.

Online Signature Verification on Mobile Device

1.Raut Akshay S., Information Technology, PREC Loni, Maharashtra, India
2. Pawar Hitesh G., Information Technology, PREC Loni, Maharashtra, India
3. Pandita Akshay ., Information Technology, PREC Loni, Maharashtra, India

ABSTRACT

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

Keywords: *Attribute, Datasets, Signature*.

---

1. INTRODUCTION

A handwritten signature is a socially and legally accepted biometric trait for authenticating an individual. Basically, 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 entities like pressure, time, etc., are also the 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 and an online signature is a plausible candidate given the familiarity users have with the concept of using a signature for the intent of authentication. There has been much work on online signature verification systems. However, none of this has been directed to the authentication on mobile devices. Old work has addressed online signatures acquired from traditional digitizers in a controlled environment.

These are different from those acquired from mobile devices in dynamic environments. First, on mobile devices and 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.

2.SIGNATURE VERIFICATION ALGORITHM

As illustrated in Figure 2, the proposed system comprises of three main components such as a feature extractor, a template generator and a matcher. An online signature is processed by the feature extractor in order to compute a set of histograms from which a feature vector is derived and 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. The rest of this section describes these three components in detail and analyzes system complexity. (For more details, please refer to for the earlier version of this work.)

2.1. Feature extractor

In the proposed system, an online signature is represented by a set of histograms and these histogram features are designed to capture essential attributes of the signature as well as relationships between these attributes. It should be noted that histograms are widely used as a feature set to capture attribute statistics in many recognition tasks. For instance, in object recognition and off-line signature verification. Using histograms for online signature verification was first suggested by Nelson et al. They have also been used as part of the feature set in. However, in and, the use of histograms is limited only to angles derived from vectors connecting two consecutive points in an online signature. In fact, as is shown below, much more information can be used to derive histograms useful in online signature verification. These include x-y trajectories, speed, angles, pressure.

2.2. User template generator

A user template is generated during the enrollment 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 quantized for each feature element resulting in a quantization step size vector *Quid* 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 $F \cdot \cdot u$ for that user and this feature vector along with the quantization step size vector are stored corresponding to the identity of the user derivatives. 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. Then, each Cartesian vector is also converted to a vector in the sequences are derived.

2.3. Matcher

During verification, given that t is claimed to be an online signature sample from user u, $\hat{F}\,(t|u)$ is calculated using Qu. Then the system derives the dissimilarity score using Manhattan distance between $F \cdot u$ and $\hat{F}\,(t|u)$ as, *Score* =

M X

$i=1|\hat{f}(t|ui - f \cdot ui|$

The system then accepts the sample t if the different score is less than a predefined threshold, other hand it rejects.

3. EXPERIMENTS ON MOBILE DEVICE DATASET

3.1.Data Collection Procedure

The process for data collection began by recruiting users from a departmental mailing list by sending a brief description of the experiment and offering a $10 dollar gift card to those who participate. Users who volunteered, were asked to create an online account with an email address, username and password on a webpage. The system then immediately took them to an introduction page that briefly described the purpose of the experiment and the procedure they would be expected to follow. An example signature was provided but no other instruction was given on the type of signature they should create. However, they were motivated to provide quality signatures by rewarding the top ten users with the most consistent samples over the entire experiment with an additional $40 gift card. Then the user was asked to create a signature and draw it five times on the screen. Visual feedback was provided so the user could see the signature they drew. All signatures were performed on the users' personal devices. An experimental protocol was designed to capture time variation effects in user signature input over the course of approximately seven days. After the first session, multiple sessions of data collection were performed where a user entered his signature 5 times for each session. At the end of each session, the screen was locked and the user was instructed to wait for a time period after which a reminder to perform the next session would be sent to his email address. The minimum time interval between each of the sessions and its immediate successor was twelve hours for the first and second, the second and third, and the third and fourth sessions. The minimum time intervals imposed between the fourth and the fifth and between the fifth and the last session were 96 hours and 24 hours respectively. The time intervals between sessions were chosen to introduce variation in times of the day when the signatures were performed and hence the context they would be performed under. During the experiment, if a user forgot his signature, he was provided with two options. First, he could reset the account and redo the process from the beginning. Second, he could click the "forgotten" button and the system would show his previous signature on the screen. In this case, he would be prompted to clear the screen before he could enter his new signature. This was to prevent a user from tracing his own signature there by increasing consistency artificially.

3.2.Signature Characteristics

This subsection provides some features of signatures that were collected. These characteristics included the length the number of strokes in the signature. A stroke in this study is the defined as a sequence of touch points starting from touch-down event to the next touchup event. Figure 5 shows the distribution of signature lengths, the distribution of signature strokes as well as the distribution of the number of signature strokes are difference between the same user. Different signatures were also comprised of the various numbers of strokes. Generally, the number of strokes can be influenced by the language and writing styles of users. In the addition it can also be caused by irregularity of interaction between the hardware sensor and the input device (fingertips in this case.) In this experiment, the users were recruited from the mailing list of a university where English is mostly used as the first language. Nevertheless, the variation in the number of strokes from user to user is noticeable. On an average, a signature had 3.38 strokes with a standard deviation of 2.28. In addition, we observed that the number of strokes were often not consistent even within the same user. On average, the number of strokes varied by 3.5 over the entire set of 30 samples taken from the same user.

***3.4. Signature* Preprocessing**

The fluctuation in the number of strokes per signature and Sampling rates are introduced in the dataset can be affect verification performance. Hence, all signatures were pre-processed by time normalization and stroke concatenation before extracting histogram features. Details of the time normalization and stroke concatenation steps used are as follows.

3.4.1. Time normalization:

When a signature is the acquired from basically touch sensitive computing devices (iOS device in this case), it is typically sampled with non-uniform rate and its the rate depends on the accessibility of computational resources at a given time and the latency of network connection. Therefore, time normalization was used in order to derive a uniformly sampled signature. This helped to minimize the variation of signatures due to different sampling rates. The process used was as follows. Let $S = \{v1, v2, v3 \; ...vN \}$ be an online signature with the sequence of N strokes where each stroke $vi = \{(x\, i1, yi1), ..., (x\, I\, M , yiM)\}$ is a sequence of touch points $(x\, j , yj)$ sampling at time $T = \{t\, I$ $1, ..., ti\, M \}$. The normalized stroke si was computed by interpolating the stroke vi at $T = \{t\, I\, 1, ti\, 1 +R, t\, i1 + 2R, ...,$ $t1i +bt\, I\, M −t\, 1\, cR ×R\}$. An example of a normalized stroke is depicted in Figure 6. After the process, all time-normalized signatures have a fixed sampling rate of 50 times per second or 20 milliseconds apart.

3.5. Signature stroke concatenation

Most of the signatures in this dataset have many strokes. Signatures with the many strokes may pose a challenge to verification algorithms by the introducing positional variation for each of the strokes. This variation could become larger when the signatures are signed on touch devices using a fingertip since each touch point may not coincide with user's intention. In order to cope with this variation, signature strokes were concatenated before verification as follows. Let $S = \{s1, s2, s3,..sN\}$ be an online signature with a sequence of normalized strokes where each stroke $si = \{(x\ I\ 1,\ yi1), ..., (x\ I\ M\ ,\ yiM\ )\}$ is a sequence of touch points $(x\ j\ ,\ yj\ )$ with length M . The immediately succeeding stroke is concatenated to the main stroke by translating the origin of the latter stroke to the end of the former stroke.

In this subsection we present experimental results using the data collection procedure as well as the pre-processing techniques described above. The algorithm used is the same as the one described in section 2, except two key differences. The histograms related to the pressure information were discarded as they were not available in this dataset. The additional histograms from Table V are empirically added as they provide.

4. CONCLUSION

This paper proposes a simple and effective online signature verification system that is suitable for user authentication on a mobile device. As a result, the privacy of the original biometric data is well-protected.its associated quantized feature vector can be trained using only enrollment samples from that user without requiring a training set from a large number of users.

5. REFERENCES

[1] A. Fall ah, M. Jamaati, and A. Soleamani, "A new online signature verification system based on combining mellin transform, mfcc and neuralnetwork," DSP, vol. 21, no. 2, pp. 404 – 416, 2011.

[2] L. Findlater, J. O. Wobbrock, and D. Wigdor, "Typing on flat glass: examiningten-finger expert typing patterns on touch surfaces," in Proceedings of the 2011 annual conference on Human factors in computing systems, CHI '11, (New York, NY, USA), pp. 2453–2462, ACM, 2011.

[3] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: a novel approach to authentication on multi-touch devices," in CHI '12, (New York, NY, USA), pp. 977–986, ACM, 2012.

[4] L. G. Plamondon, R., "Automatic signature verification and writer identification the state of the art," Pattern Recognition, vol. 22, no. 2, pp. 107– 131, 1989. cited By (since 1996) 342.

[5] M. Faundez-Zanuy, "On-line signature recognition based on vq-dtw," Pattern Recognition, vol. 40, no. 3, pp. 981 – 992, 2007.

[6] H. Feng and C. C. Wah, "Online signature verification using a new extreme points warping technique," Pattern Recognition Letters, vol. 24, no. 16,