

Evaluation of Online Signature Verification Features

Ghazaleh Taherzadeh*, Roozbeh Karimi*, Alireza Ghobadi*, Hossein Modaberan Beh**

* Faculty of Information Technology Multimedia University, Selangor, Malaysia

Gazaleh.taherzadeh07@mmu.edu.my

roozbeh.karimi06@mmu.edu.my

alireza.ghobadi@mmu.edu.my

** SOHA Sdn. Bhd. Cyberjaya, Selangor, Malaysia

modaber@soha.com.my

Abstract— in this paper, the methods used by literature to address online signature verification is studied. We propose new set of combination of current features to challenge the online signature verification. At the end, we examine one of the aforementioned methods and show the results. This research explains the classified biometrics elements in two main categories: physical and behavioural.

Keywords— Online Signature Verification; Feature Selection; Feature Extraction

I. INTRODUCTION

In these past few years, due to development and usage of communication and technology in industry, such as banking, verification for evaluating entry application, and password substitutions and etc., there is an increasing need of enhancing level of trust and applying security using biometrics elements which are also known as authentication techniques [1]. Biometrics elements are classified into two main categories: physical and behavioural [2]. Among all these biometrics elements, signature verification is considered as one of the most reliable and effective approaches in security field.

Signature verification is categorized into two main types: Static and Dynamic. Static type which is also known as Off-line verification is the process of verifying signature using pen and paper. Dynamic type, which is also known as On-line verification, is the process of verifying signature using digital pen and tablet PC. The main aim of these two methods is to compare the signature in query to the pervious sample of the signer's signature by computer and special software.

Reliable signature verification can be employed in many applications areas such as banking, law enforcement, industry, and security control. Signature verification owns best reliability among others methods, since for stolen signature the user can change or modify his/her signature whereas he/she cannot change the unique characteristics such as face or finger print. On the other hand, online signature verification uses the dynamic information such as speed, and pressure which are achieved by some special instruments during signing process. It also displays better results in contrast with static signature.

Numerous methods and algorithms have been proposed to address this problem [3-6]. Many global and local features have been employed in order to evaluate the effectiveness of

these methods and algorithms [7-8]. Many Researchers has been achieved to the discriminatory power and high consistency of these features. However, the analysis and measurement of these features individually have not been paid attention adequately.

In this paper, the current study on online signature verification methodologies and features was studied and analysed. The experimental work was conducted on analysing and evaluating all the features of online signature verification and combination of its features. According to previously achieved results found in literature, a comparative study was also done on the features and the detail of usage of each feature.

The process of our experimental work and signature verification include five steps as follow: 1) Data Acquisition: collect data from existed databases; 2) Pre-processing: contains three stages: i) Normalization, ii) Re-sampling, iii) Smoothing; 3) Feature extraction; 4) Feature matching; 5) Result.

II. SIGNATURE VERIFICATION OVERVIEW

Signature verification is the process used to recognize an individual's handwritten signature in order to prevent fraud. Signature verification is the task of authenticating a person based on his/her signature. Online (dynamic) signatures are signed on pressure sensitive tablets that capture dynamic properties of a signature in addition to its shape, while offline (static) signatures consist of only the shape information. Dynamic features, such as the coordination and the pen's pressure at each point along the signature's trajectory, make online signatures more unique and more difficult to forge in comparison with offline signatures.

III. SIGNATURE VERIFICATION METHODOLOGY

The first off-line and on-line signature verification respectively conducted by Nagel and Rosenfeld and Liu and Herbst [9]. In the following of these studies, varieties of methods and algorithms have been proposed to tackle this problem. Among the proposed methods, several approaches achieved higher prediction accuracy and lower rate of error than the others. Furthermore, much research has followed

attempting various methods for both feature extraction and matching. Some of previous works are highlighted in this part.

The other method, which was two-stage fusion to find Global and local features, proposed by Ning-Ning Liu and Yun-Hong Wang[10]. Global features are extracted as a 13 dimensional vector and the locals are extracted as time functions of various dynamic properties. Then a two-stage serial procedure is expected to combine the global and local features.

Three groups of experiments are conducted. They are the global method based on majority voting rule, the local method based on traditional DTW (Dynamic Time Warping) and enhanced DTW algorithm, and their combination through two-stage serial procedure, respectively. The experimental results prove that this method achieved a 4.02% equal error rates (EER) on SVC2004 TASK2 in comparison with the previous methods have done on SVC2004, which obviously demonstrates the benefits of fusion global and local information for on-line signature verification.

These verification systems are required a simple device which is easy to use, the pen based tablet systems are employed to attain a sequence of X-Y coordinates and pressure of the pen, since the signature is made on the surface of the tablet. Velocity, acceleration, distance travelled and another features of the signature will be obtain based on analysing this sequence of X-Y coordinates [11].

Each person has a different signature, which can be in different shapes and in different situations. Since a signature, has some features, and it is made by a user with raw data, it is consider as an input of the system. This input is going to process based on some predefined methods. To process by these methods, signature needs to be standardized based on some methods.

After standardization which is called pre-processing, features are extracted from a signature and gave the outputs which are in known signals for system. Then, a classifier will compare and test the output with the signature which is stored in a database. The result will be verified when a matched signature with output has been found in a database. The overview of a system is shown in Fig. 1.

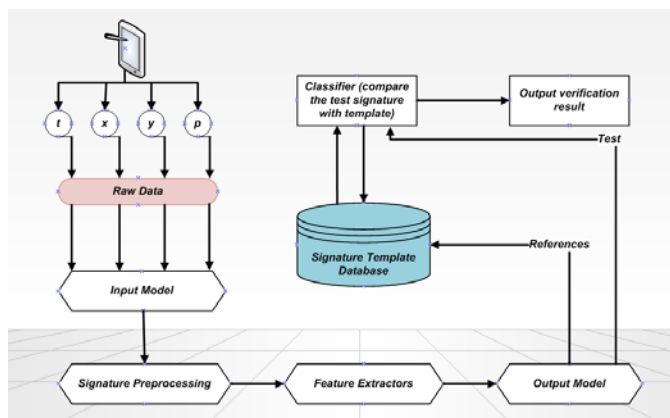


Fig. 1 overview of a system.

A. Data Acquisition

One of the signature verification subdivisions is Data Acquisition that is required to obtain the signature of the user which can be supported by different types of input tools to collect the signals for classification. Data acquisition process deals with the real time inputs of signature from input instrument, such as: the digitizing tablet and the special pen which are read into the CPU for processing and to store the signature in the database which called signature database. The digitizing tablet sends the real time inputs to the CPU for further processing and storage [12]. In general, two types of signature data are stored into the database. First type is user's genuine signature and the other type is skilled forgeries. Emulators may attempt to copy the user's genuine signature to check the accuracy of the system. Available database is used to test the functionality of the system. Typically, some of the most available databases are: SVC2004, BIOMET, and MYCT. According to the previous works, the majority of the methods and algorithms have employed SVC2004 database [13]. Each database consists of 100 sets of signature data. Each data set contains 20 genuine signatures and 20 skilled forgeries (e.g. Fig.2). Out of this set of signature, only signature data which are the first 40 signers are available for developing and evaluating the system proposed by researchers. Some features are available in SVC2004 database, such as: X-coordinate, Y-coordinate, Time stamp, Button status, Azimuth, Altitude, and Pressure.



Fig. 2 left side figures show genuine signatures and the right side figures show forgery signatures [14].

B. Pre-processing

As we mentioned in the previous sections, signature of each person will be change under different situations. Thus, the system needs to have a standardize signature by applying pre-processing.

The objective of the pre-processing phase is to get rid of noise from the input signature. Pre-processing contains three steps: Normalization, Re- Sampling Time and Smoothing [9].

1) Normalization

There are few kinds of tablets with variety of size for the different usages; people habitually may scale their signature to fill all the available free space in the tablet's area. However, the difference of size between two signatures is one of the

problems dealing with pre-processing (Fig.3) [11]. This problem could not be always solved by using scaling since the signature may have a different aspect ratio. Therefore it is better to apply normalization algorithm which respects to both width and height. Signature size can be normalized according to one of the dimensions (width or height), which does not completely remove size characteristic of a writer. It is also known that people does not equally scale their signatures with respect to width and height [15]. The size of signature is considered as one of the writer particular characteristics, i.e. considering, there is no difference in the size of active area of tablets which are used in system. Thus, writer may always sign in large or small signature.



Fig. 3 Example of normalization.

2) Re-Sampling

Re-sampling is a process which is used by some researchers to resample the input signature. The basic task of re-sampling is eliminating the redundant points of signatures (Fig.4). Once two signatures compared with respect to their shape they must be re-sample to extract more consistent shape features. From other point of view, re-sampling results in significant loss of information, since the apparently redundant data include speed characteristics of the genuine signer [11]. One of the problems with re-sampling is that the critical points, capturing the characteristics of the signature, may be lost. Critical points are sometimes added separately to the set of equidistant points obtained after re-sampling to solve this problem [15]. Dynamic Time Warping is the method which is used in this work, so that; need to consider that DTW-based systems may resample the signature into an equal-distant point sequence before string matching [16-17].



Fig. 4 a) Original b) After re-sampling [15].

3) Smoothing

Because of using digitizing tablet and digitizing pen for getting the input, the data have noisy points which need to be removed. These are easily identified by their large Euclidean distance from the neighbouring points, or large velocity. In order to remove these noisy points, applying smoothing is necessary in signature verification system. Smoothing may be done by a moving average or using various filters which are equivalent to weighted moving averages.

Extracting local features from noisy point's signature trajectories and then using them for verification may lead to have a system with poor performance.

Hence, smoothing is required for low resolution tablets (Fig.5). Some researchers have used cubic smoothing splines to both interpolate signature data between discrete tablet grid points and smooth the data, and some of them has used a Gaussian filter to smooth the signature. Gaussian filter smooths out small fluctuations in the signal while preserving its overall structure.

The x and the y direction of the signature are smoothed separately.

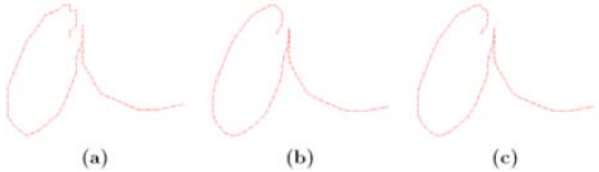


Fig. 5 a) Before smoothing b) After average smoothing c) After Gaussian smoothing [19].

C. Feature Extraction

One of the most significant processes in signature verification is feature extracting. In online signature verification, representation of data is done by sequence of points. So, the features are extracted from a sequence of points (Fig.6). Feature extraction plays an important role through the verification process. However, choosing the related features is still quite an unplanned activity that researchers are still trying to find the best features set [19].

The purpose of the feature extraction module is to enhance the variability which helps to discriminate between classes. Online features includes: pen-up, pen-down, pen coordinates, direction θ and curvature. A binary feature "1" indicates the pen is touching the pad (pen-down) and "0" indicates the pen is not touching the pad (pen-up). The direction of a stroke is determined by a discrete approximation of the first derivative with respect to the arc lengths.

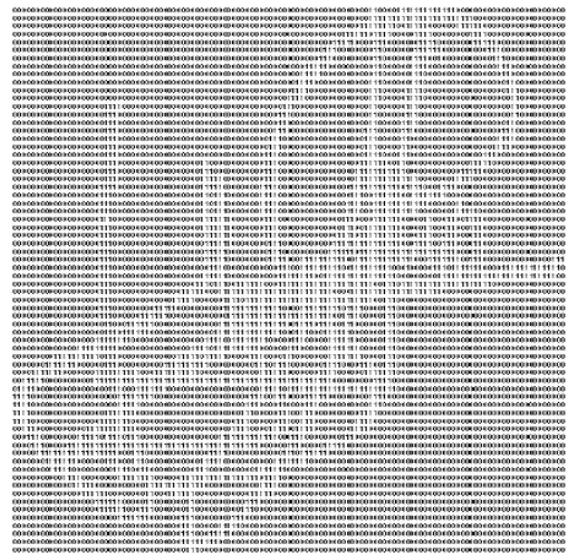


Fig. 6 Example of feature extraction.

D. Feature Matching

Each person has an original shape of signature, but it is a big deal to find two same signatures of a signer. The differentiations of these two signatures are in either shape or dynamic features. From comparing these features, a string will be assembled. These new strings which come from the extracted feature will compare together in order to reach the matching points.

When we compare the curves of two genuine signatures about x or y-axis, the number of their inflexions or the shape of local curves may vary [20].

There are many different proposed algorithms for feature matching. One of the most important algorithms is Dynamic Time Warping. DTW algorithm is a matching technique that is used to align two sequences of different length (Fig.7) [21].

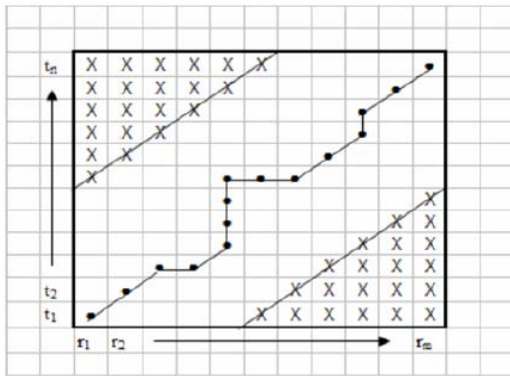


Fig. 7 This figure is the illustration of DTW algorithm which shows the possible warped path [21].

1) Global Features Extraction

Global features are the features related to the signature as a whole; for instance the signing speed, signature bounding box, and Fourier descriptors of the signature's trajectory. Global features provide information about specific cases of the signature shape (TABLE I) [11].

TABLE I
GLOBAL FEATURES FOR COMPARISON

Feature	Description
Average Pressure	The average pen-tip pressure over the entire signature
Pen Tilt	The average tilt of the pen while writing over the entire signature
Average Velocity	The average x, y velocity over all sample points
Number of Pen	Ups The number of times the pen was lifted over the entire signature

2) Local Features Extraction

Correspond to a specific sample point along the trajectory of the signature; examples of local features include distance and curvature change between successive points on the signature trajectory [11].

The computation and matching process of local features require the matching of two different sets of signature data. Nevertheless, extracting global features are more or less easier

than local features, and it has poor discriminative power. More than forty features have been documented until now. But there are still many ways to discover the most reliable feature set for signature verification.

IV. ADVANTAGES, DISADVANTAGE AND LIMITATIONS OF SIGNATURE VERIFICATION

There are several advantages to use signature verification. Some of advantages are (i) It is user-friendly (ii) Well accepted socially and legally (iii) Non-invasive (iv) Already acquired in a number of applications (v) Acquisition hardware include Off-line: ubiquitous (pen and paper) and On-line: inexpensive and already integrated in some devices (Tablet PC) (vi) If compromised, can be changed (vii) Long experience in forensic environments [12].

Signature verification system also suffers some disadvantages and limitations. Some of them are (i) High intra-class variability (ii) Forgeries (iii) Higher error rates than other traits (iv) Affected by the physical and emotional state of the user (v) Large temporal variation [12].

In signature verification, as in many shape recognition domains, it is very difficult to compare the results of different systems.

Also signature verification can be considered as a two-class pattern recognition problem, where the authentic user is a class and all her forgers are the second class. Feature selection refers to the process by which extracted descriptors (features) from the input-domain data are selected in order to provide maximal discrimination capability between classes[22].

V. SIGNATURE VERIFICATION FEATURES

Some of the features involve on signature verification present in TABLE II. TABLE II shows Mathematic formula of each feature.

I. SYSTEM IMPLEMENTATION

The aim of this paper is to investigate about online signature verification and involved features, explain about current methodologies that are used to implement, and state some advantage, disadvantage, and limitation of this system. To show a model of this system, we implemented online signature verification using C++ programming language, and employed twenty features based on TABLE II. The result shows appropriate AER (Accept Error Rate).

II. EXPERIMENTAL RESULT

Various signature verification systems have been implemented so far and many optimized features have been extracted from global and local feature sets, but the selected features that we used in this project have never been tested in the same feature set. In most of the cases, researchers tested their developed system on the database which is created and developed locally by the researchers. In some cases, the implemented system has been tested on skilled forgery to verify the robustness of the system. Whereas in some other cases, random forgeries were used.

For show the test result we combine several features randomly. Fig. 8 shows this combination result. This Figure shows Overall AER of five, six, seven, eight, nine, and ten features combination. The result shows that the best AER is combine five combination. This testing was just for more understanding about effectiveness of features and combination of them.

TABLE II
SET OF SELECTED FEATURES

No .	Features	Mathematic Formula
1	Average speed x	(average speed X)/ k , K is total number of sample point
2	Average speed y	(average speed Y)/ k , K is total number of sample point
3	total velocity	velocity + velocity ($k+i$), K is total number of sample point
4	signature width	Max Y – Min Y
5	signature height	Max X – Min X
6	max pressure	Max (pressure (k))
7	Average acceleration	average + acceleration (k)
8	Speed x	$ x \text{ normalization}_i - x \text{ normalization}_{(i+1)} $
9	Speed y	$ Y \text{ normalization}_i - Y \text{ normalization}_{(i+1)} $
10	pen direction θ	$\tan^{-1} \left(\frac{y(i+1) - y(i)}{x(i+1) - x(i)} \right)$
11	average velocity	$T = t_k - t_i$
12	Total signing duration	$\sqrt{(\text{velocity } x * \text{velocity } x + \text{velocity } Y * \text{velocity } Y)}$
13	Total pen down duration	$td = \sum_{i=0}^{\text{num}} (\text{tendi} - \text{tstarti})$
14	width to height ratio	(Signature width/Height)*100
15	number of strokes	Number of hits by pen in tablet
16	Angle Between Critical point	$\text{Tan}^{-1} * 180/\text{PI}$
17	Altitude	Lt
18	Pen azimuth	$Z t$
19	Pen Down Time Ratio	$\text{tdr} = \text{td}/t$
20	Average Pressure	Average Pressure/ k

VI. CONCLUSIONS

Many researchers have worked on the on-line signature verification and related features. There are several types of methods and algorithms to get the best results. However, the main part of online signature verification is feature extraction. There are numerous extracted features collecting in a set which is called features set.

The future work will be the study on features combination. This future research will show the best combination of features.

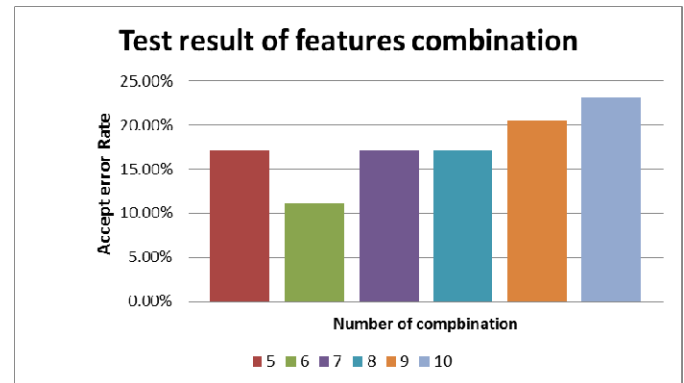


Fig. 8 Test result of feature combination.

REFERENCES

- [1] R. Martens, and L. Claesen, "On-Line Signature Verification by Dynamic Time-Warping", *13th International Conference on Pattern Recognition (ICPR'96)*, Vol.3, pp.38, 1996.
- [2] M. T. Ibrahim, M. Kyan, M. A. Khan, K. S. Alimgeer, and L. Guan, "On-Line Signature Verification: Directional Analysis of a Signature Using Weighted Relative Angle Partitions for Exploitation of Inter-Feature Dependencies", *10th International Conference on Document Analysis and Recognition*, pp. 41 - 45, 2009.
- [3] S. K. Chan, and Y. H. Tay, "Online Signature Verification using Dynamic Time Warping", *Proceedings of Third International Conference on Artificial Intelligence in Engineering and Technology*, pp. 38-42, 2006.
- [4] H. Deng, and Y. Wang, "On-Line Signature Verification Based on Spatio-Temporal Correlation", *Proceedings of the 5th international conference on Emerging intelligent computing technology and applications*, pp. 75-81, 2009.
- [5] T. A. Osman, M. J. Paulik, and M. Krishnan, "An Online Signature Verification System based on Multivariate Autoregressive Modeling and DTW Segmentation", *Signal Processing Applications for Public Security and Forensics, 2007. SAFE '07. IEEE Workshop on*, pp. 1 - 5, 2007.
- [6] M. Khalid, H. Mokayed, R. Yusof, and O. Ono, "Online Signature Verification with Neural Networks Classifier and Fuzzy Inference", *Third Asia International Conference on Modeling & Simulation*, pp. 236 - 241, 2009.
- [7] F. Leclerc, and R. Plamondon, "Automatic signature verification: the state of the art 1989-1993", *International Journal of Pattern Recognition and Artificial Intelligence*, pp. 643-660, 1994.
- [8] R. Plamondon, F. Leclerc, "Automatic signature verification and writer identification the state of the art", *Pattern Recognition*, Vol. 22, No. 2, pp. 107-131, 1989.
- [9] N. M. Herbst, and C. N. Liu, "Automatic Signature Verification Based on Accelerometry", *IBM Journal. Res. Dev.* vol. 22 PP: 245-253
- [10] N. N. Liu, and Y. H. Wang, "Fusion of Global and Local Information for an On-Line Signature Verification System", *Proceedings of the 7th International Conference on Machine Learning and Cybernetics, Kunming*, pp. 12-15, 2008.

- [11] A. A. Kholmatov, "Biometric Identity Verification Using On-Line & Off-Line Signature Verification", Master Thesis, Sabanci University, Spring 2003.
- [12] R. Martens, L. Claesen, "On-Line Signature Verification by Dynamic Time-Warping". *Proceeding in 13th International Conference in Pattern Recognition*, pp: 38, 1996.
- [13] SVC2004: First International Signature Verification Competition", Accessed on 11 December 2007 <<http://www.cs.ust.hk/svc2004/>>.
- [14] M. M. Shafiei, and H. R. Rabiee, "A New On-Line Signature Verification Algorithm Using Variable Length Segmentation and Hidden Markov Models", *7th International Conference on Document Analysis and Recognition*, pp: 443-446, 2003.
- [15] I. T. Jolliffe, "*Principal Component Analysis*", NY: Springer Verlag, 1986.
- [16] A. A. Kholmatov, "Biometric Identity Verification Using On-Line & Off-Line Signature Verification", Master Thesis, Sabanci University, Spring 2003.
- [17] A. .K. Jain, F. D. Griess, and S. D. Connell, "On-line Signature Verification", *Pattern Recognition*, Vol. 35, pp. 2963-2972, 2002.
- [18] L. Wan, and B. Wan, "On-Line Signature Verification with Two-Stage Statistical Models", *8th International Conference on Document Analysis and Recognition*, pp. 282-286, 2005.
- [19] S. M. Watt, and X. Xie, "Prototype Pruning by Feature Extraction for Handwritten Mathematical Symbol Recognition", Master Thesis, University of Western Ontario, London Ontario, CANADA, 2005.
- [20] B. Li, K. Q. Wang, and D. Zhang, "On-line Signature Verification for E-Finance and E-Comemerce Security System", *2nd international Conference on Machine Learning and Cybernetics*, pp. 3002- 3007, 2003.
- [21] S. K. Chan, and Y. H. Tay, "Online Signature Verification using Dynamic Time Warping", *Proceeding in International conference of Artificial Intelligence in Engineering and Technology*, pp: 469-474, 2006.
- [22] R. Martens, L. Claesen, "On-Line Signature Verification by Dynamic Time-Warping". *Proceeding in 13th International Conference in Pattern Recognition*, pp: 38, 1996.