CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

Biometrics are known as the science and technology of measuring and analyzing biological data. Biometric systems are used in two different modes such as verification (authentication) and identification. Human physiological and behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

i. **Uniqueness:** No two persons should have the same characteristic, and each relevant person should only have one original characteristic.

ii. **Universality:** This characteristic must exist in all individuals in the population being measured.

iii. **Permanence:** This characteristic should be time-invariant and must be a permanent part of the individual.

iv. **Authentication:** The characteristic must be able to match against similar characteristics and a positive or negative match must be able to made based on the measurement.

v. **Collectability:** The characteristic can be measured. However, in a practical biometric system i.e., a system that employs biometrics for personal recognition.

In this research, a biometric authentication system using brain signature is developed and validated using experimental identification.

The term biometrics is derived from the Greek word bio (life) and metric (to measure) automated biometric system have only become available over the last few decades, due to significant advances in the field of computer processing, many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousand of year ago. Biometrics refers to the automatic recognition of individuals based on
their physiological and behavioral characteristics. The biometric characteristics can be divided in two main classes:

1) Physiological are related to shape of the body. For examples fingerprint, face recognition, hand geometry, iris recognition and retina which has largely replaced retina, and odor/scent.
   a. Fingerprint: The analysis of an individual’s unique fingerprints
   b. Face recognition: The analysis of the facial characteristics
   c. Hand geometry: The analysis of the shape of the hand and the length of the fingers
   d. Iris recognition: The analysis of the colored ring that surrounds the eye ‘s pupil
   e. Retina: The analysis of the capillary vessels located at the back of the eye.

2) Behavioral are related to behavior of a person. For examples typing rhythm, gait, and voice. Some researchers have coined the term behavioral metrics for this class of biometrics.
   a) Signature: The analysis of the way a person signs his name
   b) Vein: The analysis of pattern of veins in the back if the hand and the wrist
   c) Voice: The analysis of the tone, pitch, cadence and frequency of a person’s voice.

A biometric system is essentially a pattern recognition system that recognizes an individual by comparing the binary code of a uniquely specific biological or physical characteristic to the binary code of the stored characteristic. Samples are taken from individuals to check if there is any similarity to biometric references previously taken from known individuals. The system then applies a specialized mathematical algorithm to the sample and converts it into a binary code and then compares it to the template sample to determine if the individual can be recognized. A reference model or reference containing the biometric properties of a person is stored in the system generally after data compression by recording their individual characteristics. These characteristics may be acquired several times
during enrollment in order to get a reference profile that corresponds most with reality (Jain et al., 2004).

This measurable characteristic the biometric, can be primarily anatomical such as eye, face, finger image, hand, and voice or primary behavioral such as signature and typing rhythm, but most biometrics combine both anatomical and behavioral components. The biometric system must be able to identify a person based on one or a combination of these biometric identifiers quickly, automatically, and with little or no human intervention in the decision. They include the following:

A. Fingerprint Verification
B. Hand Geometry
C. Speaker Verification
D. Retinal Scanning
E. Iris Scanning
F. Facial Recognition

Biometrics is a very attractive technology, because it can be integrated into any application requiring security or access control, effectively eliminating risks associated with less advanced technologies. Iris recognition is extremely accurate, but expensive to implement and needs the cooperation of the person. Fingerprints are reliable and non-intrusive but not suitable for non-collaborative individuals (Jain et al., 2000). Some of the drawbacks of the existing biometric system are summarized below:

A. **Fingerprint**
   1. Has rationally been associated with criminal activities and thus users could be reluctant to adopt this for biometric authentication
   2. Social stigma such that it is related to literate
   3. Variation occurs due to age, cut or due to working condition
   4. Rare situations like people without fingers
B. Hand Geometry
   1. Not unique to every user
   2. Physical contact includes public hygiene
   3. Not very distinctive
   4. Mutation

C. Speaker Verification
   1. Background noise must be controlled for accurate verification
   2. Large storage space required
   3. Easily influenced circumstances such as sore throat, common cold
   4. Possibility of voice imitation
   5. Possibility of creating nonexistent identities with text to speech technology
   6. Possibility in rare case where voice is lost

D. Retina Scans
   1. Extremely intrusive
   2. Low user acceptance rate
   3. Extremely expensive

E. Iris Recognition
   1. Sampling the iris patterns requires much user cooperation or complex
   2. Expensive input device
   3. Iris authentication is hampered by vision aid
   4. A lot of memory for the data to be stored

F. Facial Recognition
   1. Data acquisition is difficult, user must face in same position each access, background lighting important for accurate verification
   2. Face authentication requires images taken in a good controlled lighted environment
   3. Disguise-a major obstacle
   4. Usage may hamper due to social stigma
EEG as a biometric is relatively new compared to other biometrics. This modality has several advantages:

i. It is confidential (as it corresponds to a biometric task)

ii. It is difficult to mimic (as similar mental tasks are person dependent)

iii. It is almost impossible to steal (as brain activity is sensitive to stress and the mood of the person to produce his/her mental pass-phrase).

1.2 BIOMETRIC SYSTEMS

A biometric system or a biometric device is a real-time system which recognizes a person by measuring a particular physical or behavioral characteristic and later comparing it to a library of characteristics belonging to one or many people (Ashbourn et al., 2003). The architecture of the system is dependent on whether it is used for verification and identification.

- **Verification**: In this mode, the system performs a one-to-one search, comparing the captured biometric data with the biometric templates stored in the system database. If a match is made, the identity of the person is verified.

- **Identification**: This mode is used when the identity of the individual is not known in advance. The entire template database is then searched for a match to the individual concerned in a one-to-many search. If a match is made, the individual is identified.

1.2.1 Applications of Biometric Systems

The applications of biometrics can be divided into the following three main groups.

- **Commercial** applications include Computer Network Login, Electronic Data Security, E-Commerce, Internet Access, ATM, Credit Card, Physical Access Control, Cellular Phone, Medical Records Management, and Distance Learning.
- **Government** applications are Aadhaar - National ID Card, Correctional Facility, Driver’s License, Social Security, Welfare Disbursement, Border Control, And Passport Control.
- **Forensic** applications such as Corpse Identification, Criminal Investigation, Terrorist Identification, Parenthood Determination and Missing Children (Daugman et al., 1999).

### 1.3 ELECTROENCEPHALOGRAM (EEG)

EEG records the electrical activity of the brain. EEG is a technique that reads scalp electrical activity generated by brain structures. Local current flows are formed when brain cells are activated. EEG measures in generally current flows during synaptic excitations of the dendrites of many pyramidal neurons in the cerebral cortex. Brain cells produce tiny electrical impulse that facilitates thought, memory and motion to communicate. The existence of electrical currents in the brain was discovered in 1875 by a Liverpool surgeon named Richard Caton 1842-1926. He studied action potentials from the exposed brains of rabbits and monkeys. Hans Berger 1873-1941, a German neuropsychiatrist. In 1924, he used his ordinary radio equipment to amplify the brain’s electrical activity measured on the human scalp. Berger was the first to use the word “Electroencephalogram” to describe the brain electric potentials in humans. He placed the foundations for many of the present applications for EEG and as a result, which earned him the title as “Father of EEG” (Tudor et al., 2005).

### 1.4 PROBLEM STATEMENT

Many biometric techniques commercially available have many drawbacks as discussed which fail safe biometric. Biometric technology systems available today are not suitable for high security authentication system as they can be easily duplicated. The proposed biometric system using brain signatures is verified for its application in authentication system.
1.5 THESIS OBJECTIVES

This research has three main objectives namely,

1. To develop suitable protocols for EEG brain signal acquisition from biometric tasks.
2. To develop suitable feature extraction and classification algorithms for verifying individuals.
3. To design and development of a Graphical User Interface (GUI) for biometric verification from brain signature.

1.6 THESIS ORGANIZATION

The research work towards developing biometric authentication system using brain signature is presented with detail data acquisition of EEG signal, preprocessing, feature extraction, neural network and design a graphical user interface. The thesis is organized as follows.

Chapter 1 presents a brief overview of the research, such as introduction of biometrics, working principle, processing techniques and advantages and disadvantages of existing biometric techniques. EEG, problem statement, objective of thesis and thesis organization are also discussed here.

Chapter 2 discusses the review of literature which is a critical outlook at the existing research that is significant to the work carried out. This chapter briefly introduces the background knowledge and surrounding information about this research on the fundamentals of EEG, EEG rhythms, EEG based person authentication and identification, feature extraction and classification techniques. The work of several researchers are quoted and used as an evidence to support the concepts explained in this research work.

Chapter 3 explains the proposed methodology and various phases of research. The overall architecture is discussed here. This chapter elucidates EEG electrode placement, electrode
type and data collection for single channel and two channel systems and preprocessing is done.

Chapter 4 discusses feature extraction techniques used in the proposed research, namely parametric, non-parametric and high resolution method. Basic artificial neural network and various designing parameters of neural network.

Chapter 5 tabulates, discusses and compares the classification and single trial analysis results obtained while testing the proposed system.

Chapter 6 concludes the proposed study. It also discusses the completion of proposed objectives and scope of future extension.