**Bio Touch Pass: Handwritten Passwords for Touch screen Biometrics**

**Alternative Title**: Efficient Password Mechanism to Overcome Spyware Attacks

**Aim:**

The main aim of this project is to develop user-friendly mobile applications ensuring data protection and high security.

**Synopsis:**

The rapid and continuous deployment of mobile devices around the world has been motivated not only by the high technological evolution that allows the communication and use of social media in real time, the two most prevalent user authentication approaches have been Personal Identiﬁcation Numbers and One-Time Passwords. In our proposed approach, users draw each digit of the password on the touch screen of the device instead of typing them as usual. The handwritten digits can be first recognized using for example an Optical Character Recognition. After this first authentication stage, the biometric information of the handwritten digits is compared in a second authentication stage to the enrolment data of the claimed user, comparing each digit one by one.

**Existing System:**

In existing system handwritten signature is one of the most socially accepted biometrics as it has been used in financial and legal agreements for many years and it also finds applications in mobile scenarios. These approaches are based on the combination of two authentication stages. The security system checks that the claimed user introduces its unique password correctly, and its behavioral biometric information is used for an enhanced final verification. The software for capturing handwritten numerical digits was developed in order to minimize the variability of the user during the acquisition process. The selection of a password that is robust enough for a specific application is a key factor. The number of digits that comprise the password depends on the scenario and level of security considered in the final application.

This effect has proven to be very important for many behavioral biometric traits such as the case of the handwritten signature.

**Problem Definition:**

* The amount of data requested to the user during the enrolment.
* The security level provided by the biometric system. From the point of view of the security system, it seems clear that the ideal case would be to have as much information of the user as possible.

**Proposed System:**

Our proposed system focus on providing user-friendly mobile applications ensuring data protection and high security. User should draw each digit of the password on the touch screen instead of typing them as usual. This way, the traditional authentication systems are enhanced by incorporating dynamic handwritten biometric information. Our system involves two stages of authentication the drawn pin should be similar to pin entered during registration process.

Our second stage of authentication involves multiple options based on user preference where user can set multiple set of combinations. User can set second stage password as stroke, time, screen brightness or sensor based authentication system. The incorporation of biometric information on traditional password-based systems can improve the security through a second level of user authentication.

**Advantages:**

* These approaches enable active or continuous authentication schemes, in which the user is transparently authenticated.
* Handwritten signature is one of the most socially accepted biometrics.
* The incorporation of biometric information on traditional password-based systems can improve the security through a second level of user authentication.

**Algorithm:**

* OCR

### Modules Titles:

### User Authentication and Ecommerce View Product

### Cart and Payment Using Biometric Hand Written Password

### Biometric Password Using Strokes

### Biometric Password Using Screen Brightness and Time

### Modules Description:

### User Authentication and Ecommerce View Product

User has an initial level Registration Process. The users provide their own personal information for this process. The server in turn stores the information in its database and user can view a list of products in their page multiple list of products and their details.

### Cart and Payment Using Biometric Hand Written Password

User can select a list of product they wish to purchase the selected product will be listed in a cart page and user can initiate general purchase information has to be filled. Completing general detail user has to draw their four digit pin one by one on screen. The drawn password then converted into an image through optical character recognition numbers from each image fetched and verified with user password.

### Biometric Password Using Strokes

### User has to register their four digit password with multiple strokes during their registration process once the process completed during confirm password .User has to confirm their password with same password with stroke has to be verified. Strokes for each drawn digits should match with strokes given at time of registration.

### Biometric Password Using Screen Brightness and Time

Spyware attack will be avoided by proposing the idea that uses the screen brightness as an authentication tool. The android secure environment generates the 6 digit binary value. Based on the binary digit the brightness of the screen gets changed to high or low. If the screen brightness is high the user should input the correct PIN digit. Else the user should give the wrong and random PIN number. The system will remove the digits which inserted while the screen brightness is low and apply the HMac algorithm for the PIN given by user and generate the Signature for the user PIN which is a digestible Value in order to avoid MAN-IN-MIDDLE attack. The server gets the signature of user generated PIN and generates the signature value for the Original PIN and compare two signatures. If the two Signatures are equal the user can access the Profile of the user. If not user can’t access the profile.

### Software Requirements:

* Windows 7 and above
* JDK 1.7
* Xampp
* Android Studio 3.4
* Android Phone

**Hardware Requirements:**

* Hard Disk : 500GB and Above
* RAM : 4 GB and Above
* Processor : I3 and Above

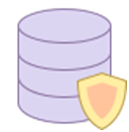
**Technology Used:**

* Core java, Android, PHP

**Conclusion:**

We propose the smart way to authenticate the social networking accounts belonging to them by using the screen brightness of android mobiles in order to avoid the spyware attack, shoulder surfing attack, and man in the middle attack.

**Architecture:**



Authentication

8

Draw Pin for registration

Ecommerce

Application

Type of Authentication need to verify

8

Password Authentication based on user input



Access denied



Access Granted