Mobile Devices and Social Networking Security Solution

Aman Jain and Shilpa Mehta

Abstract: Nowadays almost everyone is using smart phones. They are becoming an essential tool in human being's everyday life. They are not only used for mere communication such as calling or sending text messages; however, they are also used in applications such as for accessing internet, receiving and sending emails and storing documents. As a result of this, not only phone numbers and addresses are stored in the mobile device but also financial information and business details which definitely should be kept private. And if the device is being stolen, each and every information is in the hands of the new owner. That's why; the biggest challenge is the security. When it is necessary to confirm the user identity on systems to perform a given operation, the term User Authentication is used. Traditionally, people prove their identity by providing passwords. The average person today has about 25 password protected accounts (according to Microsoft study), more passwords than they can reasonably be expected to remember. People compensate by using the same password for multiple accounts, and by choosing passwords that are easy to remember. But, unfortunately easy to remember means easy to guess. Other user select difficult passwords but then write them down where unauthorized eyes can find them. That's why, identity based on what you know (login and password) and what you have (ID cards) can be easily stolen. As we want trust (security), the notion what you are is a new opportunity to user authentication. Biometric Authentication is answer for that. Biometric is a characteristic of human being that distinguishes one person from another. For example, finger prints, retina, face recognition, etc. This can be used for identification or verification of identity.

Keywords: FAR, FRR, ROC, EER, FTE, FTC.

1. INTRODUCTION

Biometrics is a science of identifying a person based on unique physiological or behavioural characteristics. It is "who you are" type of authentication. Talking simply, biometric authentication works by comparing two sets of human features to figure out if they come from the same person. Our bodies have many features that are unique enough for such verification. Because biometrics can't be guessed, lost, shared, or stolen, it is the only way to reliably verify whether the person claiming to be you is really you.

Aman Jain and Shilpa Mehta are with Electronics and Communication Engineering, Dronacharya College of Engineering, Gurgaon-123506, India
Email: amanproudtobejain@gmail.com, shilpa.frnd1155@gmail.com

2. BIOMETRICAUTHENTICATION IN SOCIAL NETWORKS

A. The Advent of Social Networks

A social network service is a website designed to build communities based on common interest and activities. Typically users can create profiles with selected personal information and interests, search or view parts or all of the profiles of the other users, connect with old friends and make new ones. Social networking websites, such as Facebook, LinkedIn and Twitter have become a popular channel for communication.

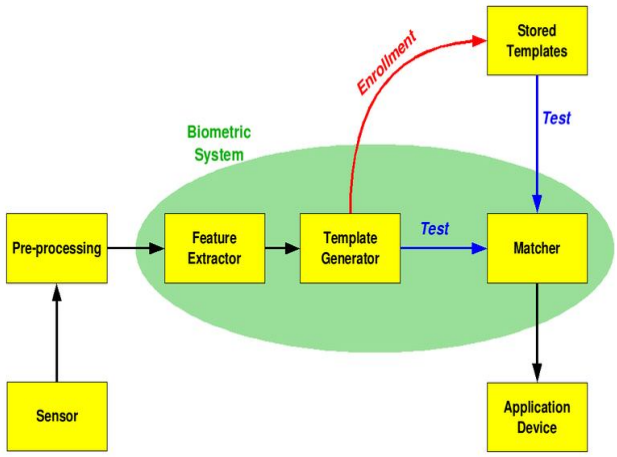


Fig. 1

B. Social Networking Today

Most major social networking sites today operate on the honour system. While many sites' policies require members to use their real name and age and to open only one account, there is no verification. Users can easily lie about their identity, with no traceability in case of a serious complaint. Many users give out too much personal information. Add to that tendency to use weak passwords, which can sometimes even be drawn from information in their profile, give away their login information and you have a huge receipt for abuse.

C. Biometrics for Social networks

The technology for such a system already exists, with a combination of human traits well suited to a social networking application. Biometric Identification of face,

voice, iris, individually or in any combination, using standard computer webcam and microphone, such as the biometric technology developed by BioID , has been available for some time.

3. BIOMETRICAUTHENTICATION IN MOBILES

A. Security Aspects

There are two types of authentication: authentication at log on time and authentication at run time. The latter one is important because it can prevent unauthorized persons from taking device in operation and accessing confidential user information from the Personal Network. The false- accept rate (FAR) and the false reject rate (FRR) are used to quantify the biometric authentication performance.

B. Convenience Aspects

If the system force you to re- enter your biometric data, would you like? Never. Surely, you will get annoyed. The FRR is closely related to user convenience. A false reject will force user to re-enter the biometric data, which will cause annoyance. This obviously leads to the requirement of low FRR of biometric authentication system.

The biometric authentication should be transparent. Transparency should be considered as a requirement for the authentication at run time, because regularly requiring a user, who may be concentrating on a task, to present biometric data is neither convenient nor practical.

4. PERFORMANCE

The following are used as performance metrics for biometric systems

A. False Accept Rate or False Match Rate (FAR or FMR)

The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, then he is treated as genuine that increase the FAR and hence performance also depends upon the selection of threshold value.

B. False Reject Rate or False Non-Match Rate (FRR or FNMR)

The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

C. Receiver Operating Characteristic or Relative Operating Characteristic (ROC)

The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matched but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

D. Equal Error Rate or Crossover Error Rate (EER or CER)

The rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate

E. Failure To Enrol Rate (FTE or FER)

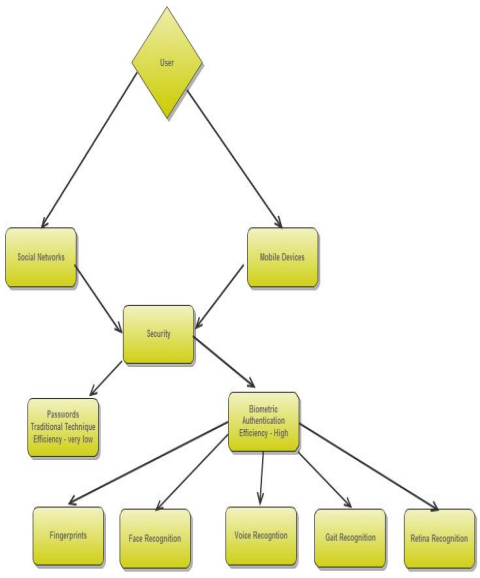
The rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

F. Failure To Capture Rate (FTC)

Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

G. Template Capacity

The maximum number of sets of data which can be stored in the system.



5. FACE RECOGNITION AS BIOMETRIC AUTHENTICATION

Face recognition, among all biometrics, is a good choice. It is only biometrics that can be really transparent, especially for authentication at run time. Just by mounting a camera on the system, the face images of the user can be caught almost constantly. This is attractive also because the cost for the camera is low, and mobile phones and PDAs generally have a camera installed.

A. Face Pre-processing

It includes three steps, i.e. face detection, face registration, and face normalization.

For fast face detection Viola and Jones proposed a detection scheme which is very efficient by using simple rectangular binary features and the integral image, and has proved to be robust against varying background and foreground.

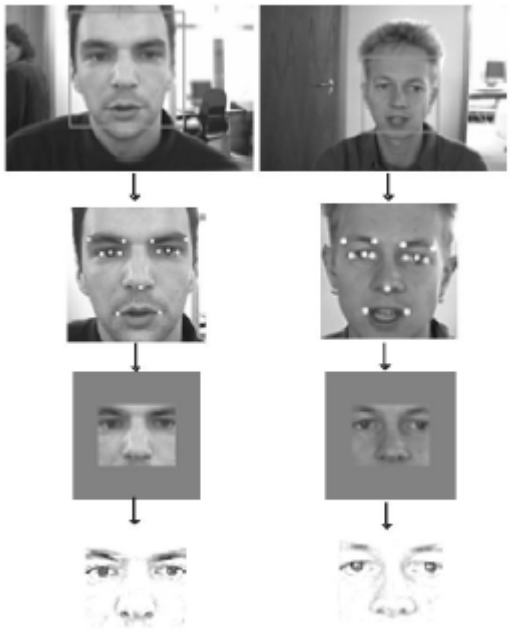


Fig. 2 Face feature extraction procedure (From top to down) face detection, facial feature detection, face registration and masking, high pass filtering

6. GAIT RECOGNITION AS BIOMETRIC AUTHENTICATION

The term *gait recognition* describes a biometric method which allows an automatic verification of the identity of a person by the way he walks. There are three main techniques in biometric gait recognition: Machine Vision Based, Floor Sensor Based and Wearable Sensor Based Gait Recognition.

A. Machine Vision Based Gait Recognition

In the machine vision based gate recognition, the system will typically consist of several digital or analog cameras with suitable optics for acquiring the gait data. Techniques such as background segmentation are used to extract features to identify a person. This technique is especially useful for surveillance scenarios.

B. Floor Sensor Based Gait Recognition

In the floor sensor based gate recognition, the sensors are placed on the floor which makes these methods suitable for controlling access to buildings. When people walk across the mat, they can be authenticated e.g. by the force to the ground which is measured by the mat.

C. Wearable Sensor Based Gait Recognition

The newest of three techniques is based on wearing the motion recording sensors on the body. It can be in different places: on the waist, in pockets, shoes etc.

We will mainly study this type of gait recognition.

The wearable sensors can be accelerometers (measuring acceleration), gyro sensors (measuring rotation and number of degrees per second of rotation), force sensors (measuring the force when walking) etc. Following Table gives overview of current wearable sensor based gait recognition studies from years 2004 to 2008.

Study	Sensor Location	EER	Number of Test Persons
Holien	Left leg (hip)	5.9%, 25.8%	60
Gafurov et al.	Ankle	8%	40
Gafurov et al.	Trousers pocket	7.3%	55
Gafurov et al.	Hip	15%	100
Huang et al.	Shoe	12%	40
Ailisto el al.	Waist	7%	15
	Waist	8%	10
			35

Table I

Performance of Current Wearable Sensor- Based Gait Recognition Systems

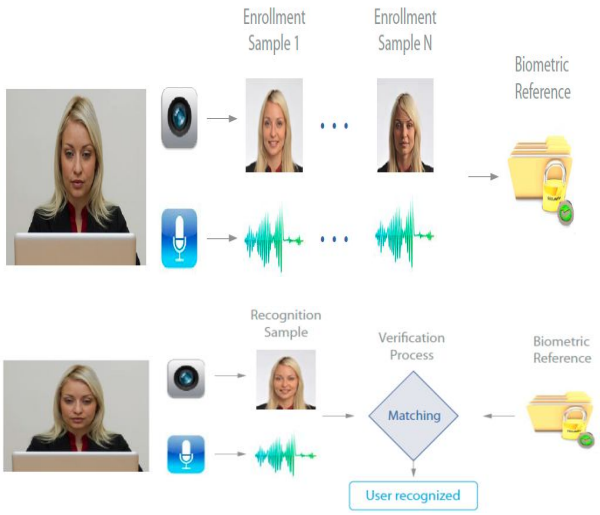
All studies except Morris and Huang et al. were using only accelerometers for collecting the gait data and reported recognition rates based on the verification criteria. Morris and Huang et al. used other types of sensors including force sensors, bend sensors, gyro sensors etc. in addition to the accelerometer sensor.

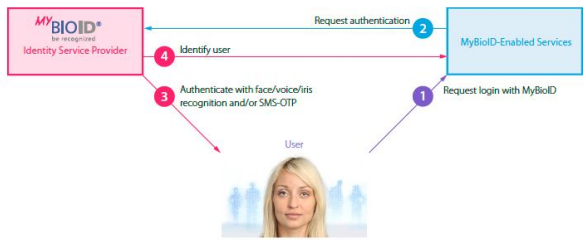
The accelerometer is focused for gait recognition for biometric authentication as it provides an unobtrusive authentication method for mobile devices which already contain accelerometers (like smart phones, PDAs etc.). That's why, it can be applied for continuous verification of the identity of the user without his intervention which is an advantage to other biometric authentication like fingerprint or face recognition.

The biometric gait recognition only works when user is walking. That's why this method has to be combined with another authentication method.

7. IMPLEMENTATION OF BIOMETRICAUTHENTICATION TODAY

A. Best example for Biometric Authentication in Social Networks is www.bioid.com





B. Various android applications are there for Biometric Authentication.

C. Unique Identification (UID) of Govt. of India uses Biometric Authentication.

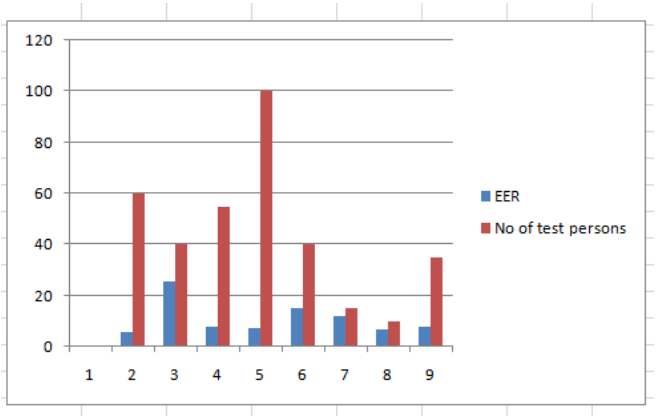
There used three biometric authentications i.e. face recognition, iris recognition and finger prints

D. It is also used in identification of culprits by matching fingerprints found in crime places with the police records or with that of suspects.

8. CONCLUSION

The security of the mobile devices is very important. My work aims at building up a secure and efficient connection between the system and the user, based on biometric authentication. A try has been made to create awareness for the biometric authentication. This paper mainly focuses for Face Recognition and Wearable Sensor Based Gait Recognition for Biometric Authentication.

9. RESULTS



10. FUTURE WORK

A. Improvement of Current Technologies

Both the face recognition and gait recognition have some advantages and disadvantages. Like, talking about the gait recognition, it main advantage is that it does not require user's intervention but its main disadvantage is that it only works when the user is walking so needs to be combined with other authentication method so not yet ready for practical use. Besides this, user does not walk always at constant speed and grounds can also be different.

So focus of future work is to create a gait recognition method which provides robust verification under different circumstances. These circumstances might be different walking conditions like walking speed or ground which will have an influence of the walk of a person and therefore might also influence the biometric recognition.

B. Implementation in Other applications

1. Facebook, LinkedIn and other social network sites should have option of logging by providing any biometric authentication. It will help the best to security concerned users.
2. Today smart phones require just pattern to be opened which is quite easy to guess. There must be employed face recognition where anyone try to operate the phone, his face is captured and automatically matched with the reference store. If both does not match, phone lock automatically.
3. Next step to Unique Identification (UID) Scheme Govt. of India can do, is that all the records must be provided to police, CID, CBI and every other investigating agency so that fingerprints found in crime places can be found easily. As sometimes, fingerprints found does not match with that in the police records, so this can be very useful.
4. High security building like Army Places etc. must be employed with Gait Recognition for Biometric Authentication.

REFRENCES

[1] D. Gafurov, "Performance and security analysis of gait – based user authentication," Ph. D. dissertation, Faculty of Mathematics and Natural Sciences, University of Oslo, 2008.
[2] M.S. Nixon, J.N. Carter, J.M. Nash, P.S. Huang, D. Cunado, and S.V. Stevenage, " Automatic gait recognition," in Biometrics – Personal Identification in Networked Society, Kluwer, 1999, pp. 231 – 250.
[3] J. Han and B. Bhanu, "Individual recognition using gait energy image", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 28, pp. 316 – 322, 2006.
[4] Z. Liu and S. Sarkar, " Improved gait recognition by gait dynamics normalization", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 6, pp. 863 – 876, 2006.
[5] S. Sarkar, P.J. Phillips, Z. Liu, I.R. Vega, P. Grother and K.W. Bowyer, "The humanid gait challenge problem: Data sets, performance, and analysis", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 27, pp. 162 – 177, 2005.
[6] J. Jenkins and C.S. Ellis, "Using ground reaction forces from gait analysis: Body mass as a weak biometric" in Fifth International Conference on Pervasive Computing, 2007, pp. 251 – 267.
[7] K. Nakajima, Y. Mizukami, K. Tanaka, and T. Tamura, "Footprint – based personal recognition," IEEE Transactions on Biomedical Engineering, vol. 47(11), 2000.