Behavioral biometrics pertains to the behavior exhibited by people or the manner in which people perform tasks such as walking, signing, and typing on the keyboard.

Behavioral biometrics modalities have higher variations as they primarily depend on the external factors such as fatigue, mood, etc. This causes higher FAR and FRR as compared to solutions based on a physiological biometrics.

**Gait Recognition**

**Gait** is the manner of a person’s walking. People show different traits while walking such as body posture, distance between two feet while walking, swaying, etc., which help to recognize them uniquely.

A gait recognition based on analyzing the video images of candidate’s walk. The sample of candidate’s walk cycle is recorded by Video. The sample is then analyzed for position of joints such as knees and ankles, and the angles made between them while walking.

A respective mathematical model is created for every candidate person and stored in the database. At the time of verification, this model is compared with the live sample of the candidate walk to determine its identity.

**Merits of Gait Recognition System**

- It is non-invasive.
- It does not need the candidate’s cooperation as it can be used from a distance.
- It can be used for determining medical disorders by spotting changes in walking pattern of a person in case of Parkinson’s disease.

**Demerits of Gait Recognition System**

- For this biometric technique, no model is developed with complete accuracy till now.
- It may not be as reliable as other established biometric techniques.

**Application of Gait Recognition System**
It is well-suited for identifying criminals in the crime scenario.

**Signature Recognition System**

In this case, more emphasis is given on the behavioral patterns in which the signature is signed than the way a signature looks in terms of graphics.

The behavioral patterns include the changes in the timing of writing, pauses, pressure, direction of strokes, and speed during the course of signing. It could be easy to duplicate the graphical appearance of the signature but it is not easy to imitate the signature with the same behavior the person shows while signing.

This technology consists of a pen and a specialized writing tablet, both connected to a computer for template comparison and verification. A high quality tablet can capture the behavioral traits such as speed, pressure, and timing while signing.

During enrollment phase, the candidate must sign on the writing tablet multiple times for data acquisition. The signature recognition algorithms then extracts the unique features such as timing, pressure, speed, direction of strokes, important points on the path of signature, and the size of signature. The algorithm assigns different values of weights to those points.

At the time of identification, the candidate enters the live sample of the signature, which is compared with the signatures in the database.

**Constraints of Signature Recognition System**

- To acquire adequate amount of data, the signature should be small enough to fit on tablet and big enough to be able to deal with.

- The quality of the writing tablet decides the robustness of signature recognition enrollment template.

- The candidate must perform the verification processes in the same type of environment and conditions as they were at the time of enrollment. If there is a change, then the enrollment template and live sample template may differ from each other.

**Merits of Signature Recognition System**

- Signature recognition process has a high resistance to imposters as it is very difficult to imitate the behavior patterns associated with the signature.

- It works very well in high amount business transactions. For example, Signature recognition could be used to positively verify the business representatives involved in the transaction before any classified documents are opened and signed.

- It is a non-invasive tool.

- We all use our signature in some sort of commerce, and thus there are virtually no privacy rights issues involved.

- Even if the system is hacked and the template is stolen, it is easy to restore the template.

**Demerits of Signature Recognition System**
- The live sample template is prone to change with respect to the changes in behavior while signing. For example, signing with a hand held in plaster.

- User need to get accustomed of using signing tablet. Error rate is high till it happens.

**Applications of Signature Recognition System**

- It is used in document verification and authorization.

- The Chase Manhattan Bank, Chicago is known as the first bank to adopt Signature Recognition technology.

**Keystroke Recognition System**

During the World War II, a technique known as *Fist of the Sender* was used by military intelligence to determine if the Morse code was sent by enemy or ally based on the rhythm of typing. These days, keystroke dynamics is the easiest biometric solution to implement in terms of hardware.

This biometric analyzes candidate’s typing pattern, the rhythm, and the speed of typing on a keyboard. The **dwell time** and **flight time** measurements are used in keystroke recognition.

**Dwell time** – It is the duration of time for which a key is pressed.

**Flight time** – It is the time elapsed between releasing a key and pressing the following key.

The candidates differ in the way they type on the keyboard as the time they take to find the right key, the flight time, and the dwelling time. Their speed and rhythm of typing also varies according to their level of comfort with the keyboard. Keystroke recognition system monitors the keyboard inputs thousands of times per second in a single attempt to identify users based on their habits of typing.

There are two types of keystroke recognition –

- **Static** – It is one time recognition at the start of interaction.

- **Continuous** – It is throughout the course of interaction.

**Application of Keystroke Dynamics**

- Keystroke Recognition is used for identification/verification. It is used with user ID/password as a form of **multifactor authentication**.

- It is used for surveillance. Some software solutions track keystroke behavior for each user account without end-user’s knowledge. This tracking is used to analyze if the account was being shared or used by anyone else than the genuine account owner. It is used to verify if some software license is being shared.

**Merits of Keystroke Recognition System**
- It needs no special hardware to track this biometric.
- It is a quick and secure way of identification.
- A person typing does not have to worry about being watched.
- Users need no training for enrollment or entering their live samples.

**Demerits of Keystroke Recognition System**

- The candidate’s typing rhythm can change between a number of days or within a day itself because of tiredness, sickness, influence of medicines or alcohol, change of keyboard, etc.
- There are no known features dedicated solely to carry out discriminating information.