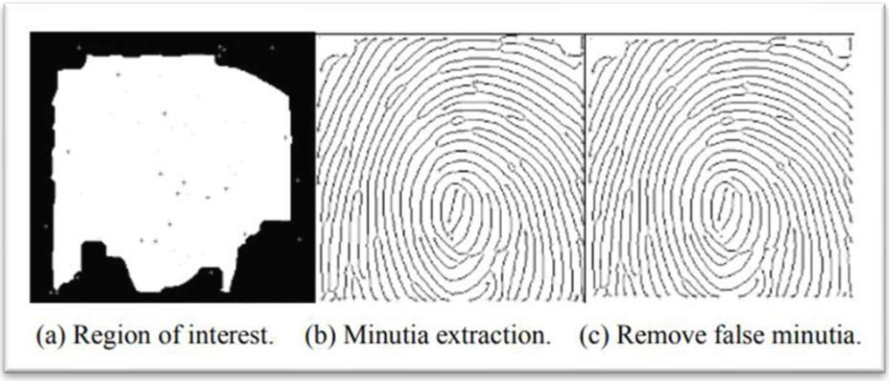
Minutia extraction and post processing

The most commonly employed method of minutiae extraction is the crossing number (CN) concept. This method involves the use of the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighbourhood of each ridge pixel in the image using a 3 x 3 window. False minutiae may be introduced into the image due to factors such as noisy images, and image artifacts created by the thinning process. Hence, after the minutiae are extracted, it is necessary to employ a post processing stage in order to validate the minutiae. A minutiae validation algorithm is employed for the purpose. For example, the minutiae validation algorithm by Tico and Kuosmanen tests the validity of each minutiae point by scanning the skeleton image and examining the local neighbourhood around the point.

Minutia match

Given two sets of minutia of two fingerprint images, the minutia match algorithm determines whether the two minutia sets are from the same finger or not. It includes two consecutive stages: one is alignment stage and the second

is match stage.



The result of minutia extraction process and removal of false minutia

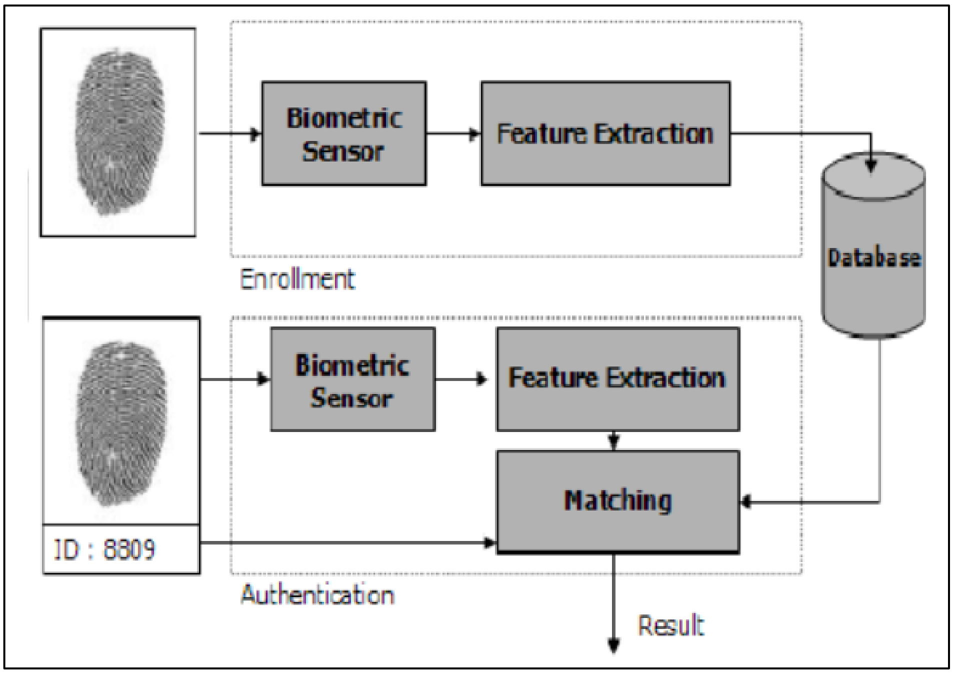
In the alignment stage, given two fingerprint images to be matched, choose any one minutia from each image; calculate the similarity of the two ridges associated with the two referenced minutia points. If the similarity is larger than a threshold, transform each set of minutia to a new coordination system whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point. And in match stage, after we get two set of transformed minutia points, we use the elastic match algorithm to count the matched minutia pairs by assuming two minutia having nearly the same position and direction are identical.

Stages of Fingerprint Authentication

Fingerprint identification is an automatic pattern recognition system with three fundamental stages:

1. Data acquisition
2. Feature extraction
3. Matching

The general system architecture of Fingerprint Authentication is depicted in Fig.



General Architecture of Biometric Authentication

1.Data acquisition:

This is the stage in which data (fingerprint) is acquired through a User interface. The obtained image is stored in database. The proposed system uses Futronic FS88 fingerprint scanner as user interface.

2.Feature extraction:

In this task the features of finger prints are extracted and stored along with its details in the system database. When the fingerprint images are fed to feature extraction module, a feature extraction algorithm is first applied to the image and its features are extracted .The proposed system consists of SVD (Singular Value Decomposition) based feature extraction.

3.Matching:

The main task of this module is to authenticate identity of a person who intends to access the system. This is the decision making the stage in the architecture. The person to be authenticated indicates his/her identity and places his finger on fingerprint user interface device. A fingerprint image is captured and is fed to a matching module. It extracts the features of the new image and matches with the person’s pattern templates stored in the system database. The proposed system consists of Euclidean distance based matching. It involves computation of Euclidean distance between two corresponding SVD points the fingerprint images and comparing it with the threshold.

Conclusion:

Biometric Authentication tools help organizations protect data and identify fraudulent activities. Biometric tools establish trust with businesses, improve their user's experiences and provide optimal security. Biometric system architecture defines fundamental organization of a biometric system, embodied in its components, their relationships to each other and to the environment, and the principles governing its design and evolution. System architecture is the conceptual model that defines the structure, behaviour, and more views of a system. Keeping things right is crucial in biometric systems architecture as a flaw in any component or sub-system can adversely affect the overall system performance. An efficiently designed biometric system serves what it is designed for. If we get down to the business, biometric systems save time, a lot of it. Expedited identification and verification processes help people clear queue faster and save time. To conclude, the usage of biometric systems will increase a lot more in future with the support of stable technologies and more cost effectiveness.