**Smartphone Authentication using Soft Biometrics**

By Radhika Bailurkar (2019430003)

Faculty Incharge: Prof Nataasha Raul

INTRODUCTION

Today, smartphones are being used widely in professional as well as personal life. These devices contain almost every data required for our daily life. The increasing use of access to sensitive and privacy data has given rise to the need of secure authentication techniques. To prevent unauthorized use of their mobile phones, most users typically rely on a feature that allows them to “lock” their smartphones using PINs, swipe patterns or passwords. These popular authentication mechanisms are susceptible to guessing, spoofing and side channel attacks such as smudge. Additionally, a fundamental limitation of PINs, passwords, and fingerprint scans is that they are well suited for one-time authentication, and therefore are commonly used to authenticate users at login. This renders them ineffective when the smartphone is accessed by an adversary after login. Continuous or active authentication addresses these challenges by frequently and unobtrusively authenticating the user via behavioral biometric signals, such as touchscreen interactions, hand movements and gait, voice and phone location. Let us look at biometrics for authentication.

BASICS OF BIOMETRICS

Biometric is the scientific field of study related to human characteristics. Biometric characteristics are unique, personal characteristics that can be used to establish a person’s identity. Unlike pass cards, keys and passwords, for example, the physical characteristics that can be used for biometric solutions cannot be transferred, or cannot be transferred easily, from one person to another. They are also not susceptible to fraud like photos and signatures. It is impossible for them to be removed. Biometrics can be classified below as:

* Physical Biometrics

Physical Biometrics focuses upon examining the biological and the physiological features of the human being.  These unique features include the shape of the hand, finger, and face, and the structure of the eye.

**Hand geometry**

The actual shape and dimensions of your hand are sometimes used for access control and time-and-attendance operations in the workplace. However, they are not as unique as fingerprints, so aren’t viable in high-security applications.

### Finger vein patterns

Fingerprints, while totally unique, can be at risk of being copied. A similar but more advanced technique looks instead at the veins underneath the fingerprint, which are virtually impossible to copy.

### The eye

The unique and complex characteristics of the iris or the retina of your eye can also be used for biometric ID. Eye biometrics are commonly used for automated passport controls and national ID programmes, and are also now starting to appear in smartphones, such as the Samsung Galaxy S8.

### Face shape

Analyzing the shape of your face, as well as its specific features (e.g. distance between the eyes or the height of your ears), is used in CCTV security systems, but can also be used as a commercial identification and marketing tool. With the huge and enduring popularity of selfies, it’s something that we may see more of in low-security smartphone apps.

* Behavioral Biometrics

Behavioral Biometrics focuses upon examining the non-biological or the non-physiological features of the human being.  This realm of Biometrics studies the unique, psychological aspects of humans.  This is the way we type on the computer keyboard, the way we sign our name, even the way we walk.

### Signature dynamics

This takes it beyond just what your signature looks like, and instead looks at how you sign. It includes analysis of the direction and pressure of your pen stroke, and combines it with the overall shape of the signature to verify your ID.

### Voice

The unique patterns in your voice can be analyzed and compared to an example voiceprint to confirm your ID. This is already used to access some online banking services and automated customer service phonelines.

### Keystroke dynamics

As well as how you write with a pen, biometric data can also come from the manner and rhythm in which you type on a keyboard.

### Gait

Gait analysis looks at the unique way you walk, which is determined by a set of personal characteristics including your age, height and weight. Special cameras can be set up to analyze people’s walking style and identify them.

### Gestures

Other physical human gestures, usually from the face or hands, can also be used to identify you. Some smartphones today use facial or smile recognition to control unlocking the device.

* Soft Biometrics

Soft biometrics provide ancillary information but are not fully distinctive and permanent, so these features cannot provide a reliable person recognition. However, such ancillary information still can be used as a secondary information to complement the primary biometric traits (face, iris, etc.), and these features can be classified to physique (e.g., color skin, gender, ethnic origin), clothing (e.g., clothes’ color), or accessories (e.g., glasses, hat).

These soft biometrics can be used to study the continuous authentication of the smart phone users. In this paper, we lay foundational work for continuous authentication schemes that rely on touchscreen input as a datasource. We investigate if it is possible to authenticate users while they perform basic navigation steps on a touchscreen device and without any dedicated and explicit security action that requires attention from the user. Our goal is to analyze how robustly such schemes operate and if they are sufficiently reliable to be used on commodity devices.

LITERATURE SURVEY

In the paper presented by Zaire Ali et al[1], touch based gesture of the user by using accelerometer data to identify the position of the phone and the finger that is being used in a touch-based gesture. The data was collected through an Android App. Then, participants were asked to perform real-world activities such as browsing through a collection of pictures and reading a document. In addition, the application prompted users to perform tasks that required gestures such as taps, double taps, long taps and swipes in various directions. This process would repeat until the app has collected data from the participant’s left index finger, right index finger, left thumb and right thumb.

As we have seen in the previous paper that how hand movements play an important part in the as a behavioral feature, Now lets look at some soft biometric trends introduced by authors Rishabh Garg et.al[2]. This survey focuses on usage of multimodal approach to biometrics. Any trait can be used as biometric means of identification when it offers desirable characteristics such as acceptability, unique, permanence, collectability and identification.

In BioSoft presented by Debanjan Sadhya et.al [3], a new multi-modal database named BioSoft which consists of biometric data collected from 75 individuals. In comparison to the already existing databases, BioSoft contains a set of 23 soft biometric traits corresponding to each enrolled individual. The speciality it deals with is the ear and the soft traits.The biometric features in this database have been collected using international standard compliant hardware (sensors) and fixed acquisition protocols.

In order to identify the intruder from the user Kirill Leyfer et al[4] , proposed this paper. In this study, they collected a large amount of the raw input gesture data from the test users with the help of the improved version of our tool TouchLogger. Then process all the collected data to normalize it and extract the features which may represent users behavior. All the processed data will form our dataset used in this study. Then train the 1-vs-rest classifier on the dataset and evaluate its results. In our case, the Gradient Boosting classifier showed an average AUC metric of 0.97 in the task of a 1-vs-rest classification of a user with a dataset generated by 10 test users.

A different approach for authentication was oberserved by the authors Zdenka Sitova et. al.[5] have introduced Hand Movement, Orientation, and Grasp (HMOG), a set of behavioral features to continuously authenticate smartphone users. HMOG features unobtrusively capture subtle micro-movement and orientation dynamics resulting from how a user grasps, holds, and taps on the smartphone. It was observe that HMOG performed better when person was walking were due to hand movements caused by taps, or due to movements caused by walking, or a combination of both(7.16% in walking and 10.05% in sitting).

Chao Shen et al[6] developed an authentication mechanism examine the reliability and applicability of using touch-interaction behavior for continuous authentication in smartphone. They modeled touch behavior with newly proposed behavior features, and apply distance metrics to obtain a distance-based eigenspace. These techniques could handle behavioral variability to some extent, and make our proposed approach robust to behavior data.

A similar approach was observed in paper[7] where the authors Mario Frank et.al. They proposed a classification framework that learns the touch behavior of a user during an enrollment phase and is able to accept or reject the current user by monitoring interaction with the touch screen. In this paper, they lay foundational work for continuous authentication schemes that rely on touchscreen input as a data source. Investigate if it is possible to authenticate users while they perform basic navigation steps on a touchscreen device and without any dedicated and explicit security action that requires attention from the user.

Hui Xu et. al.[8] stated in their study how to model multiple types of touch data and perform continuous authentication accordingly.They have justified two critical properties distinctiveness and permanence. User features of touch operations are not stable over a period of time. Touch based authentication cannot achieve an error rate close to zero.

Soft Biometrics has many number of applications to deliver. One of them by the authors, Pedro Tome et. al[9], This paper presents an experimental study of the benefits of soft biometric labels as ancillary information based on the description of human physical features to improve challenging person recognition scenarios at a distance. Three labels were assigned such as Global, Head and Body based on which traits humans are able to consistently and accurately use when describing people at a distance. Three different challenging scenarios, varying the distance between camera and subject, have been defined and used in our experiments in order to understand the behaviour of soft biometric labels and their best application to biometrics at a distance.

* Close distance (∼ 1.5m). Includes both the face and the shoulders.
* Medium distance (∼ 4.5m). Includes the upper half of the body.
* Far distance (∼ 7.5m). Includes the full body.

Table: Literature Review

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sr No | Year | Name of Paper | Author | Content |
| 1 | 2016 | At your Fingertips: Considering Finger Distinctness in Continuous Touch Based Authentication for Mobile Devices | Zaire Ali,Jamie Payton and Vincent Sritapan | Touch Gesture Authentication |
| 2 | 2018 | Biometric Authentication using Soft Biometric Traits | Rishabh Garg, Anisha Arora, Saurabh Singh and Shipra Saraswat | Soft Biometrics |
| 3 | 2015 | BioSoft – A Multimodal Biometric Database Incorporating Soft Traits | Debanjan Sadhya, Parth Pahariya, Rishi Yadav, Apoorv Rastogi, Ayush Kumar, | Multimodal database |
| 4 | 2014 | Continuous User Authentication by the Classification Method Based on the Dynamic Touchscreeen Biometrics | Kirill Leyfer and Anton Spivak | Dynamic Authentication |
| 5 | 2015 | HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users | Zdenka Sitova, Jaroslav Sedenka, Qing Yang | Behavioral biometric, energy evaluation |
| 6 | 2015 | Touch-Interaction Behavior for Continuous User Authentication on Smartphones | Chao Shen, Yong Zhang, Zhongmin Cai | Touch screen authentication |
| 7 | 2013 | Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication | Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song | Touch Authentication |
| 8 | 2014 | Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones | Hui Xu, Yangfan Zhou, Michael R. Lyu | A survey study |
| 9 | 2014 | Soft Biometrics and Their Application in Person Recognition at a Distance | Pedro Tome, Julian Fierrez, Ruben Vera-Rodriguez, and Mark S. Nixon | Person Recognition |

GAPS IDENTIFIED

* It was observed that traditional smartphone authentication techniques were applicable only during the initial process of security. Once they authenticated the user by checking his/her credentials and comparing them with the database server these techniques did not check for the user’s approval till the time he/she logged out of the system. This provided a back door for the attackers to access the users system once some time has passed by. The attacker can manipulate user credentials and have access to sensitive information of the organization.
* These problems were persistent in Hard Biometrics, so an alternate method to keep a track on user authentication system is by use of Soft Biometrics. These techniques included gesture recognition, skin color, height, weight,etc. For the successful implementation of this continuous approach was proved to be helpful. No preregistration is required. But soft biometric are often merged with hard biometric to give required results.

MOTIVATION

As the number of smartphone users have raised, there arises a need for secure authentication. These smartphone companies provide various authentication techniques like PIN, password, fingerprint scanner and face scanning. But there was no mention of continuous authentication of smartphones. Some research papers have proposed the idea of continuous authentication of users using biometrics which deal with behavioral characteristics of user like the tapping, scrolling and swiping on the touch screen. This study focuses on continuous authentication of smartphone user on touch screen medium.

ASSUMPTION

A commodity smartphone can be used or a simulation tool. We can design a workflow model where inputs are users actions on touch screen which are captured and stored as a particular pattern. We can do analysis on the pattern stored and produce results.

OBJECTIVES

1. To study basics of continuous authentication on smart-phone touch screen.

2. To do comparative analysis of different methodologies.

3. To provide solution, to design more efficient authentication system for user using smartphone touch screen.

COMPARATIVE ANALYSIS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Approach 1** | **Approach 2** | **Approach 3** | **Approach 4** |
| Methodology | SVM, kNN | FAR,FRR | FAR,FRR,ROC | kNN,RF,Gradient Boosting ,Linear SVM |
| Results | ERR of 0 to 4% for SVM | FAR = 4.68%, FRR = 1.17% | Distinctiveness and Permanence | Gradient Boosting(AUC) = 0.9692 |
| Performance | If ERR is reduced performance can be improved | Continuous evaluation required, hence medium | Extensive Data sets required, hence slow | Medium |

AUC = Area Under Curve

FUTURE PLAN

1. To carry more study on methodologies/approaches.
2. To do comparative analysis of different methodologies.
3. To provide solution that helps in improving efficiency in authenticating user using smartphone touch screen.

CONCLUSION

We have studied various methods of Smartphone Authentication from traditional methods like passwords and pins to behavioral techniques like voice, sign, gait,etc. As we delve further it was seen that these traditional techniques has major trap doors that intruders could exploit. So soft techniques were proposed as for authentication of the user. In some papers, datasets were readily available to work with whereas on the other hand some papers have mentioned the need of multimodal database system incorporating the soft traits of the user. Various methodologies helped us to decide which one were feasible and which were costly. We plan to study further into these methodologies.

REFERENCES

1. At your Fingertips: Considering Finger Distinctness in Continuous Touch Based Authentication for Mobile Devices.
2. Biometric Authentication using Soft Biometric Traits.
3. BioSoft – A Multimodal Biometric Database Incorporating Soft Traits.
4. Continuous User Authentication by the Classification Method Based on the Dynamic Touchscreeen Biometrics.
5. HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users.
6. Touch-Interaction Behavior for Continuous User Authentication on Smartphones.
7. Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication.
8. Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones
9. Soft Biometrics and Their Application in Person Recognition at a Distance.
10. Hand Book of Biometrics