Online Signature Based Application Locking System

Aswathi Nambiar
Amal Jyothi College of Engineering, MG University,
Kottayam

Bibin Babu
Amal Jyothi College of Engineering, MG University,
Kottayam

Gokul Gopinadh
Amal Jyothi College of Engineering, MG University,
Kottayam

Sujith John Philip
Amal Jyothi College of Engineering, MG University,
Kottayam

Abstract

Data security and privacy are crucial issues to be addressed for assuring a successful deployment of biometrics-based recognition systems in real life applications. In this paper, we present a highly efficient and secured authentication scheme by online verification of signature. This authentication scheme is very simple and can be used for securing the applications and various elements which can be accessed and interfaced by touch panel’s inputs. This authentication scheme is very simple and can be used for securing the applications and various elements which can be accessed and interfaced by touch panel’s inputs.

Keywords: Signature Authentication, Data Acquisition, Data Storage

I. INTRODUCTION

Biometric authentication is gaining popularity as a more trustable alternative to password-based security systems. The objective of the biometric systems is to deduce the identity of individuals. Signature is a behavioural biometric. It is not based on the physical properties, such as fingerprint or face, of the individual, but behavioural ones. Signature of a person does not change over time and is a technique that is accepted by the public and is comfortable to the public. Signature authentication can be done by two ways: one is by offline method and other is online method. Offline method of signature verification takes the signature input as an image and processes it. Online signature verification uses signatures that are captured by pressure-sensitive tablets and the dynamic properties of a signature are extracted in addition to its shape. Dynamic features include the number of pixels, velocity, length of the signature and the time taken to make the signature making it difficult to forge.[1]

In an online signature verification system, the users are first registered by providing details and then can enter 5 signature templates. Then, when a user presents a signature (test signature) claiming to be a particular individual, this test signature is compared with the values that are computed from the stored templates. If the dissimilarity is above a certain threshold, the user won’t be able to login [2].

Verification will be based on a range of parameters that will be derived from the stored 5 templates. The input signature will be compared with derived values from the stored template of signature. The key advantage is that the user need not remember the password and can make an easy access to the application. This will make the transactions more secure.

II. SYSTEM OVERVIEW

The proposed method shares the general approach and an idea suggested by some previous systems, but differs from the previous work in the selection of the features, here all the features are taken in consideration during the verification. The overall process is outlined below.

During the registration the user inputs 5 signature templates which are used to derive the characteristics of the user’s signature. The reference set of signatures, together with these parameters, are stored with a unique user identifier in the system’s database.

When a test signature made by the user the signature parameters are compared with the parameters that are derived from the stored templates. The resulting minimum, maximum range values are derived and whether the input test signature parameter values lies between them is verified during the authentication.

During authentication we will be comparing the various parameters of the input signature with the derived respective parameters of the stored 5 templates. The parameters include velocity, pixel points, length of the signature and time taken by user to make the signature. Verification will be based on a range of parameters that will be derived from the stored 5 templates.

This authentication scheme is very simple and can be used for securing the applications and various elements which can be accessed and interfaced by touch panel’s inputs. The key advantage is that the user need not remember the password and can make an easy access to the application. This will make the transactions more secure.
These steps are explained in detailed in the following subsections:

**A. Data Acquisition:**
We are using a touch based mobile capable of accepting the input signatures. For each input signature number of pixel points, length of the signature, speed at which the user makes the signature and the velocity with which the signature is done is extracted and stored in the database.

**B. Signature Authentication:**
The characteristics are extracted from the 5 stored signature templates. The parameters like the speed and velocity at which the signature is done, the number of pixel points and the length of the signature are extracted from the signatures[1]. The minimum and maximum value for this parameter is derived and the parameters that are extracted from the test input signature are then compared with the corresponding parameters of the stored template; if the value lies in the range of the stored template the signature is genuine otherwise the signatures are not same.

**C. Data Storage:**
The parameters extracted from the signature are stored in the database. The parameters that are extracted from the signature i.e. the length of the signature, speed at which the signature is done and total pixel points as well as the time taken to make the signature those values are needed for the authentication of the signature. These derived characters of the signature are stored in the database.

**D. Signature Length Extraction:**
The length of the signature is calculated by the adding the distance between each pixel points. We have the total number of pixel points with those points we can find the distance between the successive points and then continue the step until the last point is reached. In this way the length of the signature will be based on the number of pixel points not on the distance between the first and last points [3].

**E. Registration & Login:**
The use needs to enter some basic details about the user. At the time of registration the user needs to enter 5 signature templates. The various parameters are extracted from these signatures and are stored in the database. While login an input test signature is made by the user and the parameters extracted from that signature are then compared with the values that is stored in the database which was computed from the stored templates. Once the registration is successful the user can login to the system using his/her signature.
F. Signature Verification:
The parameters extracted from input signature made by the user is compared with the parameters extracted from the signature templates and is verified. The number of attempts for a user is restricted. Only 5 attempts can be made by a user. If the signature is verified and is found to be true then the user will be able to login and can edit the signatures and details that were stored while the registration process [5].

III. CONCLUSION AND FUTURE SCOPE
In this paper we have presented an online signature verification system with an improved decision criterion to separate genuine and forgery signatures. The main contribution of our system is that it considers all the four parameters while making the verification. We have also studied the effects on the performance of some common approaches taken by previous signature Verification systems and came up with improvements or suggestions for various steps of the process. For instance here all the parameters are checked while the input signature is verified. Moreover, we showed that the pressure information does not seem to be a useful feature in distinguishing forgeries from genuine. This model if integrated with a image processing system could make up a higher secured system for authentication.

REFERENCES