Online Signature Verification system

Conference Paper · April 2009

DOI: 10.1109/CSPA.2009.5069177 · Source: IEEE Xplore

6 authors, including:

Fauziyah Salehuddin
Technical University of Malaysia Malacca
101 PUBLICATIONS **370** CITATIONS
SEE PROFILE

Hazura Haroon
Technical University of Malaysia Malacca
65 PUBLICATIONS **124** CITATIONS
SEE PROFILE

Zahariah Manap
Technical University of Malaysia Malacca
14 PUBLICATIONS **113** CITATIONS
SEE PROFILE

Online Signature Verification System

Julita A., Fauziyah S., Azlina O.,
Mardiana B., Hazura H., Zahariah A.M.
Fakulti Kejuruteraan Elektronik dan Kejuruteraan Komputer (FKEKK)
Universiti Teknikal Malaysia Melaka (UTeM)
Hang Tuah Jaya, 75450 Ayer Keroh, Melaka

***Abstract*- Online Signature Verification is a process of verifying the writer's identity by using signature verification system. This system can be use as a security system such as verification for assessing entry application and password substitutions. Signature verification technology requires primarily a digitizing tablet and a special pen connected to the Universal Serial Bus Port (USB port) of a computer. An individual can sign on the digitizing tablet using the special pen regardless of his signature size and position. The signature is characterized as pen-strokes consisting x-y coordinates and the data will be stored in the signature database in the form of a txt.file. These characteristics uniquely identify a person and cannot be mimicked or stolen. In this project, the method of Support Vector Machine (SVM) is used to focuses in verifying the signature.**

I. INTRODUCTION

As we all know, each individual has his own special characteristics that no other have. These characteristics are indeed important in recognizing and authenticating individual. Since authentication of individuals has rapidly become an important issue nowadays, researchers have carried out a lot of research in this biometric field using those special characteristics of each individual for authentication. Biometric field research includes hand geometry, face prints, fingerprints, voiceprints, signatures, and non-retinal blood vessel analysis. Biometrics has been widely used in physical access control applications. Unlike personal identification number or pin, biometric features are something about the characteristics of a person [2]. Biometric features are used to provide an enhanced level of security and identification. Signatures are one of the most popular and reliable biometric features for verifying person's identity.

In this paper, a new approach for the verification of signatures based on the Support Vector Machine (SVM). The Support Vector Machine is a new type of learning machine for pattern recognition and regression problems, which constructs its solution (decision function f) in terms of a subset of the training data, the Support Vector. Support Vector Machines (SVM) is very popular since a few years. As they provide very good results for various pattern recognition problems, they also seem to be a good choice for online signature recognition. Compared to most methods used for signature verification such as Hidden Markov Models (HMM) or Dynamic Time Warping (DTW), SVM, which are based on the principle of structural risk minimization, have various advantages such as a convex objective function with very fast training algorithms. On the other hand, SVM typically are applied to data sets containing feature vectors of fixed length and not to problems dealing with time series of variable length such as in online signature recognition [6].

SVM is mainly used in classification and regression problems. In classification it involves estimation of the decision function, f using a set of training data with the labels that will correctly classify unseen test examples. Meanwhile, for regression, it is the estimation of real-valued functions, which is carried out in analogous manner to the case of pattern recognition.

II. METHODOLOGY

This section describes the methodology of the project which includes data capture, data acquisition, size normalization, feature extraction and matching image. The block diagram of the project is shown in Fig. 1.

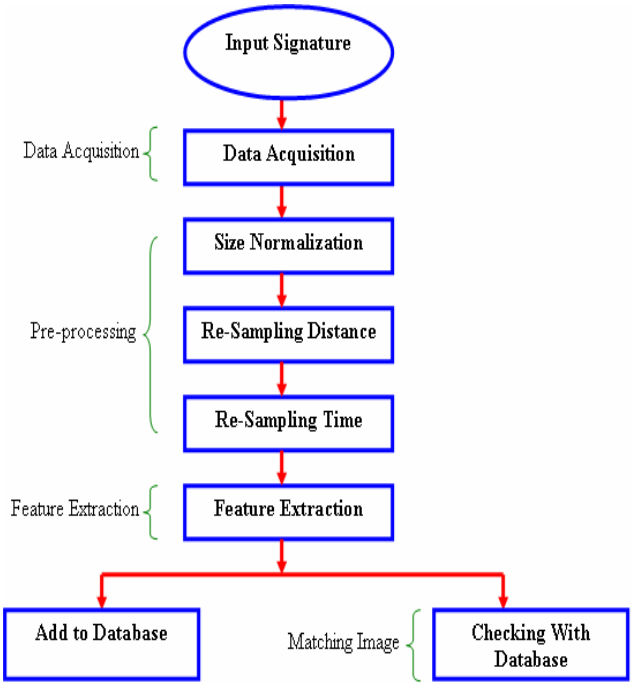

Fig. 1. Block diagram of the project

A. *Input Signature*

The input signature will be read in the x-y coordinate where the points of the signature are traced along the whole signature tracing the points correctly will enable us to know the points of the pen such as pen-up points and pen down points. This data is important and will be stored in the signature database. The main pen-down point would be the first point which indicates the ending of the signature.

Therefore the overall shapes of the signature can be presented in the sequence of conservative points in x-y coordinate. Then, these data will be stored in the signature database in the form of a txt.file.

B. Data acquisition

Data acquisition is required to acquire the signature of the user which can be based on a variety of input tools. Data acquisition process is a process where the real time inputs of signature from the digitizing tablet and the special pen are read into the CPU for processing and to store the signature in the database which called Signature database. The digitizing tablet is sending the real time inputs to the CPU for further processing and storage. The connection between signature tablet and PC can be seen in the following figure attached (Fig. 2).

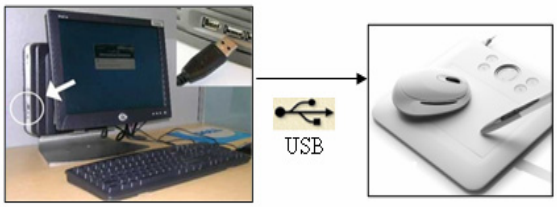

Fig. 2. The connection between tablet and PC.

C. Pre-Processsing

Pre-processing contains three steps: Normalization, Re-Sampling Time and Re-Sampling Distance. As we all know, a person's signature will always differ in size every time he sign on a paper or on other materials. Thus here comes the need for the size normalization to make each person's signature the same in size before starting to extract it features. This is to avoid the developed software to falsify a genuine signature just because of the different is sizing.

Size normalization is performed by scaling each character both horizontally and vertically [1]:

$$x_i = \frac{x_i^{\,o} - x_{\min}}{x_{\max} - x_{\min}} W$$
$$y_i = \frac{y_i^{\,o} - y_{\min}}{y_{\max} - y_{\min}} H \qquad (1)$$

where (x_i^o, y_i^o) denotes the original point (x_i, y_i) is the corresponding point after the transformation

$$x_{\min} = \min i\{x_i^o\},\ x_{\max} = \max i(x_i^o)$$
$$y_{\min} = \min i\{y_i^o\},\ y_{\max} = \max i(y_i^o) \qquad (2)$$

where W and H are the width and height of the normalized signature respectively. Re-sampling is done to make the raw data points equidistant in time using a simple linear interpolation algorithm as follows. The re-sampling step ΔS is a fraction of the total arc length L:

$$d_i = \sqrt{(x_i - x_{i+1})2 + (y_i - y_{i+1})2}$$

$$L = \sum_{i-1}^{n-1} d_i$$
$$\Delta S = \frac{L}{n_1} \qquad (3)$$

Where d_i denotes the distance of point to point and n is the number of points. After re-sampling, the characters have a fixed number (n_1) of points per character (50 points in our system) which provides a fixed size input.

D. Feature Extraction

The purpose of the feature extraction module is enhanced the variability which helps to discriminate between classes. In this system integration of the online features are used. Online features includes: pen-up down, pen coordinates, direction θ ad curvature □. A binary feature "1" indicates the pen is touching the pad (pen-down) and "0" indicates the pen is not touching the ad (pen-up). The direction of a stroke is determined by a discrete approximation of the first derivative with respect to the arc length. These approximations can be calculated as shown in Fig. 3 in which the following calculations are required.

$$\cos\theta(n) = \frac{\Delta x(n)}{\Delta s(n)} \qquad (4)$$
$$\sin\theta(n) = \frac{\Delta y(n)}{\Delta s(n)} \qquad (5)$$

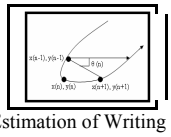

Fig. 3. Estimation of Writing Direction

The curvature of the strokes as the second derivatives d^2x / ds^2 and d^2y / ds^2 are not bounded on and the local curvature are approximated by the angle between two elementary segments. This can be shown as in Fig. 4. This angle is also encoded by its cosine and sine. Using the subtraction formulas for sine and cosine these values can be calculated as:

$$\cos\phi(n) = \cos(\theta(n+1) - \theta(n-1)) \qquad (6)$$
$$\sin\phi(n) = \sin(\theta(n+1) - \theta(n-1)) \qquad (7)$$

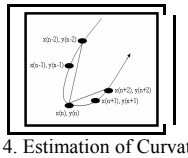

Fig. 4. Estimation of Curvature

III. EXPERIMENTATION ANALYSIS AND RESULTS

An experiment is carried out to determine the accuracy of this software, so as to prove that the objectives of this project have been achieved. This experiment involves two sections, which are software validation to prove its

effectiveness in different and an analysis from a population of 10 registered users.

A. Software Validation

Software validation has been carried out to show the effectiveness of this software in verifying signatures. Before a signature can be verified as a genuine signature, there are many aspects to consider first. Thus a validation could be made to test the results obtained through this software.

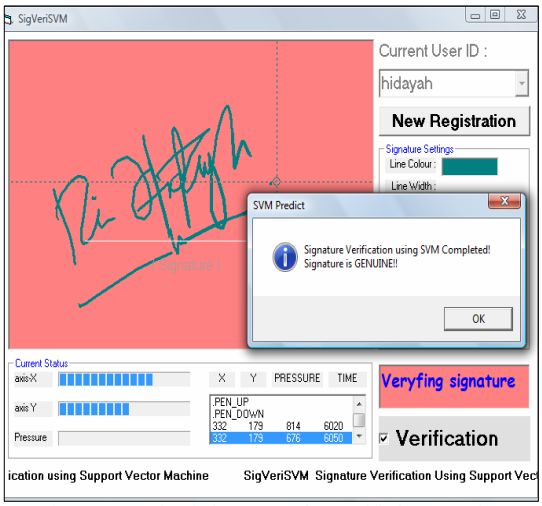

Fig. 5. Example of Signature Being Verified As Genuine

Basically, the validation process, which has been carried out is based on three aspects such as orientation of the signature in coordinate x and y, pressure applying when signing the signature and time used to sign the signature. Above is Fig. 5 showing a signature that matches the criteria needed in a signature to be verified as genuine signature.

For the orientation aspect, it takes upon the X-coordinate and the Y-coordinate as the reference. Normally, a user's signatures will definitely having the same orientation each time he or she signed. If the user signs in wrong orientation, which the changes in X-coordinate and Y-coordinate are significant, thus the signature will be verified as a forgery signature. Below is Fig. 6 showing the different orientation of signatures, which are the root cause for being verified as forgery signature.

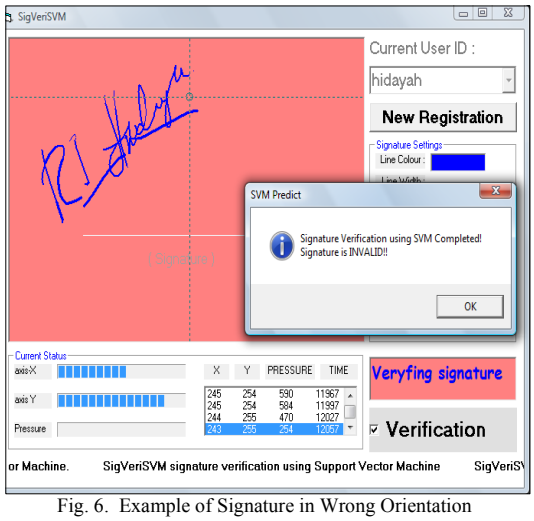

Fig. 6. Example of Signature in Wrong Orientation

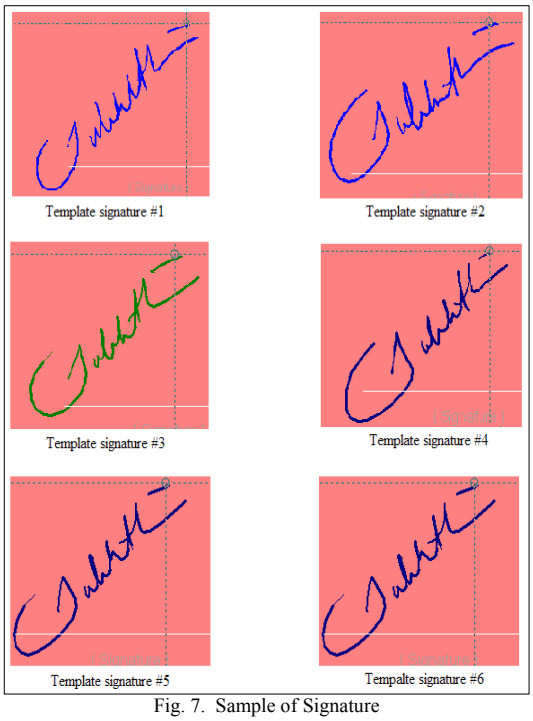

Fig. 7. Sample of Signature

As for the pressure aspect, a signature will be verified as forgery signature if the pressure applied from the pen towards the digitizing tablet is significantly different from the genuine signatures that have been trained. The pressure is measured through values where a higher value shows that pressure is hard and vice versa. Below is Fig. 8 showing different pressure applying when signing a signature that causes it to be verified as forgery

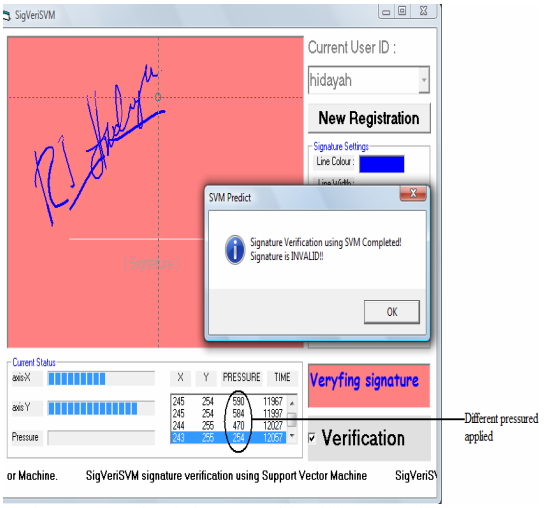

Fig. 8. Example of Signature with Different Applied Pressure

B. *FRR and FAR Analysis*

There are two quantities used to characterize the performance of the signature verification algorithm. False Rejection Fate (FRR) is defined as the percentage of genuine signatures being wrongly verified by this software as forgery signatures. False Acceptance Rate (FAR) is then defined as the percentage of forgery signatures being wrongly verified by the software as genuine signatures.

$$FRR = \frac{\text{Total Number of Tested Genuine Signatures}}{\text{Total Number of Rejected Genuine Signatures}} \times 100 \quad (8)$$

$$FAR = \frac{\text{Total Number of Accepted Forgery Signatures}}{\text{Total Number of Rejected Forgery Signatures}} \times 100 \quad (9)$$

Below is Table 1 showing the results obtained throughout the whole experiment to analyze the False Rejection Rate and False Acceptance Rate to prove the accuracy of the software developed to verify online signatures.

TABLE 1
Results Obtained Through FRR and FAR Analysis

		Genuine Signature		Skilled Forgery Signature		Unskilled Forgery Signature	
No	UserID	Tested	Rejected	Tested	Accepted	Tested	Accepted
1	Hidayah	10	0	5	0	5	0
2	Julita	10	1	5	0	5	0
3	Rifhan	10	2	5	0	5	0
4	Ismail	10	2	5	2	5	1
5	Cyndi	10	0	5	0	5	0
6	Rena	10	1	5	0	5	0
7	Rahman	10	2	5	0	5	0
8	Prema	10	1	5	0	5	0
TOTAL		80	9	40	2	40	1

The results show that the system is effective to recognize online signature with a high accuracy in real time. In the future, it is possible to improve accuracy using new feature extraction techniques and recognition methods. Also, the system can be potentially improved for the online recognition system genuine signatures. The FRR and FAR have to be as low as possible for achieve the accuracy of signature verification at 100%. The low rate of FRR and FAR have shown that this software has the capability to verify signatures within the range of acceptable accuracy.

IV. DISCUSSIONS

From the results that are obtained throughout the validation of software, it basically proves that this software has the capability of disregard of genuine signatures that do not meet the specific requirement. Even the slightest mistake in the genuine signatures can be verified a forgery signatures. This tight security that this software has will indirectly contribute towards the increased False Rejection Rate but manage to lower down the False Acceptance Rate where forgery signatures can be hardly verified as genuine signatures. Additionally, it also causes inconvenience towards user whom is not consistent in their own signatures. This investment of this tight security into the software is more worthwhile compared to having low security where the FRR will be lower down but there is an increased rate in FAR. Lower security of this signature verification software will boost more forgery cases to happen around the world.

V. CONCLUSIONS

This project is basically about the development of online signature verification using Support Vector Machine in verifying signatures that is either genuine or a forgery signature. In verifying signatures, the signatures will be processed through this software and this software would have the ability to tell us to accept or not this currently input signature. Thus the ability of this software is in verifying signatures of anyone who already has a database in this software stored in the signature database. Verifying signatures has to be accurate and reliable in order to have high quality of the software. Therefore, the error rate used to measure the accuracy and reliability of this software has to be as low as possible and within an acceptable range. Thus, the FAR and FRR has to be low and if possible 0%, meaning it has a perfectly accuracy. With its many applications of this software into our daily life especially on the transaction of financial, therefore, online signatures verification has great potential biometrics technology. The application of automatic online signature verification will become increasingly accepted in the real world.

ACKNOWLEDGMENT

First of all I would to thanks to our sponsor UTeM, secondly to our Dean, Prof. Madya Muhammad Syahrir Johal and Deputy Dean (Research) Mr. Imran Ibrahim and my Head of Department, Mr. Sani Irwan Md. Salim.

REFERENCES

[1] Abdul Fadlil, Marzuki Khalid, Rubiyah Yusuf (2005). *Online Handwritten Character Recognition Based On Online-Offline Features Using BP Neural Network* Centre of Artificial Intelligence.

[2] Andrew W. Moore (2001), *Support Vector Machine*. Carnegie Mellon University.

[3] Anil K.Jain, Salil Prabhakar ans Sharath Pankati, *Biometric Recognition: Security and Privacy Concern*, IEEE Transaction, 1994

[4] A.K.Jain,F.D.Friess, and S.D. Connel (2002). *Online Signature Verification*. Pattern Recognition, Vol 35 , pp. 2963-2972.

[5] A.Pacut, A Czajka,"Recognition of Human Signatures",pp. 1560-1564, 2001

[6] Bin Li, Kuan –Quan Wang, and David Zhang, *On-Line Signature Verification For E-finance and E-Commerce Security System*, IEEE Transaction, 2004

[7] Byron Anderson and Yi Gu, *Real Time Dynamic Signature Verification*, Goggles Transaction, 2004

[8] Cemil OZ, Fikret Ercal Demir. *Signature Recognition and Verification With ANN*. Sakaraya University

[9] Claus Bahlman, Bernard Haasdonk and Hans Burkhardt (2002). *On-line Handwriting Recognition wit Support Vector Machine-A Kernel Approach*. Albert Ludwings- University Freiburg, Germany.

[10] E.J.R Justino, F. Bortolozzi, R.Sabourin , "*Off-line signature verification using HMM for random simple and skilled forgeries*", Proc. 6th Intl. Conf. On Document Analysis and Recognition, 2001, pp. 450-453

[11] Rosielawati Binti Zawawi, *Thesis The Electronic Lock Using Signature Recognition By neural Network*, 2005

[12] V.S Nalwa (1997). *Automatic On Line Signature Verification*. Proceedings of IEEE, vol 85, pp 215-239.

[13] Woan Ning Lim, Yong Haur Tay, Marzuki Khalid (2005). *A Handwritten Character Recognition System Based On The Fuzzy Neural Network* Centre Of Artificial Intelligence

[14] Yong Haur Tay. Offline Handwritten Signature Recognition Using Hidden Markov Model (HMM) Centre of Artificial Intelligence

[15] Jose L. Camino M Travieso, Ciro R. Morales and Miguel A.Ferrer,*Signature Classification by Hidden Markov Model*. IEEE Transaction, 1999

[16] J.N.K Liu G.S.K Fung R.W.H Lau, *A signature Based Password Authentication Method*. October 1997 Proceedings of 1997 IEEE International Conference Of System, Man and Cybernetic, 631-636

[17] Mihai Costin Manolescu. *Signature Recognition Project*. Googles Transaction, 2004