Sixth International Conference on Emerging trends in Engineering and Technology (ICETET'16)
www.ijera.com
ISSN: 2248-9622, pp.20-27

RESEARCH ARTICLE OPEN ACCESS

An Efficient on-Line Signature Verification System Using Histogram Features

Mr.Abilash S[1], Mrs.M.Janani, M.E[2]
ME Computer Science and Engineering,Department of CSE, Annai Vailankanni College of Engineering
Assistant Professor,Department of CSE, Annai Vailankanni College of Engineering

Abstract: The increasing number of personal computing devices that come equipped with a touch sensitive interface. The difficulties of entering a password on such devices have led to an interest in developing alternative authentication mechanism on them. A handwritten signature is a socially and legally accepted biometric trait for authenticating an individual. In online handwritten signature verification system a sequence are acquired. This paper proposes the online signature verification method. An online signature authentication is the much needed authentication scheme. The enrollment time three sample signatures query signature are acquired from the user. The query signature histogram and crossing number information is formed and matched with the template data using Euclidian distance method. Each signature is pre-processed to make the connections in the signature. Then x difference, y difference, angle and speed features are extracted from the online signature. The junction points are computed using crossing number method for each histogram and the template junction points are computed and stored. Experimental result shows the effectiveness of the proposed algorithm than the existing methods.

***Keywords*:** Online signature, template aging, performance evaluation

I. INTRODUCTION

A handwritten signature is an efficient method in an off-line system, just an image of the user’s signature is acquired without additional attributes. 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. There has been much work on online signature verification systems. However, none of this has been directed to the context of authentication on mobile devices.

Signature verification can be divided into two main areas depending on the data acquisition method: off-line and on-line signature verification. In off-line signature verification, the signature is available on a document which is scanned to obtain its digital image representation. On-line signature verification uses special hardware, such as a digitizing tablet or a pressure sensitive pen, to record the pen movements during writing. In addition to shape, the dynamics of writing are also captured in on-line signatures, which is not present in the 2-D representation of the signature.

Signature verification can be used in all applications where handwritten signatures are currently collected such as cashing a check, signing a credit card transaction or authenticating a legal document. The ability to capture the signature and have it immediately available in a digital form for verification also opens up a range of new application areas. Basically, any system that uses a password or PIN can instead use an on-line signature for access. These include file and device access or secure physical entry systems.

Authentication is the process of determining if a user or identity is who they claim to be. Authentication is accomplished using something the user knows (e.g. password), something the user has (e.g. security token) or something of the user (e.g. biometric). The authentication process is based on a measure of risk. High risk systems, applications and information require different forms of authentication that more accurately confirm the user's digital identity as being who they claim to be than would a low risk application, where the confirmation of the digital identity is not as important from a risk perspective.

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

- Security of the system against random forgery, or zero-effort attack and its comparison to that of 4-digit PIN.

Where password-only authentication is not adequate for an application, a number of alternative methods can be used alone or in combination to increase the security of the authentication process. The three generally accepted methods for verifying the identity of a user are based on something the user knows, such as a password; something the user possesses, such as an authentication token; and some physical characteristic of the user, such as a fingerprint or voice pattern. A variety of methods are available for performing authentication.

II Related Work

The multitouch gestures for user authentication on touch sensitive devices [8] a canonical set of 22 multitouch gestures was defined using characteristics of hand and finger movement. Then, a multitouch gesture matching algorithm robust to orientation and translation was developed. Two different studies were performed to evaluate the concept. First, a single session experiment was performed in order to explore feasibility of multitouch gestures for user authentication. Second, a study involving a three-session experiment was performed. The signature verification and recognition [6] based on the symbolic representation are also proposed. The notions of writer-dependent threshold and introduce the concept of feature-dependent threshold to achieve a significant reduction in equal error rate. An online signature is a behavioral biometric used for personal authentication to complete automated transactions, gaining control of computing facilities or physical entry to protected areas. The term periocular biometric in the visible spectrum [5] refers to the facial region in the immediate vicinity of the eye. Acquisition of the periocular biometric is expected to require less subject cooperation while permitting a larger depth of field compared to traditional ocular biometric traits (viz., iris, retina, and sclera). The feasibility of using the periocular region as a biometric trait. Global and local information are extracted from the periocular region using texture and point operators resulting in a feature set for representing and matching this region. The online handwriting instead of handwritten images for registration [2] The online registrations enable robust recovery of the writing trajectory from an input offline signature and thus allow effective shape matching between registration and verification signatures. Signature is a socially accepted authentication method and is widely used as proof of identity in our daily life. Automatic signature verification by computers has received extensive research interests in the field of pattern recognition. Depending on the format of input information, automatic signature verification can be classified into two categories: online signature verification and offline signature verification. To develop a new verification criterion this combines the duration and amplitude variances of handwriting. The approach that uses online signatures in the registration phase. To develop this approach based on the observation that registration needs to be done only once, it has to be done in person in-situ (such as in a bank) where an online device is easily available. In the verification phase, the procedure is exactly the same as an offline system thus is convenient to use.

III. PROPOSED WORK

The increasing number of personal computing devices that come equipped with a touch sensitive interface meets a problem with authentication. For mobile devices the high successful and practical authentication method is handwritten online signature authentication scheme. In this context an online signature is a possible candidate given the familiarity users have with the concept of using a signature for the purpose of authentication. The signature verification process is still an unsolved problem and none of these have been directed to the context of on mobile devices. Previous 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, 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 signature instance to another and it could result in greater variation of input resolution when compared to that of stand-alone acquisition devices. Signatures on mobile devices are often drawn using a finger instead of a stylus resulting in less precise signals. So a new method which supports online signature verification on mobile devices is urgently required one.

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. The rest of this section describes these three components in detail and analyzes system complexity.

This paper is online signature verification on mobile devices. From the enrollment sample signature a template signature information should be generated. The query signature feature information should be matched with the template information and to provide the authentication status. The crossing number based junction point should increase the performance rate. The proposed method should given the high accuracy for online

signature verification

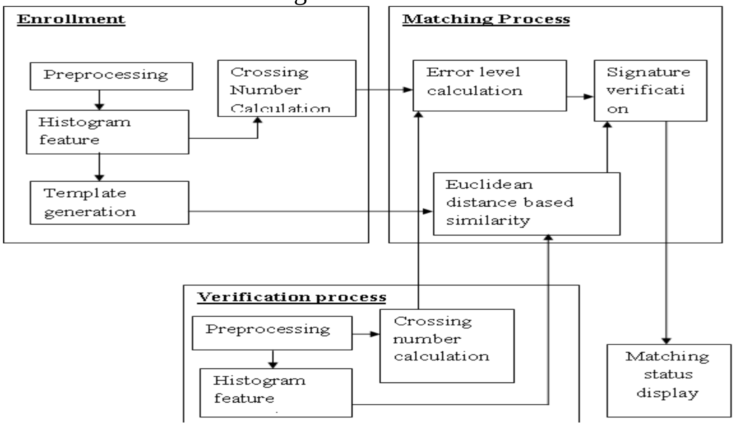


Figure 3.1 System architecture of on-line signature verification

Figure 3.1 illustrates the system architecture of on-line signature verification. These are different from those acquired from mobile devices in dynamic environments. 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 signature instance to another and it could result in greater variation of input resolution when compared to that of stand-alone acquisition devices. Last, signatures on mobile devices are often drawn using a finger instead of a stylus resulting in less precise signals.

Figure 3.2 Finger drawn signatures

An example of finger drawn signatures acquired from mobile devices is depicted in Figure3.2. Consequently, verification performance derived from traditional datasets, collected using stylus-based devices in a controlled environment, and may not carry over to online signature verification on mobile device setting. The proposed work is mainly divided into three major steps namely, Enrollment process, Verification process and Matching process

a) Enrollment Process

The variation in the number of strokes per signature and sampling rate introduced in the dataset can affect verification performance. Hence, all signatures were pre-processed by stroke concatenation before extracting histogram features. Signatures with multiple strokes may pose a challenge to verification algorithms by 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. The pre-processing stage improves quality of the image and makes it suitable for feature extraction.

b) Verification Process

During verification, a user claiming an identity u is asked to produce one instance of an online signature which is again represented by the set of features. The signature is accepted if the Euclidian distance between these two vectors is less than a predefined threshold, otherwise it is rejected. Let S be the total number of enrolled samples and M be the total number of features for each sample. And let F^{sj} = { f_i^{sj} |i = 1, . . . , M} be a feature vector of the enrolled sample s j of the user u where j = 1, . . . , S. The Equation describes the template signature and it is defined as follows

Template Signature $TS_i = \frac{1}{s}\sum_{j=1}^{s} f_i^{sj}$ (1)
where i = 1,…, M. Then, the feature vector of each enrolled sample s of the user u.

c) Matching Process

The matching processes do the authentication process for signature using Euclidian distance method. The matching process is done for query signature against the template signature. If the matching score is less than a optimal threshold and the difference of crossing number count is less than the threshold then the query signature is a authenticated one otherwise not. The system then accepts the sample t if the dissimilarity score is less than a predefined threshold, otherwise it rejects. The basis of many measures of similarity and dissimilarity is Euclidean distance. The Equation describes as distance between vectors x and y is defined as follows:

$$d(x,y) = \sqrt{\sum_{i}^{n}(x_i - y_i)^2} \qquad (2)$$

x means query signature features
y means Template signature features
n means number of histogram elements

Euclidean distance is the square root of the sum of squared differences between corresponding elements of the two vectors.

IV. IMPLEMENTATION

The online signature verification includes and implemented crossing number feature extraction, Euclidean matching, and signature sequence feature extraction process

Crossing Number Feature Extraction

The crossing number is most commonly employed method of minutiae extraction. This method involves the use of the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3x3 window. The crossing number feature extraction algorithm is described as follows

Input : Signature flow information
Output : Junction point information
Method : Crossing number method

Step 1: Convert the signature flow information into a image

Step2: Collect the 3 x 3 window size information in the sequence of P_0, P_1, P_2 …. P_7

Step 3: Find the difference of the previous and the current data from the 3 x 3 window

Step4: Find the difference of P_1 and P_8 component

Step 5: Sum of the computed step of 3 and 4 to get the crossing information value

Step 6: If the crossing value is greater than 9 then the considered pixel is marked as junction point.

Euclidean matching

Euclidean distance is only appropriate for data measured on the same scale. Here high similarity means low distance value and low similarity means high distance value. If the distance value is less than the optimal threshold and the crossing number pixel count difference is less than the threshold then the query signature verification is announced as an authenticated one, otherwise it is announced as a unauthenticated one. The Euclidean matching algorithm is described as follows

```
Input   : Query histogram features and Template histogram features.
Output  : Matching value.
Method  : Euclidean Matching
        Step 1: Load the query histogram feature in memory.
        Step 2: Load the template histogram feature in memory.
        Step 3: Find the error values.
        Step 4: Square the error values.
        Step 5: Sum of the squared error values in a consequent computed sum.
        Step 6: Find the square root value for the final sum of the value and display the matched value.
```

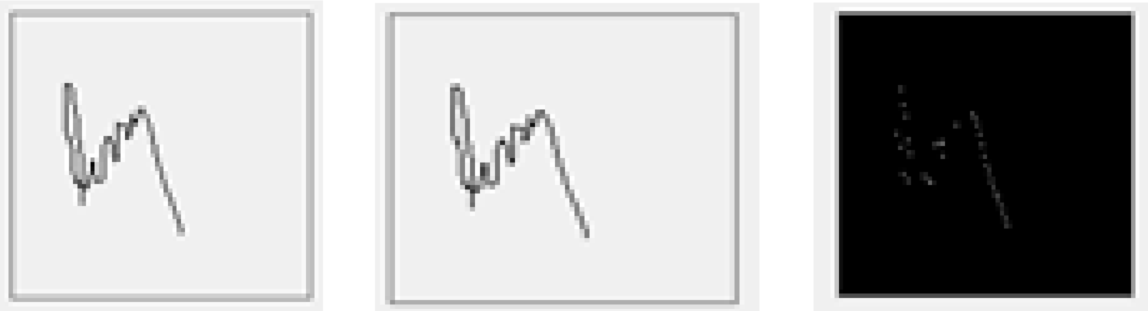
Signature Sequence Feature Extraction Method

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. This subsection describes how a set of histograms are computed from an online signature. These histograms are designed to capture essential information of an online signature attributes as well as the relationships between these attributes. The signature sequence feature extraction method algorithm is described as follows

```
Input   : Signature information of the user
Output  : Histogram feature of the given signature
Method  : signature sequence feature extraction method
          Step 1: Find the x difference for 1st order derivative
          Step 2: Find the x difference for 2nd order derivative
          Step 3: Find the y difference for 1st order derivative
          Step 4: Find the y difference for 2nd order derivative
          Step 5: Find the angle feature for 1st order derivative feature
          Step 6: Find the angle feature for 2nd order derivative feature
          Step 7: Find the speed feature for 1st order derivative feature
          Step 8: Find the speed feature for 2nd order
          Step 9: Compute histogram for 1st order x difference
          Step 10: Compute histogram for 2nd order x difference
          Step 11:Compute histogram for 1st order y difference
          Step 12: Compute histogram for 2nd order y difference
          Step 13: Compute histogram for 1st order angle
          Step 14: Compute histogram for 2nd order angle
          Step 15: Compute histogram for 1st order speed
          Step 16: Compute histogram for 2nd order speed
          Step 17: Combine all the computed histograms
```

V. EXPERIMENTAL RESULTS

An experimental result shows the effectiveness of the proposed algorithm than the existing methods. The proposed techniques the signature is drawn through the on-line signature. This scheme is authentication and the performance is accuracy. According to the result, verification performance is gradually degrades when attributes of each histogram are iteratively removed from the feature set. The step by step output for the various processes involved in the proposed Crossing number algorithm is described as follows.

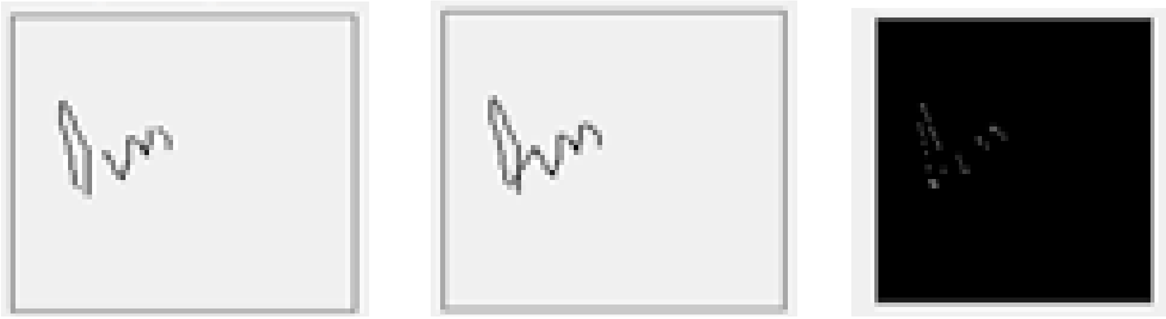


a)original signature **b)preprocessed signature** **c)crossing No feature**

Figure 4.1 Query Signature

In a query signature processing first give a original signature then preprocessed the signature the preprocess is used to continue the process and join. The crossing number based junction points computation helps to increase the security level.

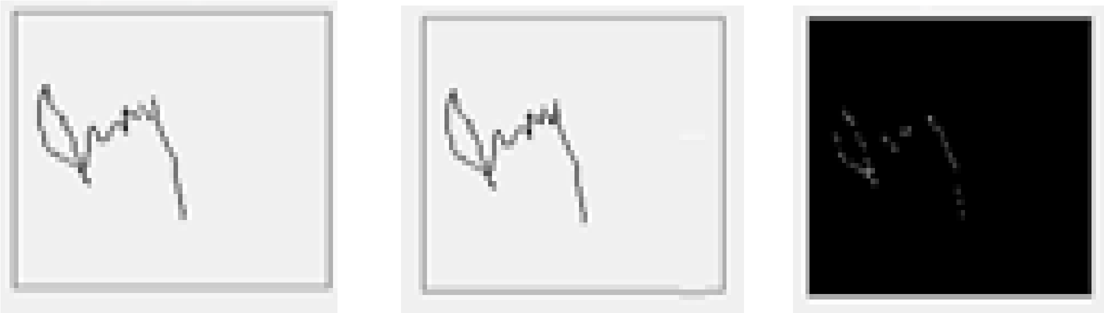
The query signature can be verified with only template signature and not for the entire database signature. It implies that these histograms, when applied with the proposed verification approach, provide complimentary information that is useful for online signature verification**.**



a)original signature **b)preprocessed signature** **c)crossing No feature**

Figure 4.2 sample signature trial1

In the sample signature trial1 first give the original signature then preprocessed and then find the crossing number feature using crossing number algorithm. The privacy protection provided by the proposed system is also investigated by analyzing the possibility of linking the identities of a user enrolled in different systems. Specifically, cross- link attacks such as those described in could be considered.

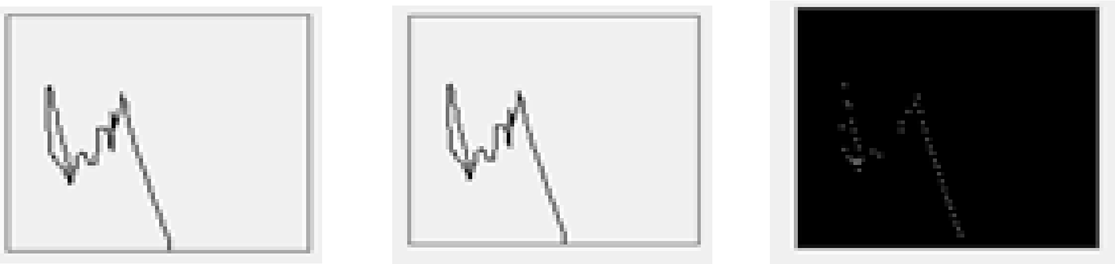


a)original signature **b)preprocessed signature** **c)crossing No feature**

Figure 4.3 sample signature trial2

In a sample signature processing trial2 give a original signature then preprocessed the signature the preprocess is used to continue the process and join. The crossing number based junction points computation helps to increase the security level.

The verification performance of individual histogram at the current configuration is slightly lower than the one when the resolution is increases, where it is higher than the one when the resolution is decreases.



a)original signature **b)preprocessed signature** **c)crossing No feature**

Figure 4.4 sample signature trial3

In sample signature trial3 process is an enrollment process the three signatures are combined and generate the template. Then match the query signature using Euclidean distance based.

If the distance value is less than the optimal threshold and the crossing number pixel count difference is less than the threshold then the query signature verification is announced as an authenticated one, otherwise it is announced as a unauthenticated one.

VI. CONCLUSION

This paper proposes an advanced and efficient method for online signature verification. The histogram features which are constructed from the x difference, y difference, angle and speed properties. The crossing number based junction points computation helps to increase the security level. The matching process is done using Euclidian distance method.

The query signature can be verified with only template signature and not for the entire database signature. This method is well suitable for mobile devices which have touch interfaces because of the bi-authentication process. The proposed scheme has the advantages of high performance in authentication is accuracy than the existing system.

REFERENCES

[1]. Argones Rua E. Maiorana E. Alba Castro J. and Campisi P. (2012) 'Biometric template protection using universal background models: An application to online signature', IEEE Trans. Inf. Forensics Security, Vol. 7, No. 1, pp. 269–282.

[2]. Ashwini Pansare and Shalini Bhatia (2012) 'Handwritten Signature Verification using Neural Network', International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 1– No.2.

[3]. Faundez-Zanu M. (2007) 'On-line signature recognition based on VQ-DTW ', Pattern Recognit., Vol. 40, No. 3, pp. 981–992.

[4]. Feng H and Wah C. C. (2003) 'Online signature verification using a new extreme points warping technique', Pattern Recognit. Lett., Vol. 24, No. 16, pp. 2943 2951.

[5]. Park U. Jillela R R. Ross A and Jain A K. (2011) 'Periocular biometrics in the visible spectrum', IEEE Trans. Inf. Forensics Security, Vol. 6, No. 1, pp. 96–106.

[6]. Guru D. and Prakash H.(2009) 'Online signature verification and recognition: An approach based on symbolic representation', IEEE Trans. Pattern Anal. Mach. Intell., Vol. 31, No. 6, pp. 1059–1073.

[7]. Kholmatov and Yanikoglu B. (2005) 'Identity authentication using improved online signature verification method', Pattern Recognit. Lett., Vol. 26, pp. 2400–2408.

[8]. Sae-Bae N. Memon N. Isbister K. and Ahmed K. (2014), 'Multitouch gesturebased authentication', IEEE Trans. Inf. Forensics Security, Vol. 9,No. 4, pp. 568–582.

[9]. Nanni L. and Lumini A. (2008) 'A novel local on-line signature verification system', Pattern Recognit. Lett., Vol. 29, No. 5, pp. 559–568, 2008.

[10]. Napa Sae-Bae and Nasir Memon (2008) 'A Simple and Effective Method for Online Signature Verification', Computer Science Department, NYU-Poly Six Metrotech Center, Brooklyn, New York, 11201 nsae-b01@students.poly.edu, memon@poly.edu