International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 54 – 58

Online Signature Verification and Authentication using Smart Phones

Harshil Shah
Student, Department of Computer Engineering, MCT's Rajiv Gandhi Institute Of Technology
Mumbai, Maharashtra
harshilshah1910@me.com

Pranav Pawar
Student, Department of Computer Engineering, MCT's Rajiv Gandhi Institute Of Technology
Mumbai, Maharashtra
pranav.pawar661@gmail.com

Mr. S.P. Khachane
Asst Professor, Dept of Computer Engineering, MCT's Rajiv Gandhi Institute Of Technology
Mumbai, Maharashtra
khachnesp@gmail.com

Shikhar Sharma
Student, Department of Computer Engineering
MCT's Rajiv Gandhi Institute Of Technology
Mumbai, Maharashtra
shikhar168@gmail.com

Shrey Pithava
Student, Department of Computer Engineering
MCT's Rajiv Gandhi Institute Of Technology
Mumbai, Maharashtra
shreygalaxy3@gmail.com

***Abstract*—** The proposed system is designed to determine whether the person signing on any touch screen device is authenticated user or not. This can be done by verifying his/her handwritten signature which is a socially accepted biometric trait for authenticating an individual. There are two types of handwritten signature verification systems: offline and online systems. In an off-line system, just an image of the user's signature is acquired without additional attributes, whereas, in an online system, a sequence of x-y coordinates of the user's signature, along with many other attributes are also acquired. In our paper, we have created a client (mobile) application which captures the user's signature and extracts various features like pressure, time and x-y co-ordinates and the server application verifies these features to find whether the signature has been done by an authenticated user or a forger. The implementation is done using Python and the GUI is coded using Xcode.

Keywords- *Handwritten signature, biometric, verification, authentication, offline, online, forger, Python, GUI, Xcode*

*****

I. Introduction

Day by day, natural and secure access to interconnected systems is becoming more and more important. It is also necessary verifying people's identity in a fast, easy to use and user-friendly way.To achieve more reliable verification or identification we should use something that uniquely recognizes the given person.

Authentication is the process of proving or verifying ones identity. It can be categorized in three types : something we know, like passwords; something we have, like bus tickets or tokens; and, something we are, like our face, voice, signatures, etc. The third type is also known as Biometric. Together, these types are known as 3 factors of authentication[2].

Biometrics means the automatic identification of a person based on his/her physiological or behavioural characteristics[1]. This method of verification is preferred over traditional methods involving passwords and PIN numbers for its accuracy and case sensitiveness. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. These characteristics are measurable and unique.

Identification can be done using a person's identity based only on biometric measurements. The comparator matches the obtained biometric with the ones enrolled in the database using a 1: N matching algorithm for identification.Verification involves the process of confirming or denying a person's claimed identity. The biometric data obtained from the user is compared to the user's data already stored in the database.

In comparison with other already adopted biometric verification techniques, signature verification presents many likely advantages like nowadays it is a socially accepted method already in use in banks and credit card transaction. Also, it is useful for most of the new generation of portable computers and personal digital assistants (PDAs) use and writing as the main input channel. A signature may be changed by the user. Similarly to a password while it is not possible to change finger prints iris or retina patterns.

In signature verification, handwritten signature is commonly used and accepted as a way to verify people's identity.Signature verification usually consists just of an "eye inspection" as if we compared two photographs, but this is not an efficient method against imposters. Document examiners commonly compare a suspect signature with several example

 ISSN: 2321-8169
54 – 58

of known valid signatures. They look for signs of forgery which include i)signature written at higher speeds than normal, ii)rounded endings and beginnings, iii)poor line quality with shaking of line and iv)stops in places where writing should be free[5].

All signatures that can be used for verification are stored in a signature database. The system uses a database, in which each individual has 25 true signatures. At the same time, each individual makes 5 forgeries of every of his/her 5 immediately previous entries in the database. This means that for every individual we have 25 true signatures and 25 forgeries made by 5 different people. Also the efficiency of this system is more as the forger tries several times to imitate the true user's signature before the forgery is acquired and finally stored in the database.

II. Literature Review

Design Of Digital Signature Verification Algorithm Using Relative Slope Method: [3]

In this paper, signature is taken in 25 different conditions and that is used to match with signature made while authenticating. Normalisation, Hidden Markov Model and Relative Slope Algorithm are used. Comparison of database signature and input signature is made for authentication. Because 25 different conditions are used for the samples, so user can use the system in multiple conditions. Extra storage space is required to store 25 signatures.

Online Signature Verification For Multi-modal Authentication Using Smart Phones: [5]

Here, we collect data(Sample signature) and will represent it on x and y axis in every possible way which are upside down, take mirror image, take mirror image of upside down etc. After representing signal, we will calculate frequency of x and y coordinated in a 10x10 grid and also will calculate angle made by line using any two points of sampled signal with x axis. Algorithm used are Frequency String Method, Angle String Method. Therefore, this approach shows effective and easy way for feature extraction, easy to implement algorithm. But this system requires more processing time.

Online signature Verification Using Mobile Devices: [4]

The technique used in this paper tries to collect more precise data information such as considering time, speed, angle, pressure of signature Algorithms used are 1-Dimenstional histograms, 2-Dimentional histograms. The advantage of this paper is that more accurate and complex algorithms are explained here which will make almost next to impossible for an unauthorized person to login to the system.

III. Existing System

Most current login authentication systems such as one used in websites tend to require a combination of either email or username along with the user's chosen password[1]. These can be regarded as one-factor authentication techniques, as they only rely on one factor i.e. something you know. These authentications systems also might have "Security Questions" for the purpose of password recovery in case the user is unable to remember it[7]. These systems have many drawbacks. Firstly, the user is required to remember a password, often a separate password for each different service or website they use so that a password leak on one site doesn't leak all their passwords[6].

The security of these passwords from brute-force attacks is often dependent on the length of the password, which means that the user often is forced to make a trade-off between security (more complex and thus secure password) and convenience (simple and thus easy to remember, but less secure).

IV. Proposed system

In our proposed signature verification system, we take 25 sample signatures as input from user in different conditions and then 25 forgeries. These are all stored in a database. Normalisation is applied to signature made while logging in. HMM is used to segment the normalised sign and assign probabilities. Relative slope algorithm is applied to calculate the relative slopes of input and stored sign and then they are compared.

The algorithm uses simple geometric features to characterise signatures that effectively serve to distinguish signatures of different persons. We have a client (mobile) application which captures the user's data and the server application verifies the data. The implementation is done using Python and the GUI is coded using Xcode.

V. Workflow of the system

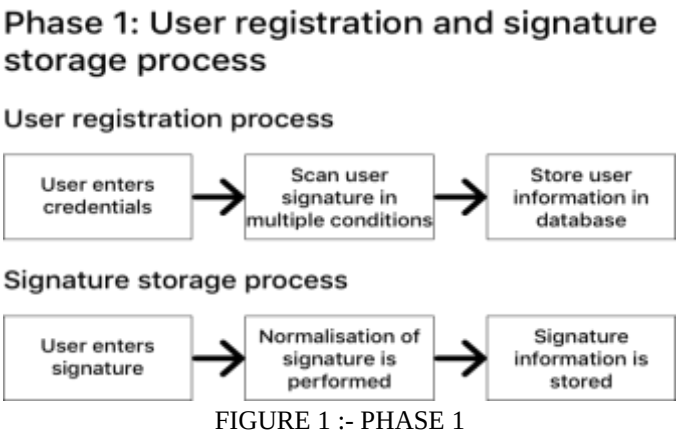

FIGURE 1 :- PHASE 1

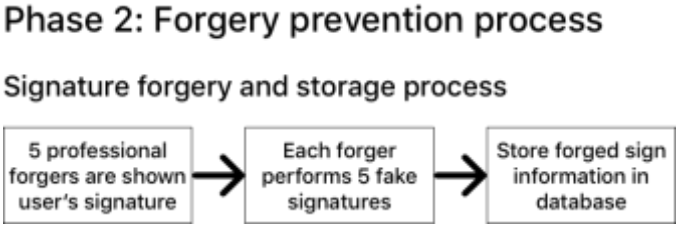

FIGURE 2 :- PHASE 2

 ISSN: 2321-8169
54 – 58

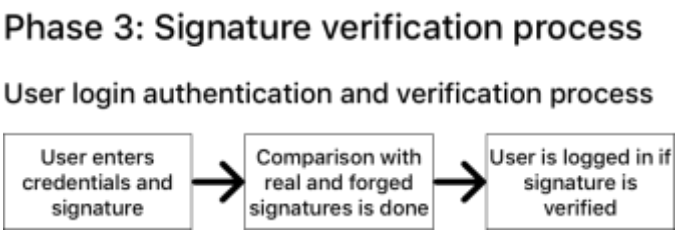

FIGURE 3:-PHASE 3

The above figures show the workflow of the proposed system in phases.

Phase 1:

In user registration process user credentials is recorded, and along with the signature performed by the user in multiple conditions it is stored in the database. For signature storage, first the user is made to perform signature in multiple different conditions. Then, normalization is performed on the signatures, and this data is then stored in the database.

Phase 2:

It consists of forgery prevention process in which we show user's signature to 5 professional forgers, each of which performs 5 forged signatures of the user's real signature. This data is then stored in the database.

Phase 3:

This phase involved verification of signature in the login process. In this, user enters credentials and signature to verify. This signature is then compared with the real and forged signatures as stored in the database. If the signature is verified as authentic, the user is logged in.

The proposed system is majorly implemented by using 2 algorithms:- Relative Slope Algorithm[3] and Hidden Markov Model[1][2].

Relative Slope Algorithm(RSA):-

This algorithm calculates all the slope values of the stored signature[3]. The steps to be followed are given below:-

Various steps to be followed are given below:

1) Using optimize HMM we can calculate the segment of the signature. Then segment can be combining to form a line segment.

2) After the line segment are obtained the relative slope are calculated.

3) Slope of line: S=dy/dx Where: dx=x2-x1 dy= y2-y1

4) For the first segment we calculate the slope between the starting point of the first segment and the ending point of the last segment.

5) However, the for the further line segment the slope is calculated based on the previous line segment.

6) In the first step global time required to put the signature and calculate.

7) The second step used to calculate the length of signature completed in unit time for this two tier time metric extraction algorithm is used.

8) And finally in verification step two level verification algorithm used in first level of verification relative slope value compare with previous value

9) And the second level extracts the global and local features consisting of relative slope value, total length and global time.

10) If the signature passes the second level of verification it considered as genuine signature

Hidden Markov Model(HMM) :-

A hidden Markov model (HMM)[1] is a statistical Markov model in which the system being modelled is assumed to be a Markov process with unobserved (hidden) states. In a hidden Markov model, the state is not directly visible, but the output, dependent on the state, is visible. Each state has a probability distribution over the possible output tokens[8]. Therefore, the sequence of tokens generated by an HMM gives some information about the sequence of states.

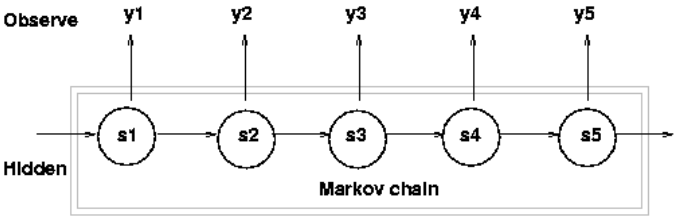

Figure 4:- Markov Chain

A Markov chain given in above figure 4 consist of two states, one is known as hidden states and other is known as observable states. Every observable state is connected to its respective hidden state which we need to find. Looking at the observable state we predict the hidden state, this is the essence of both Hidden Markov model and Markov chain.

Also there are 2 probabilities in HMM as given below:-

1)Transition probability :-

the probability of going from a given state to the next state in a Markov process.(probability of hidden state)

2)Observe probability

It is the probability of any visible state.

The basic idea of implementation of HMM in our paper is assigning initial probability to each state. During the process of feature extraction we will extract various features like pressure, time, slope and x-y co-ordinates. As the slope aspect has been covered by above algorithm we are considering pressure for implementation of markov model. Different readings of pressure form different state of markov model and to each state we assign a initial probability and and also calculate the transition probability to each state. This can be done by following the steps given below:-

 ISSN: 2321-8169
54 – 58

1) The very first step is to run a loop through the available dataset and find the max value and min value
2) After calculating min and max value use formula (max - min)/5 to divide the hole dataset into 5 ranges
3) Then again run a loop determine the number of time a data set is occurring in that range divided by the total number of datasets.
4)Transitional probability=(Occurrence in particular range/ Total datasets)
5) Now initial probability is assigned according to the formula (Occurrence in particular range/ 5)
6) Now this process is repeated for both forged and real datasets of a particular user and value is stored
7) Now the real time signature of user is present state and all calculate ranges are act as transitional states(Hidden States) or all set of possible state in which the system can make transition to.
8) Using above states we predict whether the signature is of real user or forged user(Observational state).

VI. Implemented System

The system uses a GUI to capture 25 signatures of authenticated user as well as 25 signatures of forgers. While implementing, the signatures were done by 1 authenticated user and 3 forgers. Figure 5 shows the signature of the authenticated user being accepted. Whereas figures 6, 7 and 8 shows the signatures of the forgers being rejected. Due to the normalization algorithm[7] the user can sign anywhere on the screen and the result would remain unaffected by it.

Figure 5:- Result when authenticated user signs

Figure 6:- Result when a forger signs

Figure 7:- Result when a forger signs

Figure 8:- Result when a forger signs

VII. Conclusion & future work

In the current times of increasing forgeries, it is important to use a system which will help to efficiently manage user authentication in a more systematic and secure manner. Criminal experts can be employed at every place and hence there is an increase in need to develop computerized algorithms that could verify and authenticate individuals identity. Our mobile based authentication system can be considered as a complete solution for multi-factor authentication. This is because we extract features of the users in real time and have created a training model with the help of 3-4 forgers which will cover various forgeries that could be done by many professional forgers.

In future, we would like to work on increasing the systems accuracy so that it can perform at its best even in 1-sigma range[8]. To increase the accuracy we could implement many more algorithm such as optimized HMM, Angle deviation method[7] also we can reduce the size of the database as 25 copies of signature each for real and forger will occupy lot of database.

VIII. References

[1] Juan J. Igarza, Iñaki Goirizelaia - "Online Handwritten Signature Verification Using Hidden Markov Model"

[2] Javier Ortega-Garcia, Daniel Ramos- "HMM-Based On-Line Signature Verification: Feature Extraction & Signature Modeling"

[3] P.N .Ganorkar, Kalyani Pendke - “Design Of Digital Signature Verification Algorithm Using Relative Slope Method” - eISSN: 2319-1163 | pISSN: 2321-7308, August 14

[4] Napa Sae-Bae, Nasir D Menon- **“**Online Signature Verification on mobile devices” - ISSN 2250-2459, June 2014

[5] Navid Forhad, Bruce Poon, M. Ashraful Amin, Hong Yan - “Online Verification for multi-modal Authentication using Smart Phone” -ISSN: 2078-0958, Volume 1, March 2015

[6] Kiran Kumer Gurrala, Sukadev Meher- “Online Signature Verification Techniques” - ISSN: 2319-7064, November 13

[7] Aswathy K. V. - “Online Signature Verification Techniques: A Survey”, ISSN 2091-2730

[8] Beton, M., Marie, V., Rosenberger, C.: Biometric secret path for mobile user authentication: A preliminary study. In: 2013 World Congress Computer Information Technology, pp. 1–6 (2013)