Smart Security System Based Online Signature Verification

Manju Davis, Meenu K. Benny, Nithin Jose, Shemimol. K. Shaji

Department of Electronics and Communication, Nirmala College of Engineering, Calicut University, Kerala, India

ABSTRACT

This paper studies online signature verification on touch interface-based mobile devices. A simple and effective method for signature verification is developed. An online signature is represented with a discriminative feature vector derived from attributes of several histograms that can be computed in linear time. The resulting signature template is compact and requires constant space. The algorithm was first tested on the well-known MCYT-100 and SUSIG data sets. The results show that the performance of the proposed technique is comparable and often superior to state-of-the-art algorithms despite its simplicity and efficiency. In order to test the proposed method on finger drawn signatures on touch devices, a data set was collected from an uncontrolled environment and over multiple sessions. Experimental results on this data set confirm the effectiveness of the proposed algorithm in mobile settings. The results demonstrate the problem of within-user variation of signatures across multiple sessions and the effectiveness of cross session training strategies to alleviate these problems

Keywords: MCYT-100, SUSIG, Qu

I. INTRODUCTION

A handwritten signature is a socially and legally accept biometric trait for authenticating an individual. Typically, 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 associated attributes like pressure, time, etc., are also acquired. As a result, an online signature verification system usually achieves better accuracy than an off-line system The increasing number of personal computing devices that come equipped with a touch sensitive interface and the difficulty of entering a password on such devices have led to an interest in developing alternative authentication mechanisms on them In this context, an online signature is a plausible candidate given the familiarity users have with the concept of using a signature for the purpose of authentication. However, none of this has been directed to the context of authentication on mobile devices.. First, on mobile devices, a user performs his signatures in various contexts, i.e., sitting or standing, mobile or immobile, and holding a device at different angles and orientations. Secondly, availability of computational resources may differ from one.

This paper proposes an online signature verification algorithm that is suitable to deploy on mobile devices. It is a computationally and space efficient algorithm for enrolling and verifying signatures. In addition, a signature template is stored in an irreversible form thereby providing privacy protection to an original online signature. The proposed method was evaluated on public datasets as well as new dataset collected in in uncontrolled setting from user owned mobile devices. The verification performance obtained is promising. The key contributions made by this paper are as follows:

1) A method to extract a model-free non-invertible feature set from an online signature is proposed. The feature set comprises of sets of histograms that capture distributions of attributes generated from raw signature data sequences and their combinations. By evaluating the proposed method on

public datasets, its verification performance is superior to several state of the art algorithms.

2) By applying the proposed method on the above dataset, the following aspects of online signature verification on mobile devices were investigated: impact of template aging on online signatures, effectiveness of using cross-session samples, or samples from multiple sessions, to train a classifier, and security of the system against random forgery, or zero effort.

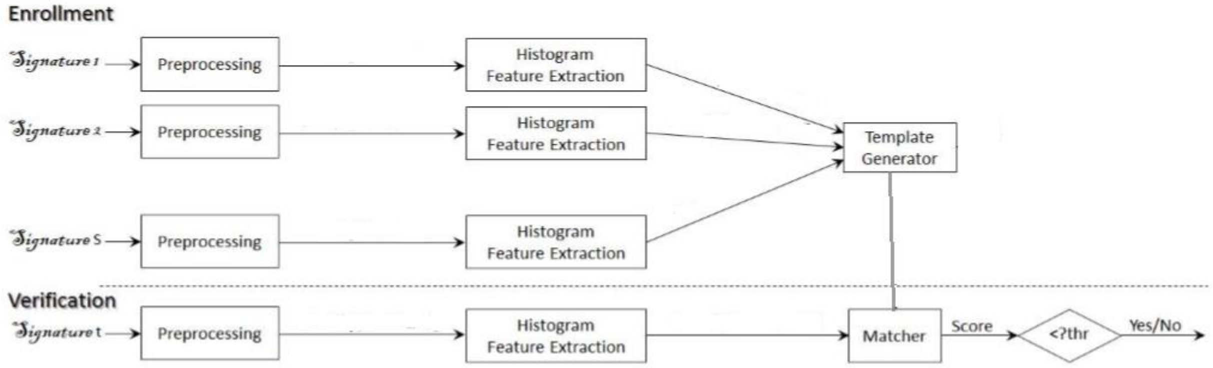

Figure 1. The proposed online signature verification system

II. II.ONLINE SIGNATURE VERIFICATION ALGORITHM

The proposed system comprises of three main components: a feature extractor, a template generator, and a matcher. First, an online signature is processed by the feature extractor in order to compute a set of histograms from which a feature vector is derived. Then, the template generator constructs a user-specific template using the feature sets derived from multiple enrolled signatures. This template is later used by the matcher to verify a test signature.

A. Feature extractor

In the proposed system, an online signature is represented by a set of histograms. These histogram features are designed to capture essential attributes of the signature as well as relationships between these attributes. It should be noted that histogram share widely used as a feature set to capture attribute statistics in many recognition tasks. The feature extraction process of the proposed system begins by converting the time-series data of a signature in to a sequence of cartesian vectors and attributes, as well as their derivatives.

B. User template generator

A user template is generated during the enrolment process where multiple signatures are acquired from a user and a feature set is computed from each of the samples. Then, the variance of each feature component is computed and is used to construct a user-specific uniform quantizer for each feature element resulting in a quantization step size vector Qu that is used to quantize each of the feature vectors derived from the enrollment samples. Finally, the average of these quantized feature vectors is used as the template □Fu for that user

C. Matcher

During verification, given that t is claimed to be an online signature sample from user u, ˆ F(t|u) is calculated using Qu.

III. RESULTS AND DISCUSSION

Impact of Signature Aging and Effectiveness of Cross-Session Training Strategy: The objective of collecting the dataset over six separate sessions was to study template aging issues in online signatures, as well as to study whether training samples from multiple sessions can better represent within-user variation thereby enhancing verification performance. In this context, first the performance of online signature verification when training and test samples are drawn from the same session is reported. Note that the results are the average performance from leave-one-out cross validation test. That is, the classifier is trained from all the samples from the same users but one, and each and every sample is used as a positive sample exactly once.

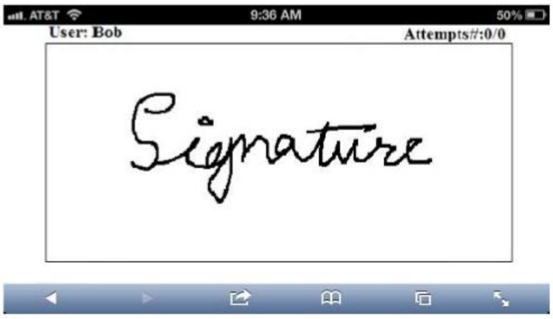

Figure 2. An example of finger drawn signatures on mobile devices

IV. CONCLUSION

This paper proposes a simple and effective online signature verification system that is suitable for user authentication on a mobile device. The benefits of the proposed algorithm are as follows First, a histogram based feature set for representing an online signature can be derived in linear time and the system requires a small and fixed-size space to store the signature template. In addition, since the feature set represents only statistics about distribution of original online signature attributes, the transformation is non-invertible. As a result, the privacy of the original biometric data is well-protected. Second, a user-specific classifier comprising of a user-specific quantization step size vector and its associated quantized feature vector can be trained using only enrolment samples from that user without requiring a training set from a large number of users. A new dataset was collected for evaluating system performance of user authentication on a mobile device. Signatures in this dataset were drawn using a fingertip in an uncontrolled setting on user owned iOS devices over six separate sessions.. In addition, it is currently possible to match different signature templates generated from the same online signature samples and thereby learn that two leaked biometric templates belong to the same user. Further investigation includes the use of other biometric key binding approaches, like fuzzy commitment, in order to strengthen security of the system, even when stored templates, helper data etc., are compromised, while preserving verification performance.

V. REFERENCES

[1]. A. Fallah, M. Jamaati, and A. Soleamani, "A new online signature verification system based on combining Mellin transform, MFCC and neural network," Digital Signal Process., vol. 21, no. 2, pp. 404-416, 2011.

[2]. L. Findlater, J. O. Wobbrock, and D. Wigdor, "Typing on flat glass: Examining ten-finger expert typing patterns on touch surfaces," in Proc. Annu. Conf. Human Factors Comput. Syst., New York, NY, USA, 2011, pp. 2453-2462.

[3]. N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: A novel approach to authentication on multi-touch devices," in Proc. CHI, 2012, pp. 977-986.

[4]. N. Sae-Bae, N. Memon, K. Isbister, and K. Ahmed, "Multitouch gesturebased authentication," IEEE Trans. Inf. Forensics Security, vol. 9, no. 4, pp. 568-582, Apr. 2014.

[5]. L. G. Plamondon and R. Plamondon, "Automatic signature verification and writer identification—The state of the art," Pattern Recognit., vol. 22, no. 2, pp. 107-131, 1989.

[6]. H. Feng and C. C. Wah, "Online signature verification using a new extreme points warping technique," Pattern Recognit. Lett., vol. 24, no. 16, pp. 2943-2951, 2003.

[7]. A. Kholmatov and B. Yanikoglu, "SUSIG: An on-line signature database, associated protocols and benchmark results," Pattern Anal. Appl., vol. 12, no. 3, pp. 227-236, 2008.

[8]. J. Ortega-Garcia et al., "MCYT baseline corpus: A bimodal biometric database," IEE Proc. Vis. Image Signal Process., vol. 150, no. 6, pp. 395-401, Dec. 2003.

[9]. L. Nanni, "An advanced multi-matcher method for on-line signature verification featuring global features and tokenised random numbers," Neurocomputing, vol. 69, nos. 16-18, pp. 2402-2406, 2006.

[10]. D. Guru and H. Prakash, "Online signature verification and recognition: An approach based on symbolic representation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 31, no. 6, pp. 1059-1073, Jun. 2009.