BioSmart: An advanced user authentication mechanism on touch screen devices

Shemin Shajan

MTech, Computer Science and Engineering, Lourdes Matha College of Science and Technology, Kerala, India

---***---

Abstract - *The use of touch screen devices, especially smart mobile devices for storing sensitive information and accessing online services is increasing nowadays. At the same time, methods for authenticating users into their devices and online services should not only be secure, but also should provide increased privacy and user-friendliness. Biometrics is an efficient and accurate way to provide user authentication. But unimodal biometrics suffers from many different types of security problems. In this paper, multi modal biometric is used to secure smart mobile devices.A combination of physiological and behavioral biometrics is used to implement the proposed system. Lock pattern dynamics which is a secure and user friendly two factor authentication method is used as the first technique in authentication. This technique incorporates biometric feature by measuring the speed at which the lock pattern is drawn, which is unique to an individual. In order to reduce the false rejection rate, an additional face recognition technology is also incorporated. Here, face is captured using the inbuilt camera of the device, thus avoiding the use of expensive biometric capturing devices, which is the major disadvantage of most of the biometric systems. It is shown that the combination of lock pattern dynamics and face recognition improves the security of devices than traditional unimodal biometric systems and at the same time, provides better usability. The proposed system achieves an equal error rate of approximately 2.93, meaning that multimodal biometrics technique can be used to authenticate users into their devices in a highly efficient and secure manner.*

Key Words: Biometrics, Pattern dynamics, User experience, Authentication, Equal error rate, Lock pattern, Touchstrokes, etc...

1. INTRODUCTION

As touch screen devices are becoming increasingly powerful and popular, security of the data stored in touch screen devices, especially mobile devices, like email addresses, sensitive documents, etc., becomes very important. Most of the current devices have password /pin number/pattern lock protection to address security. For sensitive services such as mobile payment, a strong user authentication is required. Indeed, only biometrics has a relationship between the user and its authenticator. Biometrics refers to metrics related to human characteristics. Biometric authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological and behavioral characteristics.

Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

Many real life applications uses biometric systems such as airport security, building access, schools etc.Most of such system are implemented as unimodal biometrics. Unimodal biometric systems refer to the systems that uses a single biometric feature.Most of the unimodal biometrics system suffers from different kinds of problems. For example, the main disadvantage of physiological biometrics is that authentication can be done by force and also the use of expensive hardware .The main problems with behavioral biometrics is that human behavior may change depending upon the situation.So, under stress or extreme psychological conditions, the behavior of a person may differ from his normal behavior.

Inorder to overcome these problems, a possible solution is the use of multimodal biometrics.That means, the combination of two or more biometric features in a single biometric system.

In the proposed method, I am using a combination of physiological and behavioral biometrics to provide user authentication on touch screen devices. Face recognition and touch stroke dynamics are used for implementing physiological and behavioral biometrics respectively. Here, the term touch strokes means keystrokes on touchscreen devices.

2. RELATED WORK

Biometric based mobile authentication is an emerging issue, with relatively few references. Some recent papers

[1], [2], and [3] deal with keystroke dynamics based recognition. The first paper deals with user identification on mobile devices, using keystrokes dynamics based authentication, relying on 11-digit telephone numbers and text messages as well as 4-digit PINs classify users. The second develops a more efficient system, with optimized enrollment and verification steps, whose principle is extended in the latter paper for touch screen, handled mobile devices, along with a pressure feature measurement. Many works have been done to propose biometric systems for user authentication on mobile devices.

Face recognition and eye recognition are dealt with in [4], where as in [5], real time training algorithm is developed for mobile devices. The authors propose to extract local face features using some local random bases and then to incrementally train a neural network. Image processing also concerns hand biometrics on mobile as in the reference [6], where hand images are acquired by a mobile device without any constraint in orientation, distance to camera or illumination. The author of [7] details an iris recognition system, based on a three-step pre-processing method relying on (a) automatic segmentation for pupil region, (b) helper data extraction and pupil detection and (c) eyelids detection and feature matching. Apart from the literature dedicated to biometric solutions for mobile authentication related to a specific modality, some appears propose an overview on the underlying topic. We can mention the recent paper [8]. The authors focus on biometrics on mobile phone through some standard modalities (fingerprint, speaker recognition, iris recognition, and gait) and propose a new application to ECG measurement and remote telecardiology, with an extra portable heart monitoring device.

One of the first automated faces recognition systems was described in [9], marker points (position of eyes, ears, nose, etc) were used to build a feature vector (eg: distance between the points, angle between them). The recognition was performed by calculating the euclidean distance between feature vectors of a probe and reference image. Such a method is robust against changes in illumination by its nature, but has a huge drawback: the accurate registration of the marker points is complicated, even with state of the art algorithms. Some of the latest work on geometric face recognition was carried out in [10]. A 22-dimensional feature vector was used and experiments on large datasets have shown, that geometrical features alone my not carry enough information for face recognition. Most of solutions are classical modalities implemented on a mobile device. The user experience is in general not good and not very well fitted for a mobile device. An approach that tracked the user's "unique touch features, such as finger pressure and trajectory, the speed and acceleration of movement" as the person interacted with the touch screen device is proposed in [11]. Recent papers [12] and [13] deals with incorporating biometric feature into the traditional unlock screen pattern in android touch screen devices.

In the next section, I propose a biometric system for mobile device providing a better security while permitting a very good usability.

3. PROBLEM ANALYSIS

Currently, most of the solutions for authenticating users into their devices and other mobile services are based on the same solutions offered when using desktop computers, which usually involve the use of a PIN, a strong password, or some sort of extra external security token device.

These techniques become cumbersome when applied to mobile devices and do not always provide a satisfactory user experience. Besides, they are not a sustainable approach for the future of mobile interactions, in which people would carry only one secure trustable device to perform most operations and would preferably use only one hand to operate such device.

3.1Lock pattern process overview

Lock patterns are one type of recall-based graphical password. They have been criticized because of their vulnerabilities to *smudge attacks* (i.e., recognizing the Fingers' grease on the screen), *shoulder-surfing attacks* (i.e., observing or recording with a video camera the moment of authentication), and others.

Adding biometric analysis to lock patterns can enhance the security of this type of graphical passwords by becoming a two-factor authentication mechanism.

Lock pattern biometrics have the potential to be employed as an authentication method and that individuals can be identified by the way they draw a lock pattern on a touch-screen.

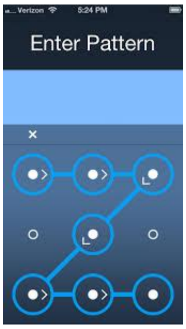


Fig-1: Typical android unlock screen pattern

3.2. Two and three factor authentication method.

Supposing that the pattern is only known to the legitimate user, the chances for an imposter to successfully authenticate into the system are further reduced. For example, given that there are 16,032 combinations of six-dotted patterns in the current implementation of the Android lock patterns, let the probability of an imposter entering the correct lock pattern on the first attempt to be Pr(*Pattern Guessing*) = 1/16,032 = 0.00006. Similarly, let the probability of the lock pattern biometric system to authenticate an imposter that knows the legitimate lock pattern, which is given by the value of the False Acceptance Rate (FAR), be Pr(*FAR*) = 0:05. Thus, the probability of these two mutually independent events happening is given by

$$\Pr(\textit{Pattern Guessing} \cap \textit{FAR}) = (0.00006)/(0.05) = 0.000003.$$

In other words, this solution provides a two-factor authentication in which the probability that an attacker with an unknown pattern would be let into a system enhanced with biometrics is about 0.0003%, thus providing a much more secure solution than one-factor 4-digit and 5-digit PIN codes (0.01% and 0.001%). This probability can be further adjusted depending on the level of security required by a system.

3.3 Impact of training trials on performance.

As with all biometric systems a number of training trials have to be input in order to accurately detect the identity of an individual, since biometric behavior cannot be captured with a single trial.

3.2 Face recognition technique overview

As mobile phones are becoming increasingly powerful, security of the data stored in mobile phones like email addresses, sensitive documents, etc., becomes very important. Most of the current phones have password protection to address security. However, a face recognition scheme is much more secure and flexible as it provides distinctive print to gain access and also the user need not remember passwords.

Face recognition is an application used for identifying a person from a digital image or a video frame. “Face Recognition" is a very active area in the Computer Vision and Biometrics fields, as it has been studied vigorously for 25 years and is finally producing applications in security, robotics, human-computer-interfaces, digital cameras, games and entertainment.

"Face Recognition" generally involves two stages:

1. *Detection*, where a photo is searched to find any face (shown here as a green rectangle), then image processing cleans up the facial image for easier recognition.
2. Face Recognition, where that detected and processed face is compared to a database of known faces, to decide who that person is (shown here as red text).

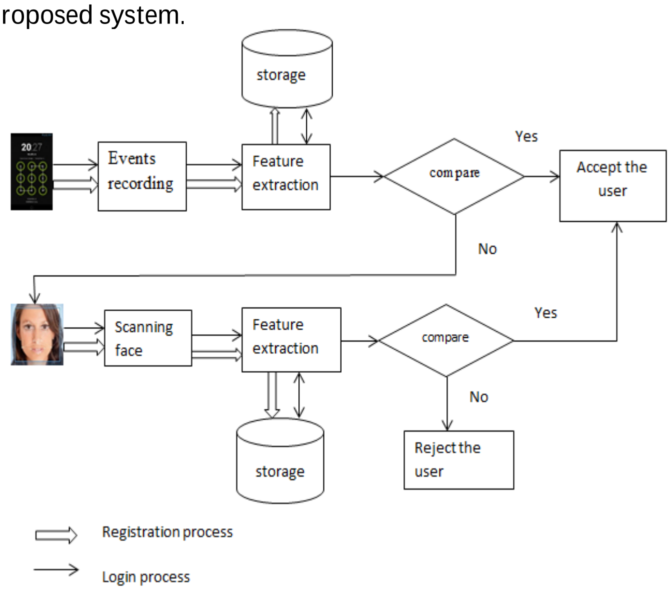
It is usually harder to detect a person's face when they are viewed from the side or at an angle, and sometimes this requires 3D Head Pose Estimation. It can also be very difficult to detect a person's face if the photo is not very bright, or if part of the face is brighter than another or has shadows or is blurry or wearing glasses, etc.

4. Proposed System

Proposed system incorporates keystroke dynamics, which is a behavior biometric along with traditional screen unlock pattern to avoid disadvantages of normal pattern recognition systems which includes smudge attacks and eavesdropping. The main advantage of using behavioral biometrics is increased security.

Even if another person sees the pattern either via smudge or eavesdropping, the speed in which original user draws the pattern cannot be reproduce easily.

An issue that can happen with traditional unlock screen pattern is that under pressure, the original user itself may be unable to reproduce the original drawing speed. To overcome this problem, face recognition is added along with traditional pattern lock. If drawing speed fails, user is prompted to scan their face.As face recognition is unique for a user, this system overcomes the disadvantage of traditional behavioral biometric system.Figure 2 shows the architecture of the proposed system.



One of the problems with biometrics is the expensive capturing devices.But in the proposed system, no such device is needed since an inbuilt camera is used for capturing faces

The biometric system intends to increase security for a quick logical access control to the mobile device. It is composed of a two factor approach. It is intended to first recognize the user by the knowledge of a password represented by a secret path. I used the classical Android unlock screen approach. This approach to enter a password is quicker and is more usable for a mobile device. Second, the behavior of the user while giving the secret path is analyzed. This information is combined to make the decision concerning the identity verification of the user.

4.1 Extracted features

1. Start time:
It is the time in which pattern drawing starts. This is the current system time in milliseconds when the user's finger touches the first cell of the pattern
2. End Time:
It is the time in which pattern drawing finishes. This is the current system time in milliseconds when the user's finger is removed from the last cell.
Calculate the total time:
Total time=End Time-Start Time;
which is the total time that the user needs to enter the secret path.

4.2Enrollment

User is asked to draw the secret path 2 times. The above mentioned times are recorded. Then the user is prompted to go to face capturing UI.The user can store 2 to 10 faces. The faces are stored in a temporary storage area.

4.3 Login

During login, the user has to first draw the pattern. If the user draws the correct pattern and the drawing speed matches with that of registration, the user can immediately access the device. But if the drawing speed didn't match with the drawing speed during registration, the user is prompted to go to face capturing UI.The user gets access to the device only if the captured face matches with any of the stored faces.If the user draws an incorrect pattern, the system will immediately rejects the user without going for face recognition.

4.4 Setting Threshold Value

A Threshold value for drawing speed is set for the proposed system. The use of threshold value is that even for a single user itself, the speed in which he first draws the pattern during registration may not be exactly the same with the pattern he subsequently draws.There may be some slight difference in the order of magnitude of milliseconds.We need to incorporate this threshold value because otherwise,it is an impossible condition that the user draws the same pattern again in the same speed.The user can access the system if the difference between two pattern drawing times is less than the threshold value.
For example, if the threshold is set as 200ms and the pattern drawing time during registration is 1000ms, then the user get access to the system if the pattern drawing time during login is between 800ms and 1200ms.

4.5. Face Recognition Algorithm

I used Eigen face algorithm for face recognition. Face recognition based on the geometric features of a face is probably the most intuitive approach to face recognition the eigenvectors are derived from the covariance matrix of the probability distribution over the high dimensional vector space of face images. The Eigen faces themselves form a basis set of all images used to construct the covariance matrix. This produces dimension reduction by allowing the smaller set of basis images to represent the original training images. Classification can be achieved by comparing how faces are represented by the basis set.

Algorithm

Let $X=\{x_1,x_2,x_3.......x_n\}$ be a random vector with observations; X_i is an element of R^d

1. Compute the mean μ

$$\mu = \frac{1}{n} \sum_{i=1}^{n} x_i$$

2. Compute the Covariance matrix S

$$S = \sum_{i=1}^{n} (x_i-\mu)(x_i-\mu)^T{}_i$$

3. Compute the eigenvalues λ_i and eigenvectors v_i of S.

$$Sv_i=\lambda_i v_i$$

4. Order the eigenvectors descending by their eigenvalue. The K principal components are the eigenvectors corresponding to the K largest eigenvalues.

The K principal components of the observed vector $x$are then given by:

$$y = W^T(x-\mu)$$

Where $W = (v_1, v_2, v_3, . . . ,v_k)$

The reconstruction from the PCA basis is given by:

$$X=Wy + \mu$$

Where $W = (v_1, v_2, . . v_k)$

The Eigen faces method then performs face recognition by:

- Projecting all training samples into the PCA subspace.
- Projecting the query image into the PCA subspace.
- Finding the nearest neighbor between the projected training images and the projected query image

5. PERFORMANCE ANALYSIS

Data collected from 12 different participants were used for analysis.

Performance analysis was done on 3 different stages.
1. Pattern touch strokes dynamics only
2. Face recognition only
3. Combination of pattern touchstrokes and face recognition.

5.1 Pattern touchstroke only

A.BASED ON NO.OF TRIALS
The following table shows the result of 12 participants subjected to different training trials

Table 1- Relationship between success rate and no.of training trials

Participants	2 trials	5 trials	10 trials
A	A	A	A
B	R	A	A
C	R	R	R
D	A	A	A
E	R	A	A
F	R	R	R
G	A	A	A
H	R	R	A
I	R	R	A
J	A	R	A
K	R	A	A
L	A	A	A
Success %	41.66 %	58.7 %	83.33 %

A-Accept
R-Reject

From the table, it can be seen that as the training trials increases, success rate also increases. The success rate was 41.66% for 2 trials.The rate was increased to 58.3% and 83.33% for 5 trials and 10 trials respectively.

B.BASED ON THRESHOLD

The following table shows the FAR and FRR obtained when different thresholds are used.

Table2-Relationship between drawing speed threshold and error rate

Threshold	FAR	FRR
200 ms	4.8%	40%
300 ms	6%	33.4%
400 ms	7.9%	21.6%
500 ms	10.39%	10.39%
600 ms	15.5%	7.9%
700 ms	20.3%	6.4%
800 ms	22.9%	4.3%

At 500 ms threshold, almost equal FAR and FRR were obtained.So,I selected 500 ms threshold for the proposed system.

5.2 Face recognition only

A number of face images can be stored from a minimum of 2 to maximum of 10. The FAR(false acceptance rate) of face recognition is low as about 0.2%.But typically,face recognition applications have a higher FRR of about 20 because of the following reasons.
1. The face can be obstructed by hair, glasses, hats, scarves, etc.
2. Changes in lighting or facial expressions can cause problems.
3. The relative angle of the target's face influences the recognition score profoundly.
A solution to this problem is to capture more number of faces in different environments during enrollment. It can be seen that as the no.of stored images increases,FRR decreases.

5.3 Using combination of pattern touchstrokes and face recognition

The above results show that secure authentication can be done using biometric technologies -touchstroke dynamics and face recognition. But still, both of them possess some difficulties.
In the case of only pattern dynamics, it is found that best performance is shown at 10 training trials (higher success rate) and 500 ms (the system gives an equal error rate of 10.39%).
Also, in the case of face recognition only analysis,it is found that FRR can be decreased by increasing the no.of stored images(in this case,10 images).
So, In the analysis of the combined pattern touchstrokes and face recognition system, combination of these 3 features is used.
1. 10 training trials

2. 500 ms threshold.
3. Storing 10 faces.

An equal error rate of 2.93 was obtained during analysis. Figure 3 shows the ROC curve of the proposed system.

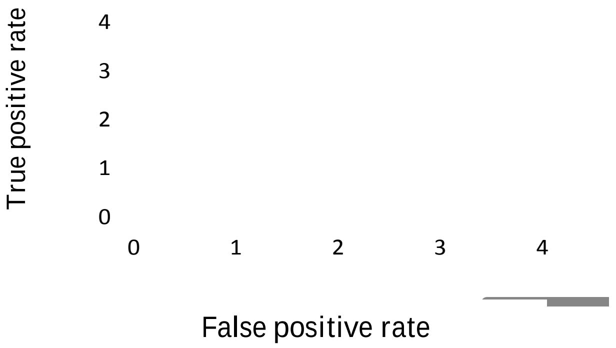


Fig-3: ROC curve of BioSmart

5. CONCLUSION

The results show that adding biometric information to lock patterns can enhance the security of pattern recognition system by providing two-factor authentication towards the smart device.Inaddition,relatively low error rate can be obtained by incorporating a physiologic biometric technique such as face recognition.An EER of 2.93 was obtained which is lower than the individual unimodal biometric systems.Hence,combination of different biometric systems offer better performance than unimodal biometric system. Thus the proposed system offers a biometric system for touch screen devices that provides a better security while permitting a very good usability.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Asst.Professor Mrs.Chithira Rakshmi G who guided me throughout my thesis work, without whose knowledge and assistance,I would not have completed my thesis work.

REFERENCES

[1] N. Clarke and S. Furnell, *"Advanced user authentication for mobile devices,"* Computers & Security, vol. 26, pp. 109–119, 2007.

[2] S. Hwang, S. Cho, and S. Park, *"Keystroke dynamics -based authentication for mobile devices,"* Computer & Security, vol. 28, pp. 85–93,2009.

[3] T.-Y. Changa, C.-J. Tsaib, and J.-H. Lina, *"A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices,"* The Journal of Systems and Software, vol. 85, p. 11571165, 2012.

[4] A. Hadid, J. Y. Heikkila, O. Silven, and M. Pietikainen, *"Face and eye detection for person authentication in mobile phones,"* in 1st ACM/IEEE International Conference on Distributed Smart Cameras, 2007

[5] K. Choi, K.-A. Toh, and H. Byun, *"Realtime training on mobile devices for face recognition applications,"* Pattern Recognition, vol. 44, p.386400, 2011.

[6] A. de Santos-Sierra, C. Sanchez-Avila, J.Guerra-Casanova, and A. Mendaza-Ormaza, Hand Biometrics in Mobile Devices. InTech, 2011, ch. Advanced Biometric Technologies, available from: http://www.intechopen.com/books/advanced biometric technologies/hand-biometrics-in-mobile-devices1

[7] S. Wang and J. Liu, Biometrics on Mobile Phone. In-Tech, 2011, ch. Recent Application in Biometrics, pp. 3–22, available from: http://www.intechopen.com/books/recent-application-inbiometrics/biometrics-on-mobile-phone.

[8] J.-S. Kang, "Mobile iris recognition systems: An emerging biometrictechnology," in International Conference on Computational Science (ICCS), 2010.

[9] http://docs.opencv.org/modules/contrib/doc/facerec/facerec_tutorial.html#kanade73

[10] http://docs.opencv.org/modules/contrib/doc/facerec/facerec_tutorial.html#bru92.

[11] Tao Feng , Ziyi Liu , KyeongAn Kwon et.al *Continuous Mobile Authentication Using Touchscreen Gestures*

[12] Michael Beton, Vincent Marie, Christophe Rosenberger. Biometric Secret Path for Mobile User Authentication: A Preliminary Study. International Conference on Mobile Applications and Security Management (ICMASM), Jun 2013, Tunisia. pp.6, 2013.

[13] Julio Angulo and Erik Wastlund, *Exploring Touch screen Biometrics for User Identification on Smart Phones,* IFIP Advances in Information and Communication Technology Volume 375, 2012, pp 130-143.

[14] https://en.wikipedia.org/wiki/Biometrics.

BIOGRAPHIES

Shemin Shajan received Btech from Kerala university in 2013, currently pursuing Master's degree in Computer Science and Engineering from Kerala University.