ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 4, April 2017

GAIT Analysis Using Weka: Guard Mobile Device

Komal Mehta[1], Saurabh Dhiman[2]
Student, Dept. of C.S.E, Jaypee institute of information technology, Noida, India[1]
Student, Dept. of C.S.E, Jaypee institute of information technology, Noida, India[2]

Abstract: In today's era, the mobile device is considered as paramount for one and all. Reliability is the main concerns else it can be way off the beam. To secure the content in our device we proposed a continuous and implicit authentication method in this paper by collaborating some devices (such as sensors- accelerometer) with K-means clustering technique using Weka 3.6.9. We trained our device by considering different parameters as well as different age groups. After evaluating we achieve promising results on most of the cases. If the individual is intruder then phone doesn't permit to access our device and gets locked.

Keywords: WEKA; Mobile device; Accelerometer; Gait analysis techniques, Security, Pattern Recognition

I. INTRODUCTION

Smart phone have evolved rapidly from pure voice communication devices to a general purpose mobile computers. Security of mobile devices is becoming more crucial over time as these devices accumulate a lot of sensitive data about their users, such as emails, pictures, communication data, etc. Typically password stills the most common authentication mechanism. There are many more methods which are available for security purpose such as Finger print recognition, pattern on screen or face recognition [1].

We purpose an authentication method for smart-phones taking advantage of Gait analysis. Gait is a person's manner of walking for a long time, detecting changing in walking can help to identify disease in early stages. Another advantage of gait analysis is that it work in the biometric manner similar to those of finger print and face recognition with added advantage it is not likely to be forgotten or stolen like a password. Gait analysis could be used in different types as for verification or identification. In verification, it will identify the user by comparing the captured data with the new data .In identification it will identify user among a group of users [2]. Here we will focus on the identification of the user.

All the readings will be fetching by the accelerometer which read X, Y, Z coordinates of the user such that the user body will be aligned with the accelerometer axes. Reading for each and every user will be different in case of accelerometer. For identification, we will use the Weka tool which will work on the back-end , Weka is used for the classification of large data set by implementing different types of algorithm here we will focus on Simple K-Means Algorithm which will differentiate the trusted user with un-trusted user by making different centroid of the data set.

The objective of our research in this area is to enhance the ability of android as much as IOS.

The rest of this paper is organized as follows: Section 2 discuss techniques we were used. Section 3 comprises the ways of collecting data. Section 4 presents framework of our work. Section 5 shows the implementation part. Section 6 concludes this paper.

II. RELATED WORK

To do Gait Analysis using mobile device, we used some techniques i.e. Sensor based Gait-Recognition, Physics Toolbox Accelerometer, Weka 3.6.9 & K-means clustering. We elaborate all these as follow:

A. Sensor based Gait-Recognition

Biometric systems operate by receiving biometric data from user, bring out feature set from the acquired data, and comparing this feature set against the enlisted set in a database. An enrolment sample of individual is trained previously and stored in the backend. To verify the identity of user the comparison between trained and testing samples has done [3].

We did our work on Sensor-based gait recognition and utilized acceleration of the movement of device for authentication. As our device moves, there X,Y,Z

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 4, April 2017

coordinates vary and these were stored in CSV file which must be different from person to person .

B. Physics Toolbox Accelerometer

An accelerometer is equipment that computes proper acceleration. This accelerometer sensor app measures and displays a graph of G-Force vs. Time (s) and Acceleration (m/s/s) vs. Time (s) in x, y, and/or z dimensions, as well as total magnitude [4].

The net magnitude of acceleration or G-Force data can be recorded and exported in an e-mail or through Google Drive as a .csv attachment using a comma or a semicolon as a delimiter.

Fig. 1.Accelerometer

C. Weka

Weka is a ratite bird found only on the islands of New Zealand. The tool named Weka is a Troupe of machine learning algorithms for data mining tasks. It is open source software issued under the GNU General Public License. There are two ways to apply the algorithm that is it can be applied directly to a dataset or called from their own Java code. It contains tools for some specific tasks such as data pre-processing, classification, clustering, association rules, visualization etc. It is well-pertinent tool for developing new machine learning schemes [5].

Here we use 3.6.9 version of weka as it is stable one.

D. K-Means clustering

K-Means is unsupervised learning algorithms which efficiently solve the well-known clustering problem. The procedure follows a simple and easy way to classify a given data set through a certain number of clusters. The basic idea is to define k centers, for each k cluster. These centers should be placed in appropriate way because different location of centers shows different result. So, place each center as far as possible. After that each data points are associated with nearest data centers. This step is completed after all points are associated. At that point we need to re-evaluate k new centroids [6].

After we have these k new centroids, clustering is done again that is creation of new binding among data points and data center. This whole process is done till the position of data centers remains same as that of previous one. The motive of this K-means clustering is to minimize the objective function.

$$J(V) = \sum_{i=1}^{c} \sum_{j=1}^{nC_i} \left(||x_i - v_j|| \right)^2 \qquad (1)$$

Where, *'$||x_i - v_j||$'* is the Euclidean distance between x_i and v_j.
'c_i' is the number of data points in i^{th} cluster.
'c' is the number of cluster centers.

III. Data Collection

Data used in this paper is collected using a standard mobile phone which contains the accelerometer. The mobile uses an android platform and the output of data are stored in CSV file. We extract some particular features of the persons using our device.

Each time we extract features by assuming the mobile device accelerometer must be active in the person hand. These are:

a) *Normal walk*: Record when the person moves normally.

b) *Fast walk*: Record when the person moves fastly.

c) *Running*: Record when they run.

d) *Jogging*: Record when they jogg.

e) *Stairs up-down normally*: Record when they go up-stairs normally.

d) *Stairs up-down fastly*: Record when they go rapidly on up-stairs.

IV. Architecture

In this section we provide description about our proposed work. Firstly, Mobile will take the reading of all the trusted user on multiple features (Such as Normal walk, Fast walk, jogging, Normal Stairs walk, Fast Stairs walk) via accelerometer which is pre available in the device that means training the data, later all the readings will be stored

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 4, April 2017

in the native database and accordingly take reading on the predefined time interval.

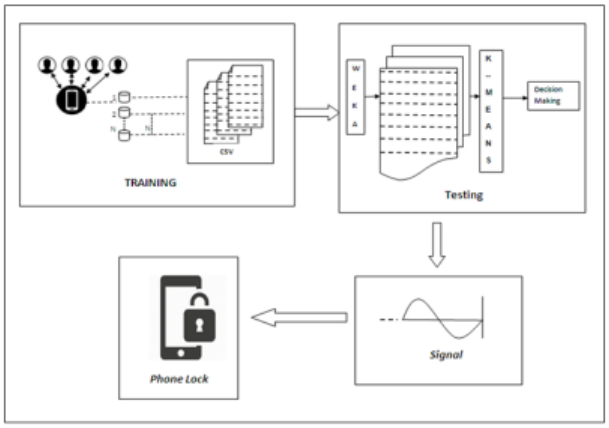

Fig. 2.Proposed framework

All the trusted user readings and the new readings will move to the testing phase through mail and the testing done on the data set by applying Simple K- Means on the Weka tool which will classify that the new generated reading matches with any of the trusted user reading or not and will generate some result on that and transfer that result to the mobile device if the decision is positive then mobile remain unlock [9] but if decision comes out to be negative than Mobile get locked. The whole step by step methodology is shown in figure 10.

V. IMPLEMENTATION

Here, we elaborate the way to conclude the person who is using our phone. Firstly, by using our accelerometer we measure the X, Y, Z coordinates of all the features we extract of the person and got the CSV file as an output. Then we combine the readings(X, Y, Z coordinate) of all the features. We got the 6 CSV files each of different features. Then those CSV files run on Weka and got the different clusters that are equal to the no. of training set. When new one picks that mobile device, we send their readings to our system via mail and match their cluster to the other ones via Weka. If the two clusters overlap to each other than that new one is the existing one in the training set and also identifies the person as each person got the different color. If no two cluster overlap, then we send the signal to our device and its get lock so no new person can access our device without our permission [11].

A. *Evaluation*

To evaluate the performance of our proposed model we have to train the set firstly and the testing is done.

1) *Training phase*

We consider all 6 parameters and forms clusters using Weka. To differentiate the coordinates of each person we assign different color to everyone as shown in figure 3-8. The coordinates are colour of each individual according to their way of movement and form a group called cluster. Here, we consider 11 different users and stores their data in our devices in all parameters form. , we assign 'Y' parameter of persons to X axis and 'Z' parameter to 'Y-axis.

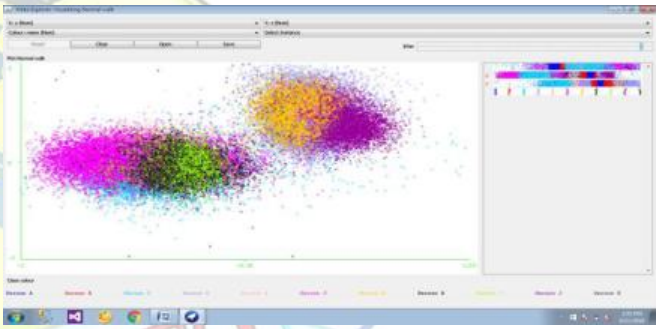

Fig.3.Normal walk clusters

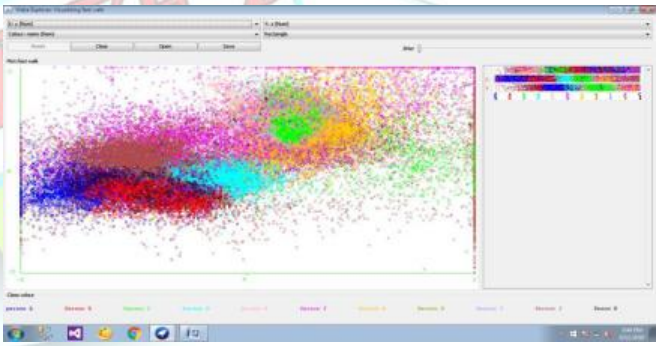

Fig.4.Fast walk clusters

Fig.5.Clusters for running

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 4, April 2017

2) Testing phase:

In this phase, we test that user who picked our device is authenticated or not. For this purpose we consider one person L moves and our acclerometer save his/her X,Y,Z coordinates. If he/her is the one whose reading is save in our testing set then their cluster must overlap to each other else not. So we observe both the cases.

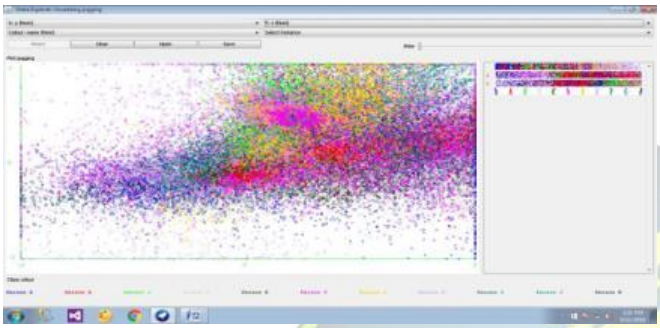

Fig. 6.Clusters of jogging

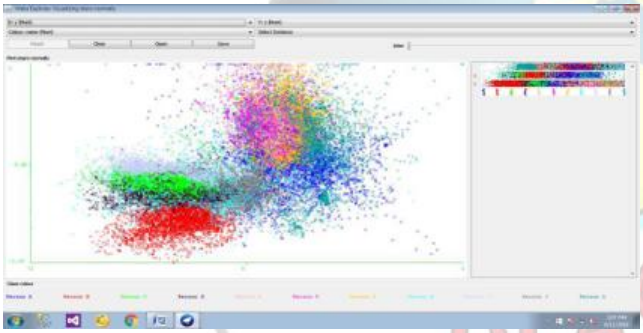

Fig. 7.Stairs-normal clusters

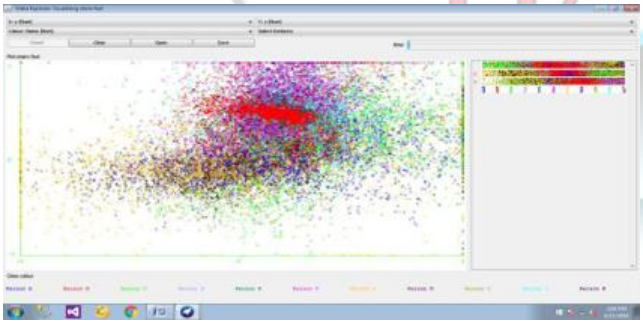

Fig. 8.Stairs-fast clusters

Case 1: When the device is on the existing ones user(trained user). If the user is same that is authorized then the YES signal is passed through Weka and the device remains unlocked. In figure 9, person L now overlap with person K i.e black and green color overlap with each other at so many coordinates so we conclude they both are same.

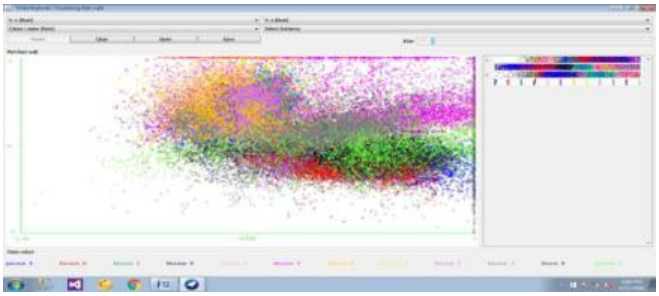

Fig. 9.Fast walks testing

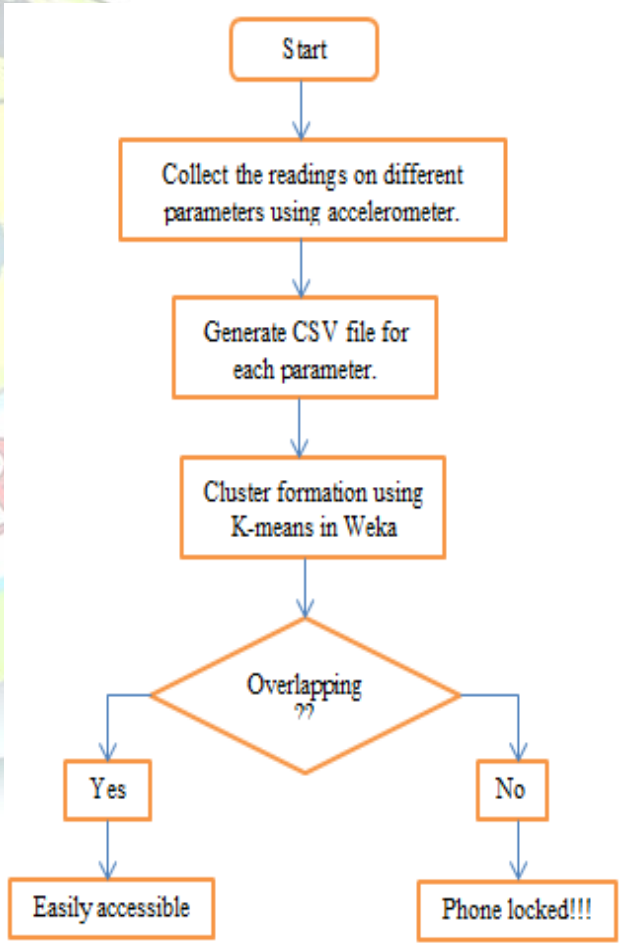

Fig. 10.Intended flow chart

In figure 11, person L now overlap with person K i.e brown and blue color overlap with each other at so many coordinates so we conclude they both are same.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 4, April 2017

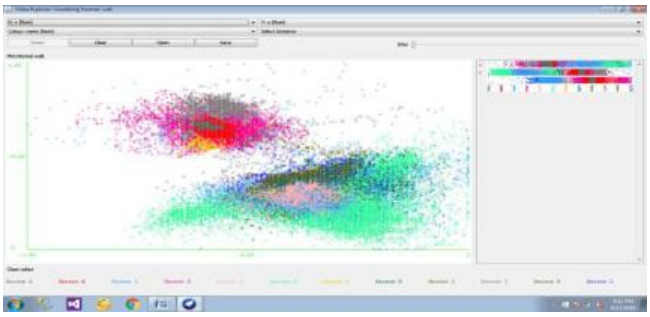

Fig. 11.Normal walks testing

In figure 12, person L now overlap with person D i.e sky blue and red color overlap with each other at so many coordinates so we conclude they both are same. So, we easily conclude the user identification.

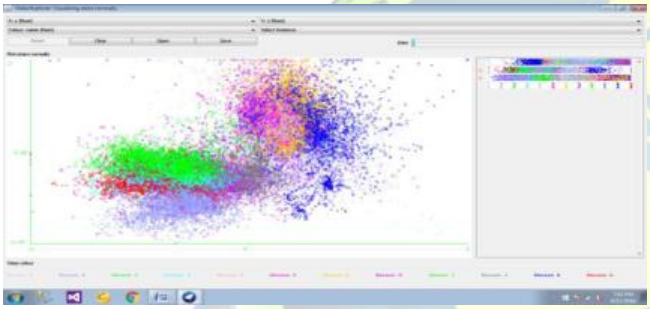

Fig. 12.Stairs-normally testing

Case 2: When the device is on the new user (non trained user). If the new user pick device their coordinates are not matched with trained data. Then by using Weka we send NO signal to device which results the lock on screen and our device become safe. In figure 13-15, there is no overlap between anyone. So the person m is non- authorized.

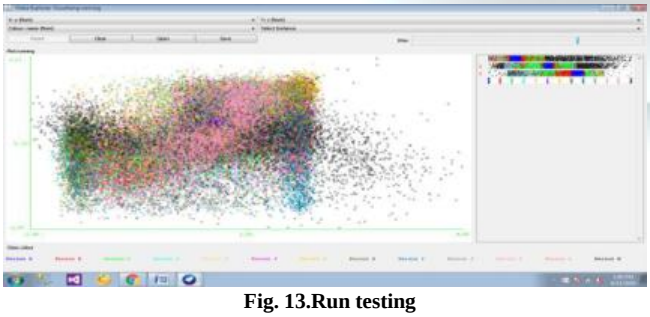

Fig. 13.Run testing

VI. CONCLUSION

This study presented a new method to prevent our personal device from others. The proposed method of guarding our device from intruder is beneficial because only the authenticated used can access the phone and if non-authorized individual try to access the content then our device gets locked as their pattern is not stored in database (trained set). We applied our method on more

Fig 14.Fast-Stairs testing

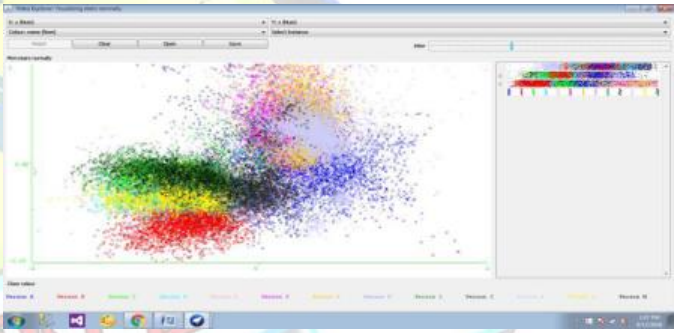

Fig.15. Normal-stairs testing

than 20 individuals and also on different age groups. This is not the end of work. We further try to apply this technique on big data as well as using cloud storage for decision making.

REFERENCES

[1]. Shoaib, Muhammad, et al. "A survey of online activity recognition using mobile phones." Sensors 15.1:2015.

[2]. Whittle, Michael W. Gait analysis: an introduction. Butterworth-Heinemann, 2014.

[3]. Gafurov, Davrondzhon, Kirsi Helkala, and Torkjel Søndrol. "Biometric Gait Authentication Using Accelerometer Sensor." JCP 1.7:2006.

[4]. Gafurov, Davrondzhon, Einar Snekkenes, and Patrick Bours. "Gait authentication and identification using wearable accelerometer sensor." Automatic Identification Advanced Technologies, 2007 IEEE Workshop on. IEEE, 2007.

[5]. Singhal, Swasti, and Monika Jena. "A study on WEKA tool for data preprocessing, classification and clustering." International Journal of Innovative technology and exploring engineering (IJItee) 2.6: 2013.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 4, April 2017

[6]. Cai, Xiao, Feiping Nie, and Heng Huang. "Multi-View K-Means Clustering on Big Data." IJCAI: 2013.

[7]. Tudor-Locke, Catrine, et al. "How many steps/day are enough? For older adults and special populations." International Journal of Behavioral Nutrition and Physical Activity 8.1: 80:2011.

[8]. Shull, Pete B., et al. "Quantified self and human movement: a review on the clinical impact of wearable sensing and feedback for gait analysis and intervention." Gait & posture 40.1: 11-19:2014.

[9]. Wang, Xinlei Oscar, et al. "Enabling reputation and trust in privacy-preserving mobile sensing." IEEE Transactions on Mobile Computing 13.12: 2777-2790: 2014.

[10]. Skotte, Jørgen, et al. "Detection of physical activity types using triaxial accelerometers." Journal of Physical Activity and Health 11.1: 76-84:2014.

[11]. Young, Tzay Y., and P. S. Liu. "Handbook of pattern recognition and image processing." Academic Press. 1986.

[12]. Cappozzo, Aurelio. "Gait analysis methodology." Human Movement Science 3.1: 27-50:1984.

BIOGRAPHY

Komal Mehta is M.Tech student in specialization of mobile technology from Jaypee Institute of Information Technology Noida. She received B.Tech from Maharshi Dayanand University (MDU), Rohtak Haryana in 2014. Her research areas are Networking, Wireless sensors etc.

Saurabh Dhiman is M.Tech student in specialization of mobile technology from Jaypee Institute of Information Technology Noida. He received B.Tech from Graphic Era University, Dehra Dun. His research areas are Andrioid, Web Development, and Computer Networking etc.