A

Seminar report

on

# BIOMETRICS

Submitted in partial fulfillment of the requirement for the award of degree
Of MCA

www.studymafia.org

**SUBMITTED TO:**

www.studymafia.org

**SUBMITTED BY:**

www.studymafia.org

# Preface

I have made this report file on the topic **BIOMETRICS** , I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to …………..who assisting me throughout the prepration of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

www.studymafia.org

# Contents

www.studymafia.org

# Introduction

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives.

Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and cost effective.

More information about biometrics, standards activities, government and industry organizations and research initiatives on biometrics can be found throughout this website.

www.studymafia.org

## History

There are evidences of biometric uses on human history as early as prehistorical age. Estimated 31000 years old caves are adorned with prehistorical pictures apparently signed by fingerprints stamps of authors. Another evidence is the use of fingerprints by Babylonian at 500 B.C. They used to record business transactions on clay tables in which were found fingerprint stamps.

The first reported use of biometrics was related by portuguese explorer Joâo de Barros in the 14th century. He described the practice of chinese merchants of stamp children´s palmprints and footprint to distinguish from one another.

The first real biometric system was created in 1870 by french anthropologist Alphonse Bertillion and turned biometrics a distinguished field of study. He developed an identification system (Bertillonage) based on detailed records of body measurement, physical description and photographs.

Despite their imprecise measures and difficulty to apply methodology, the Bertillonage was an important advance on criminal and people identification. It began to fail when it was discovered that many people share the same anthropologic measures.

The first classification method for fingerprints was developed in 1892 by Sir. Francis Galton. The features used by Galton´s method were the minutiae that are still used nowadays.

Some years later in 1896, Sir Edward Henry General Inspector of the Bengal police, began to use Galton´s method to replace the antropometrics system for identification of criminals. Henry created a method to classify and store fingerprint that lets a quick searching of records. Later, that method was introduced by Henry in London for the first British fingerprint file.

www.studymafia.org

## Types of Biometrics

**There are two types of biometrics.**

**1.Behavioral biometrics**- Used for verification .
**2.Physical biometrics**- Used for either identification or verification.

**Physical biometrics:**

- Fingerprint- Analyzing fingertip patterns.
- Facial Recognition- Measuring facial characteristics.
- Hand Geometry- Measuring the shape of the hand.
- Iris recognition- Analyzing features of colored ring of the eye.
- Vascular Patterns- Analyzing vein patterns.
- Retinal Scan- Analyzing blood vessels in the eye.
- Bertillonage- Measuring body lengths (no longer used).

**Behavioral biometrics:**

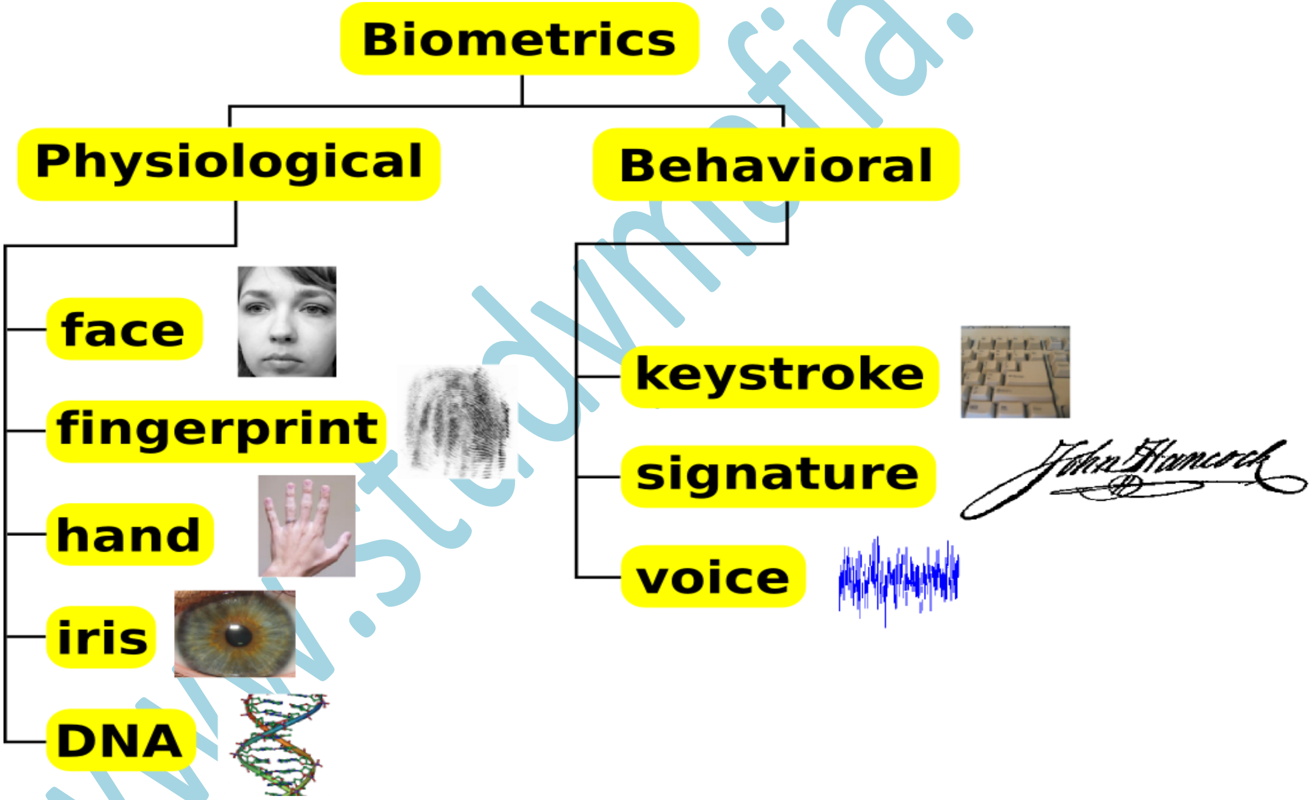
- Speaker Recognition- Analyzing vocal behavior.
- Signature- Analyzing signature dynamics.
- Keystroke- Measuring the time spacing of typed words.

www.studymafia.org

## Characteristics of Biometric

**Biometric characteristics** can be divided in two main classes:

- **Physiological** are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition (which has largely replaced retina recognition), and odor/scent.
- **Behavioral** are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term "behaviometrics" for this class of biometrics.



www.studymafia.org

# Applications

In the last years has considerably increased the area of application of biometrics and it's expected that in the near future, we will use biometry many times in our dayly activities such as getting in the car, openning the door of our house, accessing to our bank acount, shoping by internet, accessing to our PDA, mobil phone, laptops, etc.

Depending of where the biometrics is deployed, the applications can be categorized in the following five main groups: forensic, government, commercial, health-care and traveling and immigration. However, some applications are common to these groups such as physical access, PC/network access, time and attendance, etc.

## Forensic

The use of biometric in the law enforcement and forensic is more known and from long date, it is used mainly for identification of criminals. In particular, the AFIS (automatic fingerprint identification system) has been used for this purpose.

Lately the facial-scan technology (mug shots) is being also used for identification of suspects. Another possible application is the verification of persons of home arrest, a voice-scan is an attractive solution for this problem. The typical application are:

- **Identification of criminals-** collecting the evidence in the scene of crime (e.g., fingerprints) it is possible to compare with data of suspects or make a search in the database of criminals.
- **Surveillance** --using cameras one can monitor the very busy places such as stadiums, airports, meetings, etc. Looking in the crowds for suspect, based on the face recognition biometric, using a images (e.g., mug shots) database of wanted persons or criminals. Since the events of September 11, 2001, the interest in biometric surveillance has increased dramatically, especially for air travel applications. Currently there are many cameras monitoring crowds at airports for detecting wanted terrorists.
- **Corrections -**This refers to the treatment of offenders (criminals) through a system of penal incarceration, rehabilitation, probation, and parole, or the administrative system by which these are effectuated. Is this cases a biometric system can avoid the possibility of accidentally releasing the wrong prisoner, or to ensure that people leaving the facilities are really visitors and not inmates.
- **Probation and home arrest -** biometric can also be used for post-release programs (conditional released) to ensure the fulfilment of the probation, parole and home detention terms.

www.studymafia.org

## Government

There are many application of the biometry in the government sector. An AFIS is the primary system used for locating duplicates enrolls in benefits systems, electronic voting for local or national elections, driver's license emission, etc. The typical application are:

- **National Identification Cards -** the idea is to include digital biometric information in the national identification card. This is the most ambitious biometric program, since the identification must be performed in a large-scale database, containing hundred of millions samples, corresponding to the whole population of one country.

  This kind of cards can be used for multiple purposes such as controlling the collection of benefits, avoiding duplicates of voter registration and drivers license emission. All this applications are primarily based on finger-scan and AFIS technology, however it is possible that facial-scan and iris-scan technology could be used in the future.

- **Voter ID and Elections -** while the biometric national ID card is still in project, in many countries are already used the biometry for the control of voting and voter registration for the national or regional elections. During the registration of voter, the biometric data is captured and stored in the card and in the database for the later use during the voting. The purpose is to prevent the duplicate registration and voting.
- **Driver's licenses -** In many countries the driver license is also used as identification document, therefore it is important to prevent the duplicate emission of the driver license under different name. With the use of biometric this problem can be eliminated. however it is important that the data must be shared between state, because in some country such as United States, the license are controlled at the states as opposed to the federal level.
- **Benefits Distribution (social service) -** the use of biometry in benefits distribution prevents fraud and abuse of the government benefits programs. Ensuring that the legitimate recipients have a quick and convenient access to the benefits such as unemployment, health care and social security benefits.
- **Employee authentication -** The government use of biometric for PC, network, and data access is also important for security of building and protection of information. Below are more detailed this kind of applications also used in commercial sector.
- **Military programs -** the military has long been interested in biometrics and the technology has enjoyed extensive support from the national security community.

## Commercial

Banking and financial services represent enormous growth areas for biometric technology, with many deployments currently functioning and pilot project announced frequently. Some applications in this sector are:

www.studymafia.org

- **Account access -** The use of biometric for the access to the account in the bank allows to keep definitive and auditable records of account access by employees and customers. Using biometry the the customers can access accounts and employees can log into their workstations.
- **ATMs -** the use of biometric in the ATM transaction allows more security,
- **Expanded Service Kiosks -** A more receptive market for biometrics may be special purpose kiosks, using biometric verification to allow a greater variety of financial transaction than are currently available though standard ATMs.
- **Online banking -** Internet based account access is already widely used in many places, the inclusion of biometric will make more secure this type of transactions from home. Currently, there are many pilot programs using biometric in home banking.
- **Telephony transaction -** Voice-scan biometric can be used to make more secure the telephone-based transactions. In this type of application, when the costumer calls to make a transaction, a biometric system will authenticate the customer's identity based on his or her voice with no need of any additional device.
- **PC/Network access -** The use of biometric log-in to local PCs or remotely through network increase the security of the overall system keeping more protected the valuable information.
- **Physical access -** the biometric is widely used for controlling the access to building or restricted areas.
- **E-commerce -** biometric e-commerce is the use of biometrics to verify of identity of the individual conduction remote transaction for goods or services
- **Time and attendance monitoring -** In this sector the biometrics is used for controlling the presence of the individuals in a determine area. For example for controlling the time sheet of the employees or the presence of students at the classroom

## Health Care

The applications in this sector includes the use of biometrics to identify or verify the identity of individuals interacting with a health-care entity or acting in the capacity of health-care employee or professional. The main aim of biometrics is to prevent fraud, protect the patient information and control the sell of pharmaceutical products. Some typical application are:

- **PC/Network Access -** the biometrics are used to control a secure access of the employees to the hospital network, primarily, in order to protect the patient information,
- **Access to personal information -** Using biometrics, the medical patient information maybe stored on smart card or secure networks, this will enable the access of the patients to their personal information.

www.studymafia.org

- **Patient identification -** In case of emergency, when a patient does not have identification document and is unable no communicate, biometric identification may be a good alternative to identify.

## Travel and Immigration

The application in this sector includes the use of biometrics to identify or verify the identity of individual interacting during the course of travel, with a travel or immigration entity or acting in the capacity of travel or immigration employee. Typical application are:

- **Air travel -** In many airport are already used a biometric system in order to reduce the inspection processing time for authorized travelers.
- **Border crossing -** The use of biometrics to control the travelers crossing the national or state border is increasing, specially in regions with high volume of travelers or illegal immigrants.
- **Employee access -** Several airport use biometric to control the physical access of employees to secure areas.
- **Passports -** Some country already issues passports with biometric information on a barcode or smart chips. The use of biometrics prevent the emission of multiple passports for the same person and also facilitates the identification at the airports and border controls.

www.studymafia.org

## Biometric Modality

There is no single biometric modality that is best for all implementations. Commonly implemented or studied biometric modalities include: Fingerprint, face, iris, voice, signature and hand geometry. Many other modalities are in various stages of development and assessment.

Many factors must be taken into account when implementing a biometric system, including but not limited to: physical location, security risks, task (identification or verification), expected number of end users, user circumstances.. Each biometric modality has its own strengths and weaknesses that must be evaluated in relation to the application before implementation.

The effectiveness of a particular implementation of biometric technology is dependent on how and where the technology is used.

Key decision factors for selecting a particular biometric technology for a specific application includes but is not limited to:

- The environment
- Throughput needs (the required speed of the transaction)
- Costs associated with obtaining and storing templates and conducting biometric recognition
- Population size and demographics
- Ergonomics
- Interoperability with existing systems
- Other user considerations — for instance, an access control system to a coal mine, where individuals might have very worn and/or dirty fingerprints, will not be a suitable environment for a fingerprint reader.

www.studymafia.org

# Biometric Devices

## Iris Scanner

Iris cameras perform recognition detection of a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. It combines computer vision, pattern recognition, statistical inference and optics.

Of all the biometric devices and scanners available today, it is generally conceded that iris recognition is the most accurate. The automated method of iris recognition is relatively young, existing in patent since only 1994.

Iris cameras, in general, take a digital photo of the iris pattern and recreating an encrypted digital template of that pattern. That encrypted template cannot be re-engineered or reproduced in any sort of visual image. Iris recognition therefore affords the highest level defence against identity theft, the most rapidly growing crime.

The imaging process involves no lasers or bright lights and authentication is essentially non-contact. Today's commercial iris cameras use infrared light to illuminate the iris without causing harm or discomfort to the subject.

The iris is the coloured ring around the pupil of every human being and like a snowflake, no two are alike. Each are unique in their own way, exhibiting a distinctive pattern that forms randomly in utero. The iris is a muscle that regulates the size of the pupil, controlling the amount of light that enters the eye.

www.studymafia.org

Iris recognition is rarely impeded by glasses or contact lenses and can be scanned from 10cm to a few meters away. The iris remains stable over time as long as there are no injuries and a single enrolment scan can last a lifetime.

Some medical and surgical procedures can affect the overall shape and colour of an iris but the fine texture remains stable over many decades. Even blind people can use this scan technology since iris recognition technology is iris pattern-dependent not sight dependent.

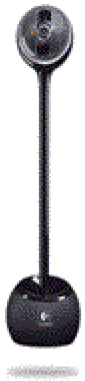
Iris scanning is an ideal way of biometric identification since the iris is an internal organ that is largely protected by damage and wear by the cornea. This makes it more attractive then fingerprints which can be difficult to recognize after several years of certain types of manual labour.

## Fingerprint Scanner

A fingerprint scanner is an electronic device used to capture a digital image of the fingerprint pattern. This scan is digitally processed to create a biometric template which is stored and used for matching.

www.studymafia.org

## Face Camera



Face detection is used in biometrics, often as a part of (or together with) a facial recognition system. It is also used in video surveillance, human computer interface and image database management. A face camera is a webcam with 2 Mpx or above which can take a clear crisp photograph of the face.

Some recent digital cameras use face detection for autofocus. Also, face detection is useful for selecting regions of interest in photo slideshows that use a pan-and-scale Ken Burns effect. That is, the content of a given part of an image is transformed into features, after which a classifier trained on example faces decides whether that particular region of the image is a face, or not.

A face model can contain the appearance, shape, and motion of faces. There are several shapes of faces. Some common ones are oval, rectangle, round, square, heart, and triangle. Motions include, but not limited to, blinking, raised eyebrows, flared nostrils, wrinkled forehead, and opened mouth.

The face models will not be able to represent any person making any expression, but the technique does result in an acceptable degree of accuracy. The models are passed over the image to find faces, however this technique works better with face tracking. Once the face is detected, the model is laid over the face and the system is able to track face movements.

www.studymafia.org

## Advantages of Biometrics

• Increase security -Provide a convenient and low-cost additional tier of security.
• Reduce fraud by employing hard- to- forge technologies and materials. For e.g. Minimize the opportunity for ID fraud, buddy punching.
• Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. prevent unauthorized use of lost, stolen or "borrowed" ID cards.
• Reduce password administration costs.
• Replace hard-to-remember passwords which may be shared or observed.
• Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access.
• Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!
• Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance.
• Unequivocally link an individual to a transaction or event.

www.studymafia.org

# Conclusion

Biometrics can only be limited by limiting one's imagination. Biometric technology is now being used in almost every area. Not only that, but various types of biometric systems are being used to achieve various functionalities.

We have short listed a few highly popular applications of biometrics technology. Although this list is no way complete it is simply an effort to list a few of the more popular biometric applications.

www.studymafia.org