*Impact Factor (SJIF): 3.632*

**International Journal of Advance Research in Engineering, Science & Technology**

*e-ISSN: 2393-9877, p-ISSN: 2394-2444*

***(Special Issue for ITECE 2016)***

# Gait Authentication

**Shruti Saiparia [1], Kuldeep Jindani[2], Jay Tevani[3]**

[1]*Computer Science & Engineering, SLTIET*
[2]*Computer Science & Engineering, SLTIET*
[3]*Computer Science & Engineering, SLTIET*

***Abstract*** *— This paper describes Gait Authentication which is an emerging biometric technology which involves people being identified purely through the analysis of the way they walk. It has attracted interest as a method of identification because it is non-invasive and does not require the subject's cooperation. This paper presents approaches of Biometric gait recognition and security and challenges of it as well. There are three types of Biometric gait recognition: machine vision, wearable sensor and floor sensor. Gait patterns are extracted from physical device which is attached with lower leg. From output of device acceleration in three directions are noticed: vertical, forward-backward and sideways motion of lower leg. Two different methods are used for authentication: histogram and cycle length. In histogram equal error rate is 5% and in cycle length it is 9%.This paper contain cycle length detection. In this paper we have discussed on spoof attacks on Gait authentication systems as well.*

***Keywords:*** *Biometric authentication, Gait authentication, Histogram, Cycle-length, Prototype sensor mat*

## I. INTRODUCTION

Mobile ad-hoc network is formed by the collection of some mobile nodes which can act both as a sender as well as Authentication is used to check whether user is claimed or not. There are three types of authentication:

- Knowledge based,
- Token based,
- Biometric based

Knowledge based authentication means you have to know the passcode to prove that you are having rights to use.In token based authentication simply you need a key to open a lock. Token means here a hard-thing. Above both approach it is difficult to secure a passcode or a token. But in biometric based authentication you just have to prove who you are by your unique physical identity.

## II. APPROACHES FOR BIOMETRIC GAIT RECOGNITION

There are three approaches to user authentication based on biometric.

- Machine vision
- Wearable sensor
- Floor sensor

### 2.1 Machine Based Gait Recognition

Johnson and Bobick[1] derived static body parameters like height, distance between feet, distance between head and pelvis, the maximum distance between pelvis and feet and used them for Gait recognition. Mostly algorithms for MV based recognition consider human silhouette.

The primary advantage of MV-based recognition is in being captured from the distance when other biometrics are not accessible. Surveillance and forensics are usually application areas for MV-based gait recognition. Although it can't constitute identification in terms of fingerprints.

In figure 1 an example of DET curve is shown. For reporting performance of biometric system in verification mode, Researchers often use a decision error trade-off (DET) curves.

In figure 2 an example of CMC curve is shown. To evaluate the performance of a biometric system in identification mode, a cumulative match characteristics (CMC) curve can be used.

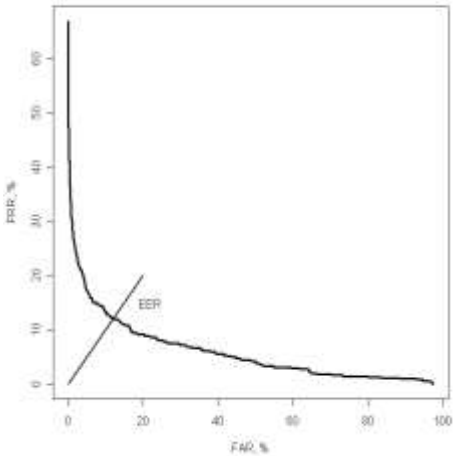


*Figure 1: An example of DET curve from [1]*

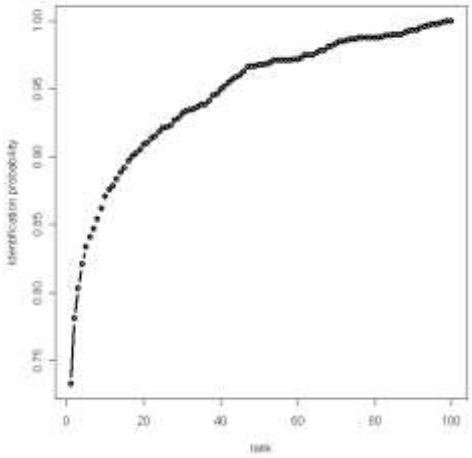


*Figure 2: An example of CMC curve from[1]*

### 2.2 Wearable-sensor Based Gait Recognition

In WS-based gait recognition, gait is collected using body worn motion recording (MR) sensors . The MR sensors can be worn at different locations on the human body. It can be attached with hip or lower leg[1]. The acceleration of gait, which is recorded by the MR sensor, is utilized for authentication. In the MR sensor was attached to the belt of the subjects, around the right hip as shown in Figure 3.

*Figure 3: The MR sensor attached to the hip from [1]*

*Figure 4: The MR sensor attached to the lower leg*

One of the main advantages of the WS-based gait recognition over several other biometric modalities is its unobtrusive data collection. The WS-based approach was proposed for protection and user authentication in mobile and portable electronic devices. With advances in miniaturization techniques it is feasible to integrate the MR sensor as one of the components in personal electronic devices

### 2.3 Floor-sensor Based Gait Recognition

In Floor-sensor approach, a set of sensors are installed on the floor as shown in figure:5.[1] Such sensors enable to measure features related to gait when a person walks on them. Orr and Abowd collected 1680 footstep profiles from 15 subjects. Using this data they achieved up to 93% correct recognition rate. FS- based features are stride length, stride cadence and time on toe to time on heel ratio for recognition. These features are 80% sufficient to recognize FS based data. One of the main advantages of FS-based gait recognition is in its unobtrusive data collection. The FS-based gait recognition can be deployed in access control application and is usually installed in front of doors in the building. Such systems can find deployment as a standalone system or as a part of multimodal biometric system. In addition to providing identity information, the FS-based gait system can also indicate location information within a building.

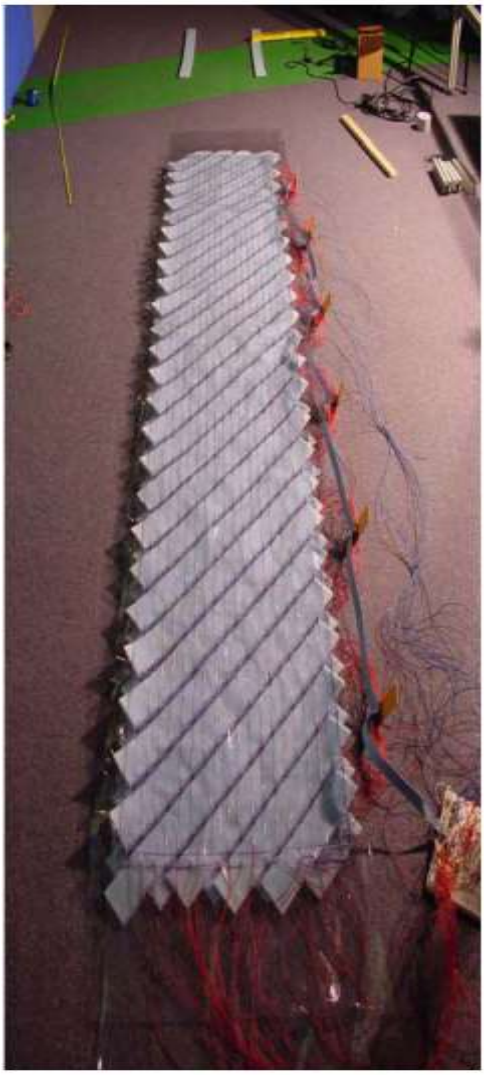

*Figure 5: A prototype sensor mat*

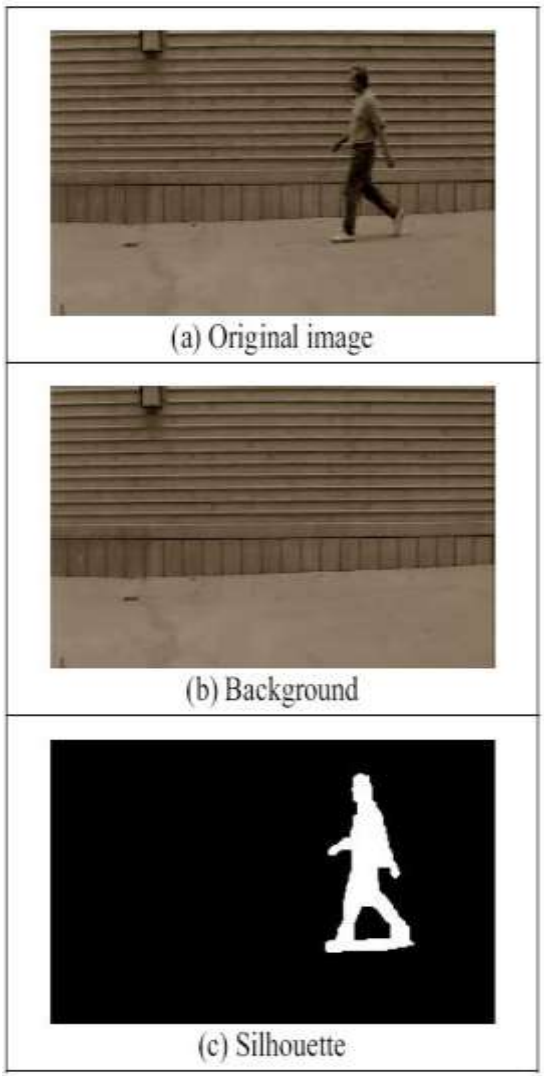


*Figure 6: An example of silhouette extraction*

## *III. GAIT RECOGNITION ALGORITHMS*

There are mainly two algorithms for Gait Recognition.

- Histogram
- Cycle length

### 3.1 Histogram

A n-bit histogram of combined gait signal is computed and then histogram readings are normalized by the number of recorded observations. For calculating distance metric between two histograms we use following formula. This formula [5]gives absolute distance.

$$dist(x,y) = \sum_{i=1}^{n} |x_i - y_i|.$$

Here $x_i$ is the probability of a data falling into bin I of the enrollment's normalized histogram x,
$y_i$ is the probability of a data point falling into bin I of the verification's normalized histogram y.
The distance value represents similarity score between two gait samples.

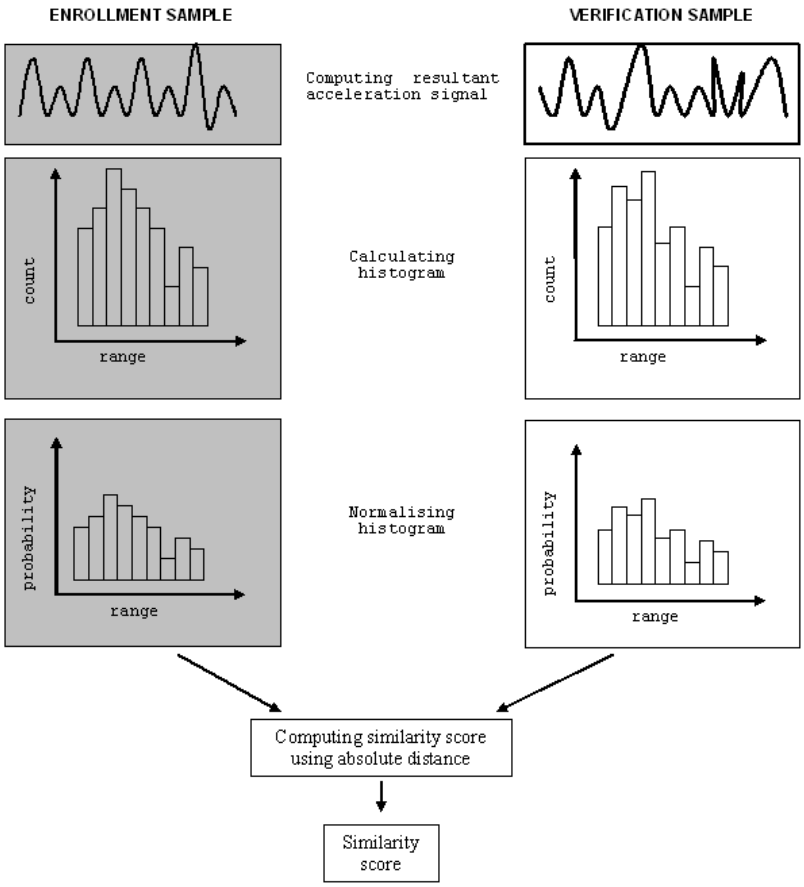


**Figure 7: The process of applying the histogram similarity method from [5]**

### 3.2 Cycle Length

The method is based on the comparison of gait cycle groups. The cycles are detected from the gait signal with help of the cycle length. The cycle groups are then created based on the observations point inside cycles. The cycle groups represent gait cycles as populations of general observation points. The idea of the comparison is to calculate similarity scores between corresponding groups and to create the similarity vector. The final comparison score is then determined based on the similarity vector.

**Finding the cycles**: The gait cycles are easiest to detect from the vertical acceleration signal. The data is first scaled by the formula [5],

$$x_{i_f} = x_{i_o} - \bar{x},$$

Where $x_{if}$ is a scaled value,
$x_{io}$ is an observed value and
$\bar{x}$ is the mean value of the data set.

After scaling the starting points of each cycle are observed, as shown in Figure 8.

**Cycle groups[5]**: The number of groups depends on the cycle length. The longer the cycle is, the more observation points there are in one cycle. The first observation points (points where acceleration is zero) from each cycle were collected to the first group $G_1$, the second observations from each cycle created the second group $G_2$, and so on until $G_{16}$. An example of the groups is presented in Figure 9.

**Comparison of groups[5]**: The ideal situation is that the person walks in a similar style all the time. His speed would be constant and his walking pattern would be the same. This would lead to equal gait cycles and therefore normally distributed gait groups because the values of the observation points at the same phase of the curve would be very close to each other. The variance of the cycle group would be very small and the mean value of the group could be used for comparison of the two different gait signals. Even though our experimental data represents far from ideal data set, the mean of the groups were still tested for comparison.

The similarity of the equal means for each group $G_i$ of persons A and B were calculated by two sample t-tests[5]:

$$T_i = \frac{\bar{G}_{Ai} - \bar{G}_{Bi}}{\sqrt{\frac{s_{Ai}^2}{N_{Ai}} + \frac{s_{Bi}^2}{N_{Bi}}}}.$$

The variances $s_{Ai}$ and $s_{Bi}$ of the groups were considered to be unequal. The sample size N is the same in all groups. After comparison between two persons datasets, the statistic value vector T contains 16 probability scores. In order to compare the statistical vectors, the final score value S was calculated. The final score comparisons were made based on the probability 0.27,

$$S = \sum_{i=1}^{16} s_i,$$

Where

$$\begin{cases} s_i = 1, \ if \ T_i \geq 0.27, \\ s_i = 0, \ otherwise. \end{cases}$$

The final similarity score S is then a value between 0 and 16.

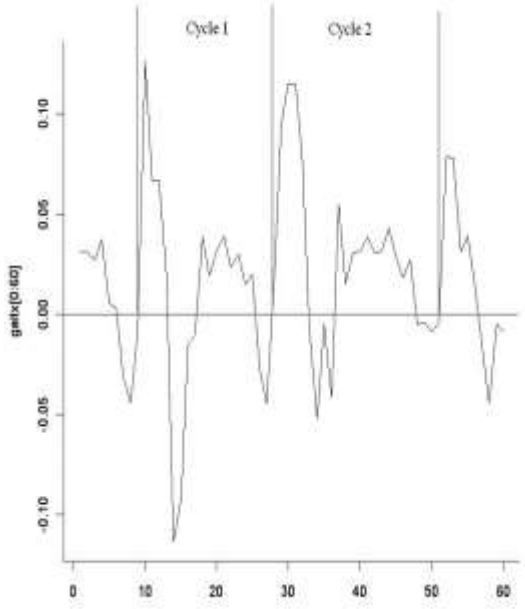


*Figure 8: Gait cycles from [5]*

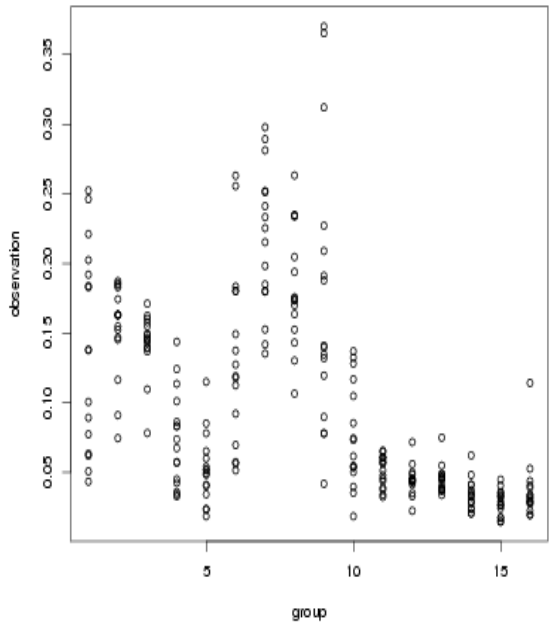


*Figure 9: Cycle group from[5]*

## *IV. ATTACKS ON GAIT BASED BIOMETRIC SYSTEM*

1) Typical points of attack on a biometric authentication system[3].
2) Presenting fake or imitated biometric to the sensor[7].
3) Submission of a previously obtained digital biometric sample[7].
4) The feature extractor is attacked so that it produces feature values dictated by the attacker[7].
5) Extracted feature values are substituted by the ones selected by the attacker in the fourth type of attack[4].
6) The score of the matcher is changed to produce a desired high or low matching score[2].
7) Attack on the database (i.e., modification) of biometric[6]
8) The transmission channel between the template database and matcher module is attacked (i.e., data in transit are Modified ).[4]
9) Alternation of decision (rejects or accepts).[3]

## *V. CONCLUSION*

Sensor based gait recognition is recent topic in area of biometric gait recognition. In Gait recognition approach, gait patterns are derived using sensors attached with human body. Primary advantage of accelerometric based gait recognition over other biometric authentication is the ability to enable unobtrusive user authentication. In this paper we have presented approaches for biometric gait recognition. It is important to done this approach by proper algorithm. Hence, algorithms for applying Gait recognition are also provided in this paper with required formula for feature calculations. In this paper we have listed attacks on gait based biometric system. All these topics will constitute the basis for our future work.

## VI. REFERENCES

[1] K. Jain, A. Ross, and S. Prabhakar. "An introduction to biometric recognition." IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, 14:4–20, January 2004.
[2] Davrondzhon Gafurov, "Gait Authentication and Identification Using Wearable Accelerometer Sensor", CONFERENCE PAPER · JULY 2007.
[3] Dimosthenis Ioannidis, "Gait Recognition Using Compact Feature Extraction Transforms and Depth Information" IEEE Transactions on Information Forensics and Security
[4] Patrick Bours, Kjetil Holien "Improved Cycle Detection for Accelerometer Based Gait Authentication"
[5] Davrondzhon Gafurov, Kirsi Helkala, and Torkjel Søndrol, " Biometric Gait Authentication
[6] Using Accelerometer Sensor", Norwegian Information Security Lab
[7] Davrondzhon Gafurov, Patrick Bours, "Paper1 Spoof Attacks on Gait Authentication System, " in Norwegian Directorate of Health
[8] Ngo Thanh Trung, Yasushi Makihara, Hajime Nagahara, Ryusuke Sagawa, Yasuhiro Mukaigawa, "Phase Registration in a Gallery Improving Gait Authentication" IEEE Communication Magazine