ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Positional Invariant Features Based Online Signature Verification for Personal Authentication

Preeti S Pattankude[1], Tushar Bedke[2]

PG Student, Department of DECS, Maratha Mandal Engineering College Belgaum, Karnataka, India[1]

Assistant Prof, Department of ECE, Maratha Mandal Engineering College Belgaum, Karnataka, India[2]

ABSTRACT: This project presents positional invariant features based online signature verification on touch interface mobile devices for personal identification and authentication. The proposed system uses set of attributes such as x, y coordinates and pressure of all signature points of each user as an input. Histograms set will be used to represent online signatures. These set of histogram features are designed to get essential attributes of the signature and relationships between these attributes. These histogram sets are widely used as feature set to capture attribute statistics in the process of recognition. The feature extraction will begin by converting Cartesian coordinates to polar coordinates and deriving positional invariant features from those attributes. Before signature verification, an enrollment of user signature is done to generate the template for authorized user. The template is consists of two vectors such as quantization vector and quantized histogram feature vector (absolute and relative frequency). This process is very flexible and need constant space to store. At verification stage, the same feature vectors are extracted from test input with help of quantization vector of enrolled signatures and its matching is done by using SVM classifier algorithm. By using SVM classifier, decision is made either authentication or unauthorized user. And to provide the more security for signature we are providing separate authorization key for each user. The Performance of system will be validated with recognition percentage measure and it shows that used methodologies provides better accuracy in performance and more flexible than previous approaches.

KEYWORDS: Histograms, Cartesian coordinate, Polarcoordinates, Svm Classifier

I. INTRODUCTION

Signature Reliability, authenticity and authorizations are highly necessary for many common places such as aircraftboarding, crossing borders of international, entering in a secure physical location, and performing financial (economical) transactions.Ahandwritten signature is a legally and socially accepted biometric trait for authenticating an individual. Typically, there are 2 types of handwritten signature verification systems: “*off-line*”and “*online*”systems. In off-line system, just an image of the user’s signature is acquired without additional attributes, whereas, in online system, a sequence of x-y co-ordinates of the user’s signature, along with associated attributes like time, pressure etc, are also acquired. So, an online verification system usually achieves more accuracy than off-line system. The increasing of personal computational devices that is equipped with a touch sensitive interface and the difficulty in entering a password on those devices have led to an interest in developing alternative authentication(security) mechanisms on them. In this context, online signature is a reasonable candidate given the familiarity users have with the concept of using a signature for the purpose of authorization. There has been much work on online signature verification systems. However, no one of this has been directed to the context of authentication on computing mobile devices.

Existing work has been addressed that online signatures obtained from traditional digitizers in a controlled environment. These are different from those obtained from mobile device in dynamic environment. Initially, on computing mobile device, a user performs his signatures in various contexts i.e., sitting/standing, mobile/immobile and holding a device at different orientation and angles. Secondarily, when compared with stand-alone obtained devices, availability of computational resources (results) may differ from one signature to another signature instance and it will

DOI:10.15662/IJAREEIE.2015.0505133

results in larger variation of input resolution. Finally, to get result of less precise signals, signatures are drawn on mobile devices by using a finger instead of stylus.

Performance verification derived from datasets oftraditional one, collected using stylus-based devices in a systemof controlled environment, and may not carry over signature online verification on setting of mobile devices. In addition, other characteristics of a system such as,aging of templates and effectiveness training of cross sessions may be different, when signatures are acquired from computing mobile devices. Proposed paper insists that verification of signature online, algorithm which is suitable to deploy (install) on computing mobile devices. This algorithm is computationally and space efficient for verifying (validating)signatures and enrolling. In addition, templatesof signaturesare kept in an irreversible form thereby, providing authenticity to an original signature. This method was evaluated on public datasets and new datasetsobtained in uncontrolled settings from user owned computing devices. The produced performance of online signature verification is promising. The main contributions done by this particular paper are below mentioned:-
1. A method to extract a model-free non-invertible feature set from an online signature is introduced. That particular set of features contains histogram sets that capture distribution of attributes originated (created) from signaturesraw data sequences and their combinations. By evaluating the proposed algorithm on public datasets, its performance verification is superior to several states of the algorithms.
2. In computing mobile device verification environment, new dataset was collected from 180 users. This dataset contains the signatures which were drawn with fingertip, in an uncontrolled settings on user owned iOS device and over six different sessions with intervals ranging from 12 to 96 hours.
3.After applying this proposed method on the above dataset, the following aspects of online signature verification on computing mobile devices were investigated-
• Impact of template aging in online signatures.
• Effectiveness of using cross-sessions samples, or samples from multiple sessions, to train a classifier.
• Security and authenticity of the system against random forgery, or zero-effort attack, and its comparison to that of 4 digits PIN.

II. PREVIOUS WORK

Usually online signature verification techniques can be classified into two approaches, namely, feature based and function-based [5]. The earlier refersto an approach where the matching process is done by using descriptive features of a signature. Examples of well-known function-based approaches include Dynamic Time Warping Algorithm (DTW) [6], [7], and Hidden Markov Models (HMM) [8] to a method where the matching process is done using, directly or indirectly, the original time series data points of a signature. The latter method that is a function-based system typically yields better verification performance than a feature-based system. However, during the matching process, a dynamic structure of the original signature is revealed resulting in a possible privacy problem if the matching has to be done remotely.

Function based systemis generally more difficult and slower than feature based systems [6]. Even not as good as, when a template protection approach is applied in order to provide biometric privacy or security, verification performance frequentlyget worseextensively. For example, Maiorana et al havesuggested a convolution system to defend the original signature sequence of a user, which can be directly applied to any function based method.Original input sequence is splited into*W* subsequences. Every subsequence consist different length based on random constraints.

This method has been applied with HMM and DTW based authenticationsystems Inevery case verification rates were lower when compared to using the original versions of the signatures. In a feature-based system an online signature is represented by a feature vector. For that reason, the original biometric sample need not be stored or else transmitted. Many well-knownalgorithms are used to derive authentication keys from feature vectors. The main challenge for the feature-based approach is to developanexpressive set of features that are used efficiently and effectively to verify an online signature [5], [6],In the collected works, there are so many methods to derive a set of features from an online signature. In the year 2005, Fierrez-Aguilar et al suggested a set of 100 features; they are total duration of the signature, totalnumber of pen ups, sign variations of *(dy/dt)*and (*dx/dt*), etc. To represent a signature and apply a feature selection method to rank the proposed features. Based on 100 features of signatureset, Nanni suggested a multi-matcher method to verify an online signature. In addition, to this Guru and Prakash developed a symbolic demonstration of an online signature and presented the theory of writer independent threshold in order to increase verification accuracy. In recent times, Argones etalhave derived a set of HMM model features fromthe universal background method. The good stated verification performance obtained by their system is favorable. The system achieves 4800 features from alterationof 16 different HMM models, which is computationally difficult task. Furthermore, the universal background model is trained from the pool of 2500 genuine and forged signatures from 50 users on the same device requirement, where a user-specific classifier is trained from 10 signatures. These are making it less feasible to be in employment for mobile device for authentication, where the fixed sensors are different from one model to other. In addition to this HMM-based method is not tough to the known template aged problem this results significant deterioration of verification presentation when verifyingsamples and enrollment samples are from different periods.

III. PROPOSED METHOD

Online signature verification on touch interface based mobile devices for personal authentication by Matching histogram of positional invariant features from signature attributes such as Cartesian and polar coordinates and pressure is done and procedure is shown in Fig 1.

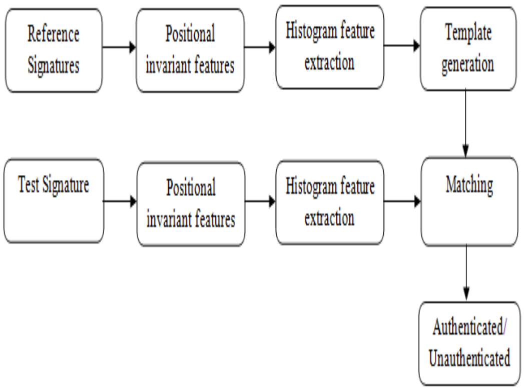
Reference Signatures
Positional invariant features
Histogram feature extraction
Template generation
Test Signature
Positional invariant features
Histogram feature extraction
Matching
Authenticated/ Unauthenticated

Fig 1: Block Diagram of Proposed Method

- ***Positional Invariant Analysis:***

An online signature is represented by a set of histograms. These histogram features are designed to capture necessary attributes of the signature as well as relationships between these attributes of the signature. It should be noted that histograms are extensively used as a feature set to capture attribute statistics in many recognition tasks. For example, in an object recognition and off-line signature verification process. Using histograms for online signature verification was first suggested by Nelson et al . They have also used as part of the feature set in [1], and conversely in [1] and the use of histograms arerestricted only to angles derived from vectors connecting two successive points in an online signature. In statistic, as is shown below, more information can be used to derive histograms beneficial in online signature verification. These include speed, x-y trajectories, pressure, angles, and their derivatives. The feature extraction process of the proposed method begins with converting time-series data of a signature in to a sequence of Cartesian vectors and attributes, as well as their derivatives. Then, every Cartesian vector is converted to a vector in the polar coordinate system. Lastly, histograms from these vector sequences are derived. Detailed process of feature extraction is as follows.

Let $X = \{x1, x2, . . . ,xn\}$,
$Y = \{y1, y2, . . . ,yn\}$, and
$P = \{p1, p2, . . . ,pn\}$ be the x *co-ordinate* and y co-ordinates and pressure attribute, respectively, of a signature with length n sampled at times $T = \{t1, t2, . . . , tn\}$. For datasets used in this experiment, all signatures were sampled at a constant rate. Hence the time information is understood and is overlooked. One important observation isthat if time intervals are not constant, a normalization process using information from T can be applied to the sequences X, Y, and

P former to being processed by the system. To initiate with, the vectors *X*1, *Y* 1, and *P*1 together with their derivatives are computed as follows,

$$\mathbf{X}^1 = \{\mathbf{x}_i{}^1 \mid \mathbf{x}_i{}^1 = \mathbf{x}_{i+1} - \mathbf{x}_i\},$$
$$\mathbf{Y}^1 = \{\mathbf{u}_i{}^1 \mid \mathbf{y}_i{}^1 = \mathbf{y}_{i+1} - \mathbf{y}_i\},$$
$$\mathbf{P}^1 = \{ \mathbf{P}_i \},$$

$$\mathbf{X}^k = \{x_i^k \mid x_i^k = x_{i+1}^{k-1} - x_i^{k-1}\},$$
$$\mathbf{Y}^k = \{y_i^k \mid y_i^k = y_{i+1}^{k-1} - y_i^{k-1}\},$$
$$\mathbf{P}^k = \{p_i^k \mid p_i^k = p_{i+1}^{k-1} - p_i^{k-1}\},$$

By computing differences between each pair of successive points as above, the vectors *X*1 and *Y*1 capture the positional invariant features of the signature. And by iterating this process of taking differences *k* times results the*kth*order derivative, *Xk*and *Yk*, of the original *X* and *Y* sequences respectively.
Then, a series of vectors

$$\mathrm{V} = \{v_i^* \mid i = 1, 2, \ldots, n\}$$

$$v_i^k = \langle x_i^k, y_i^k, r_i^k, \theta_i^k, p_i^k \rangle$$

Where,

$$\theta_i^k = \tan^{-1}(y_i^k / x_i^k),$$
$$r_i^k = \sqrt{(x_i^k)^2 + (y_i^k)^2}$$

- ***Template Generation***

We will generate templates during the enrollment process where multiple signatures are taken from a user and a feature sets are computed from each of the samples. Then,variance of each of the featuresection is computed and is used to create a user-specific uniform quantizer for each of the feature element resulting in a quantization step size vector *Qu*this is used to quantize each of the feature vectors imitativefrom the enrollment samples. Lastly, an average of these quantized feature vectors are used as the template ¨*Fu* for the user. This feature vector and as well as the quantization step size vectors are stored matching to the identity of the user.

During verification stage a user is asked for an identity *u* is to produce one exampleof an online signature which is again represented by the set of features. Then the quantization step size vector, Q^umatching to that identity is used to derive a quantized feature vector from the signature input. Afterwards, the system compares these quantized feature vectors in contrast to the stored feature vector template F^u.The signature is accepted ifa trained samples result matches with test and reference signatureInthe training phase we choose a number of genuine andForged signatures for training the SVM classifier. In the verification phase when a test signature is input to the system is compared to each of the reference signatures of the requested person. The person is authenticated if the resulting dissimilarity measure is below or equals a threshold value of the classifier, otherwise denied.

The detailed description on howto derive the quantization step size vector $Q^u$and the template feature vector are explained below. Consider Sbe the total number of enrolled samples and *M* bethe total number of features for each sample. And let$\boldsymbol{F^{sj}} = \{ f^{sj}{}_{i\backslash i} \mid \boldsymbol{i} = 1, \ldots, \boldsymbol{M}\}$be a feature vector of the enrolled sample***s j***of the user ***u***where***j* = 1, . . . , *S*.** The quantization stepsize vector of the user ***u*, $\boldsymbol{Q^u} = \{q_i{}^u \mid i = 1, \ldots, M\}$,** is achievedby calculating the standard deviations over all the enrolled samples for each feature and using a several of this as the quantization step size. That is,

$$q_i^u = \sqrt[\beta]{\frac{1}{S}\sum_{j=1}^{S}\left(f_i^{S_j} - \mu_{f_i^{(u)}}\right)^2}, i = 1, \ldots, \mathrm{M}$$

Where,

$$\mu_{f_i^{(u)}} = \frac{1}{S}\sum_{j=1}^{S} f_i^{S_j}$$

*β*is experimentally fixed at 1.5. Then, the quantized feature vector of each enrolled sample*s* of the user *u*

,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

$$\hat{F}^{(S_j\backslash u)} = \{\hat{f}_i^{S_j} | i = 1, \ldots, M\}$$

From the quantization step sizes $\boldsymbol{q_i^u}$in$\boldsymbol{Q^u}$(adding a small _to prevent division by zero) as follows,

$$\hat{f}_i^{(s_j|u)} = \left[\frac{f_i^{s_j}}{q_i^u + \epsilon}\right], \quad i = 1, \ldots, M$$

Where$\epsilon$is at 0.002 and 0.8 for histograms with absolute and relative frequencies, respectively.
Lastly, the user-specific feature vector template, F^u =$\{f_i^u|i= 1, \ldots , M\}$, is derived by averaging the quantizedfeature vectors of all the enrolled online signature samplesfrom the user *u*.

$$\ddot{f}_i^u = \left[\frac{\sum_{j=1}^{S} \hat{f}_i^{(s_j|u)}}{S}\right], \quad i = 1, \ldots, M$$

A pair (Q^u F^u) comprising of the quantization step size vector and its associated feature vector template is then stored and later used to verify a claimed signature of the user *u*.

- ***Histogram Analysis***

One dimensional histograms:These capture distributions of separate attributes. The histogram ∅1 capturesthe angle distribution of an online signature which reproduces the relationship between two signaturescharacters. In the same way, ∅2 captures the distribution of the angles of the first derivative since it deals information about how these vectors are aligned an characteristic that is completely ignored in the histogram∅1. R^1 determines the speed distribution of an online signature which is one of the unique features that is distinctive among users and especially useful in contend with skilled forgeries.

Two dimensional histograms – These capture distributions of association between pairs of characteristics. For example<∅1 *R*1 and <∅2 *R*1 >captures the distribution of dependency between speed and angle of the first and the second halves of the online signature. Similarly, <∅1 ∅1 *d*(1,2*)* >captures the distribution of the relationship between three sequential angularcoordinates of an online signature classification while provided thatchanging flexibility when comparing two different signatures from the same user.

- ***Feature Matching***

Previously matching was done by using Euclidian distance metric matching .To improve the accuracy of the system we are replacing Euclidian distance metric by SVM classifier. To provide security for each user's signature separate passwords are assigned to each user at verification stage first we will match the password for both test and reference signature if it matches then further process will be continued which is followed by SVM classifier The SVMi.e support vector machine a learning method tries to find an optimal hyper plane for separating two classes. Therefore, themisclassification error of data both in the training set and test set is minimized. The classification based on SVM involvestraining and testing stagesInthe training phase we choose a number of genuine andForged signatures for training the SVM classifier. In the verification phase when a test signature is input to the system, it is compared to each of the reference signatures of the claimed person. The person is authenticated if the resulting dissimilarity measure is below or equals a threshold value of the classifier, otherwise denied.

IV. SIMULATION RESULTS

We arestoring signatures as well as passwords for each user in database for particular application and for verification process we will extract these signatures to compare with the input signature. First we will match the passwords of input signature and reference signature if password is matched then further process is continued and if the input signature is present in the database, then the particular person is considered as an authorized person. If that input signature is not present in the database, then the person will be considered as unauthorized person. Usually this technique is required to achieve authenticity and security for personal sensitive information, such as boarding an aircraft, crossing international borders, entering a secure physical location, and performing financial transactions.

Database sample signature is shown in Fig.2. Later we will plot the signature as shown in Fig.3.this figure explains maximum and minimum value of x coordinate and y coordinate and then we will extract the invariant features of these signaturesand we will represent these in histogram form as shown in Fig4.

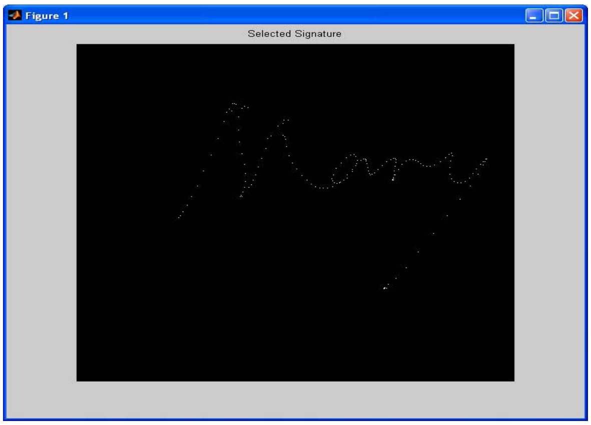

Fig2: Sample of signature

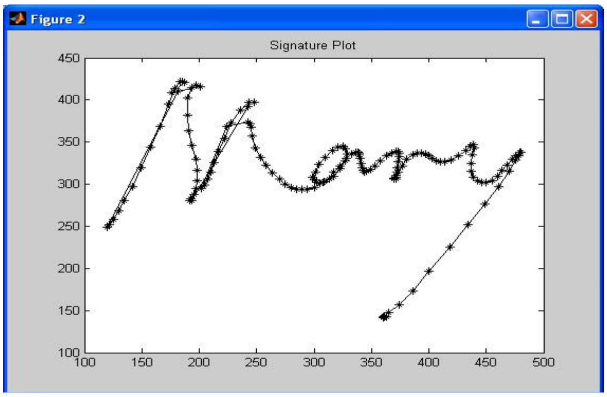

Fig 3: Signature plot

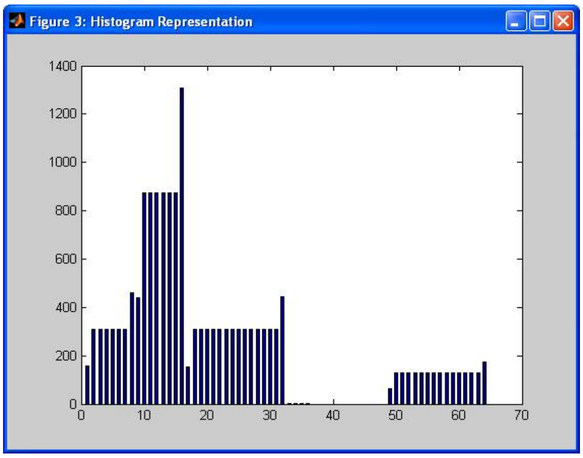

Fig 4: Histogram representation

DOI:10.15662/IJAREEIE.2015.0505133

By applying histogram feature extraction along with SVM classifier methodwe can achieve better performance parameter like accuracy of 93%, sensitivity 92.85%, and Specificity 92.3077% these parameters are shown in Fig 5.and by applying SVM classifier method we achieved accuracy of 93% which is better accuracy when comparing it with earlier method that is Euclidian distance metric matching.If we store more different signature samples of each user then we can achieve better performance of the system which is shown in fig 6

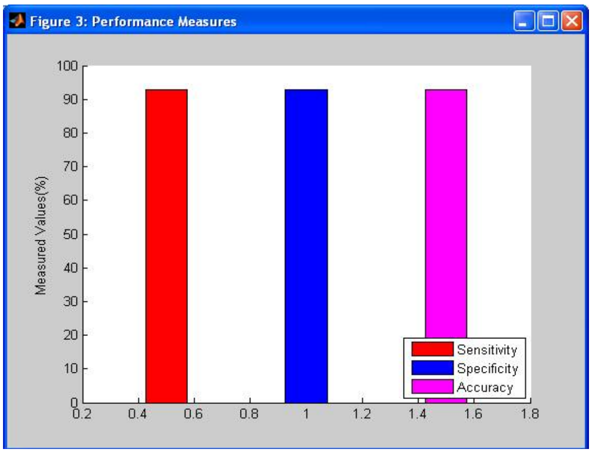

Fig5: Performance measures in percentage

- **Performance Evaluation**

The performance of classifier can be evaluated through following parameters,

Sensitivity: It measures the proportion of actual positives which are correctly identified.

Sensitivity = Tp. / (Tp + Fn)

Where,

Tp = True Positive: Forgery correctly classified as Forgeries.

Fn = False negative: Forgery incorrectly classified as Original.

Specificity: It measures the proportion of negatives which are correctly identified.

Specificity = Tn./(Fp + Tn)

Where,

Fp = False Positive: Original incorrectly classified as Forgeries

Tn = True negative: Normal correctly classified as normal

Total accuracy:(Tp+Tn). /(Tp+Tn+Fp+Fn)

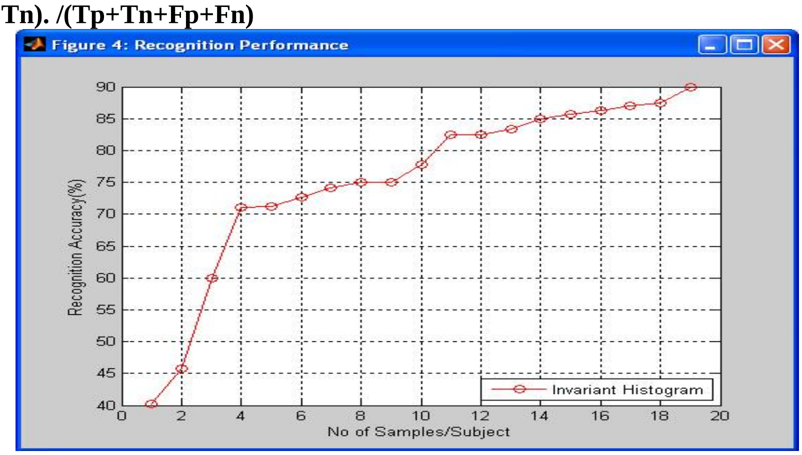

Fig 6: Recognition performance

DOI:10.15662/IJAREEIE.2015.0505133

V. CONCLUSION AND FUTURE WORK

This paper proposes a simple and effective online signature verification system that is suitable for user authentication on a mobile device. The use of the proposed algorithm are as follows, First password matching is done then the verification process starts ie, 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, to this the feature set represents only statistics about distribution of original online signature features, the conversion is non-invertible. As a result, of this the privacy of the original biometric data is good 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 enrollment samples from that user without requiring a training set from a large number of users. SVM classifier achieves better accuracy compared with Euclidian distance matching method.

One motivating area for future work is the design of an enrollment protocol that can capture an intra-user variation effectively within a single session. In addition, at present it is possible to match different signature templates generated from the same online signature samples and thereby obtain that two leaked biometric templates belong to the same user.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] L. Nanni, “An advanced multi-matcher method for on-line signature verification featuring global features and tokenised random numbers,” *Neuro computing*, vol. 69, nos. 16–18, pp. 2402–2406, 2006.

[5] 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.

[6] 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.

[7] N. Sae-Bae and N. Memon, “A simple and effective method for online signature verification,” in *Proc. Int. Conf. BIOSIG*,pp. 1–12, 2013.