International Journal of Engineering Research and General Science Volume 3, Issue 4, July-August, 2015
ISSN 2091-2730

Online Signature Verification Techniques: A Survey

Aswathy K. V.
M.tech Scholar, Dept. of CSE, Sree Buddha College of Engg. For Women,
Pathanamthitta, Kerala, INDIA
aswathy.kv24@gmail.com

Abstract— Signature is one of the accepted biometric traits for the identification. Like any other biometric features, the signature is unique to everyone. Many of the fields that need authentication use the signature as an identity. So many technologies have been emerging in this field. Handwritten signatures made by each person can have various features. These characteristics cannot be reproduced by any other person as such, even though there may be some structural similarities visible. Depending on the type of characteristics that we are considering, the signatures are of online and offline. Most of the studies show that the online systems are working more effectively than offline systems since the former use an input device to acquire some additional features, commonly refer dynamic features. This paper goes through various research works implemented in the online signature verification so far.

Keywords— Online signature, Dynamic Time Warping, Hidden Markov Model, Feature extraction, Preprocessing

INTRODUCTION

Handwritten signature is invasively used for person's identity verification. It is a behavioral biometric trait of users. It cannot be similar for everyone. The people even having identical names will have different signatures. This uniqueness of the signature is taken as an advantage for many fields to recognize the person. The signature verification has applications in fields such as banking, insurance, healthcare, ID security, document management, e-commerce, and retail point-of-sale.

The signature verification systems can be mainly classified into offline and online systems. The offline systems use image of the signature and require the static features of the signature for verification. So there will be a chance of misusing such signatures by the forger who get the images of genuine one. On the other hand, the online signatures are those which have dynamic features for verification and are more reliable than offline. It can provide more accurate results than offline.

Online signature verification system comprises of two stages: (i) Enrollment stage and (ii) Verification stage. In the former stage, the user is enrolled in the system by drawing multiple online signatures from which a user template will be constructed for verification and in the latter stage, the user claims its identity by inputting a signature using devices such as tablets, mobile devices etc. and the system accepts the signature only if the distance between the enrolled template and the newly input one is less than a predefined threshold.

The researches in the online signature verification so far followed two basic approaches, function-based and feature-based or parametric. In the function-based approach, the time series data points describing the local properties of the signature are used for the signature verification, e.g.: position trajectory, velocity, acceleration, force or pressure. These approaches can produce better results. But many recent works have been focused on the feature-based approach, where the descriptive features of the signature are used for verification. The function-based is again classified into local and regional approaches. The technique of Dynamic Time Warping (DTW) and the Hidden Markov Models (HMM) are belonging to the local and regional approaches respectively. Most of the works used the MCYT-100 and SUSIG databases for the verification.

The online signature verification system passes through the following phases: (i) Data acquisition and preprocessing (ii) feature extraction and (iii) verification. The rest of this paper explains these phases.

PHASES OF SIGNATURE VERIFICATION

A. DATA ACQUISITION AND PREPROCESSING

The data collection is done either using a digitizing tablet or a touch interfaced based technologies provided on PDA, Tablet PCs and smart phones. The most traditional online data acquisition devices are the digitizing tablets. It is not quite easy to being natural. Inputting online signatures through digitizers is done under a controlled environment. This restriction may lead to so many inconveniences for users. Electronic pens with touch-sensitive screens and digital-ink technologies that avoid signer disorientation by providing immediate feedback to the writer are good examples of such efforts. Using electronic pens is another technology that are capable of detecting position, velocity, acceleration, pressure, pen inclination, and writing forces, with the use of strain gauges,

magneto elastic sensors, shift of resonance frequency, and laser diodes. Some input devices use ink pen, which is exactly like using a conventional pen on standard paper positioned on the tablet. In this case, the pen produces conventional handwriting using ink, while producing an exact electronic replica of the actual handwriting. Recently, a stylus-based device that captures a series of snapshots of writing by using a small charge-coupled device camera has been proposed. This stylus has a stress sensor for detecting the pressure applied on the ball point and can determine pen-up/pen-down information. Most recently touch screen smart phones [9] have been used as the signature acquisition device since it is easily available and its nature of providing uncontrolled environment. The users can input their signatures bringing the phone at any convenient position.

Fig.1: A traditional signature and an online signature

Preprocessing of online signatures is commonly done to remove variations that are thought to be irrelevant to the verification performance. Resampling, size, and rotation normalization are among the common preprocessing steps. In the preprocessing phase, the signature is undergone some enhancement process for extracting features. For offline signatures, typical preprocessing algorithms are concerned about signature extraction, noise removal by using filters, signature size normalization, binarization, thinning and smearing. Using offline signatures in fields such as banking is an open challenge to do the verification since some other properties have to be considered. For online signatures, some important preprocessing algorithms are filtering, noise reduction, and smoothing.

Berrin yanikoglu et al [1] proposed an online signature verification using Fourier descriptors. In this work, they have done the preprocessing in two steps that are pen-up durations, and drift and mean removal. Napa Sae-Bae et al[9] has been done preprocessing by time normalization and stroke concatenation before feature extraction.

B. FEATURE EXTRACTION

The features extracted from an online signature can be categorized into two: function features and parameter features. The function features are represented in terms of a time function and parameter features are represented as a vector of elements. The parameter features are again divided into two: local features and global features. The local features are those extracted from each sample point of the input signature. These features can be classified into component-oriented features, which are extracted at the level of each component, for example, height-to-width ratio of the stroke, relative positions of the stroke, stroke orientation, etc. and pixel-oriented features, which are extracted at the pixel level, for example, grid-based information, pixel density, gray-level intensity, texture, etc. The global features are concerned about the whole signature. These features are derived from the signature trajectories. Typical global features are the total time taken to write a signature, number of pen-ups, the orientation of the signature, the number of components of the signature, etc. The global features are extracted in the feature-based approach and local features are extracted in the function-based approach of the online signature verification.

Loris Nanni et al [2] extracted the global information with a feature-based representation and recognized by using an ensemble of classifiers in their work featuring multi-matcher method of online signature verification. They show that this new method outperforms the existing methods which are highly dependent on hashing threshold. The use of ensemble of classifiers makes them independent. D.S. Guru and H.N. Prakash [3] proposed an online signature verification and recognition system based on the symbolic representation of the signature, which is a feature-based approach where the global features are expressed in the form of interval-valued data. Also they have provided the concept of write-dependent threshold and feature-dependent threshold leading to outperform other global feature-based systems. Alisher Kholmatov et al [4], on their studies, uses three local features such as x–y coordinates relative to the first point of signature trajectory, the x and y coordinate differences between two consecutive points, and the curvature

differences between two consecutive points. They didn't use the pressure information as a local feature because, according to them this feature is not useful for discriminating the genuine and the forgery signatures. Napa Sae-Bae et al[9] used histogram based feature sets to represent the online signatures.

C. VERIFICATION

There are mainly two techniques for verification in the function-based approach, DTW and HMM. DTW is a method that calculates an optimal match between two given sequences with certain restrictions. This method takes a signature sample as input and aligns it non-linearly with respect to the stored reference signature. However it gives better performance and accuracy, it has some drawbacks such as heavy computational load and warping of forgeries. With the presence of forgeries, forged signals also undergo DTW to be trimmed, so as to be more authentic. So many works has been implemented the verification techniques either by an extended form of DTW or the combination of DTW and some other techniques. Some works have been implemented in the DWT (Discrete Wavelet Transform) domain. This method shows high rate of verification.

Hao Feng et al [5] proposed a new warping technique known as extreme points warping (EPW) to overcome the drawbacks found in DTW. They proved that this new method is more adaptive in the field of signature verification than DTW, given the presence of forgeries. DTW does the warping of the whole signal, but EPW warps a set of selected points. The new method usually selects peak and valley points and computes a rise-distance and drop-distance. Then check whether both the distances are greater than or equal to a threshold, which is a pixel value. This follows a matching process and a segment warping process and thus achieves the warping of the whole signal.

Hidden Markov model (HMM) is another widely used pattern recognition approach. It is a popular statistical tool for modeling a wide range of time series data. HMMs are extended finite state machines. It consists of two states: hidden and observable states. The sequence of hidden states produces an observed state. This concept of HMM can be applied in the online signature verification also as a functional approach. Julian Fierrez et al [6] have proposed HMM-based online signature verification where they got the best configuration when two HMM states are used.

Loris Nanni et al [7] have done another study to protect the signature template where they used both DTW and HMM for the matching purposes and also used a linear programming descriptor classifier which is trained by using global features. Maged M.M. Fahmy [10] used DWT (Discrete Wavelet Transform) to find out the difference between genuine signature and its forgery, along with which neural network classification was implemented.

SIGNATURE TEMPLATE SECURITY

The biometric template protection is a major concern among the researchers since the attacks against the biometric traits are challenging for the users to prevent them from disclosing their identity. Other authorization mechanisms such as using passwords cannot reveal a person's identity, but biometric traits can do it and the misuse of which lead to the privacy loss of a person.

Many research works have been blooming to solve the problem of privacy and/or security of biometric templates. Emanuele Maiorana et al [8] have introduced a novel non-invertible transformation-based approach known BioConvolving which can provide both security and renewability of any kind of biometric including signature. A combination of two template protection techniques known as BioHashing and BioConvolving has been discussed in [7] in which they claimed that both the techniques can provide the security favourably in some extend.

ACKNOWLEDGMENT

This work has not been completed unless I wish my thanks to those who helped me. I take this opportunity to convey my gratitude to our respected Principal and HOD for their support and a special thanks to Dr. Jayamohan sir for his valuable suggestions and guidance throughout this work.

CONCLUSION

This paper has made a review work based on the technologies developed in online signature verification. While going through these technological advancements, it is realized about the widespread recognition of the signature and its applications over various fields. Being significant, it has many challenges over its security. So recent works have mainly focused on the signature template protection. Also varying input devices for enrolling signatures is another developing area in this field. The sample signatures to experiment the research works are now obtained from various signature databases such as MCYT-100, SUSIG, etc. So the novice research scholars will not have any difficulty of getting sample training sets. Thus signature-based authentication has now become a demanding research area.

REFERENCES:

[1] B. Yanikoglu, and A. Kholmatov, "Online signature verification using Fourier descriptors," EURASIP J. Adv. Signal Process., vol. 1, p.260516, Jan. 2009.
[2] L. Nanni, "An advanced multi-matcher method for online signature verification featuring global features and tokenized random numbers", Neurocomputing, vol. 69, nos. 16-18, pp. 2402-2406, 2006.
[3] D. Guru and H. Prakash, "Online signature verification and recognition:An approach based on symbolic representation", IEEE trans. Patten Anal. Mach. Intell., vol. 31, no. 6, pp. 1059-1073, Jun. 2009.
[4] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method", Pattern recognit. Lett., vol. 26, pp. 2400-2408, Nov. 2005.
[5] H. Feng and C.C. Wah, "Online signature verification using a new extreme point warping technique", Pattern recognit. Lett., vol. 24, no. 16, pp. 2943-2951, 2003.
[6] J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, "HMM-based on-line signature verification: Feature extraction and signature modeling", Pattern Recognit. Lett., vol. 28, pp. 2325-2334, Dec. 2007.
[7] L. Nanni, E. Maiorana, A. Lumini, and P. Campisi, "Combining local, regional and global matchers for a template protected on-line signature verification system," Expert Syst. Appl., vol. 37, pp. 3676-3684, May 2010.
[8] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition," IEEE Trans. Syst., Man, Cybern. A, Syst.,Humans, vol. 40, no. 3, pp. 525-538, May 2010.
[9] Napa Sae-Bae and Nasir Memon,"Online Signature Verification on Mobile Devices", IEEE trans. on information forensics and security, vol. 9, no. 6, june 2014.
[10] Maged M.M. Fahmy, "Online handwritten signature verification system based on DWT features extraction and neural network classification", Ain Shams Engineering Journal (2010) 1, 59-70.