Cluster Comput
DOI 10.1007/s10586-017-1129-4

VerSig: a new approach for online signature verification

Mehr Yahya Durrani[1,2] · **Salabat Khan**[1] · **Shehzad Khalid**[3]

Received: 31 March 2017 / Revised: 9 July 2017 / Accepted: 16 August 2017

Abstract This paper introduces, VerSig, a new proposed scheme for online signature verification. The proposed scheme is based on creation of a signature envelope by employing dynamic time warping method. This envelope provides the basis for decision of forged and authentic signatures. The scheme only uses basic features such as X, Y coordinates of the signature. A well known and standardized Japanese handwritten dataset (provided for ICDAR 2013 signature verification competition) is used to evaluate the performance of proposed method. Proposed method is compared with state of art methods and observed to offer significant improvements in terms of overall accuracy of prediction.

Keywords Online signature verification · Feature selection · Template selection · Dynamic time warping · Signature envelope

1 Introduction

Biometric identification is considered as most reliable authentication technique used for security purposes. Biometric identification can be subdivided in to biological traits e.g., finger print recognition, iris scanning, and behavioral traits such as handwritten signature verification, voice recognition etc [1]. Signature verification is one of the oldest and most commonly used methods for a person's identification. Almost all types of financial instruments as well as legal documents are still authenticated by way of a handwritten signature. Signature verification is thus an active area of research for researchers for centuries. A renewed interest is taken by the research with the proliferation of mobile devices which use signatures or patterns for unlocking the mobile devices [2].

Signature verification can be classified as: (1) offline signature verification, and (2) online signature verification; whereas the former concerns with verification of the signatures available on a paper and the later focuses on the signatures obtained through a specialized digital hardware such as graphic tablet [3]. Signature verification is a two class pattern recognition problem [4] and like any other pattern recognition problem, it relies on storage of some sort of features extracted from given samples. The extracted features from template samples/ signatures are later stored in a database for verification purposes. A detailed survey of various features used in signature verification systems is presented in [5] which identified 46 global and 39 local features for signature verification. Any signature presented to the system for verification goes through the same process. The features are extracted from sample currently being observed and match against the features of the template signatures present in the database of the system. Since, two signatures of a person cannot exactly be the same; a threshold value of similarity is used for decision of whether the signature is authentic or forged.

A generalized architecture of a signature verification system is presented in Fig. 1. The system is first trained with the help of training data, and later in the testing phase an unseen sample is given to test the ability of the system to correctly label the target sample. In case of signature verification system, the training data obtained from graphic tablet, requires to undergo certain preprocessing steps such

✉ Mehr Yahya Durrani
mehr.pk@gmail.com

[1] Department of Computer Science, COMSATS Institute of Information Technology, Attock, Pakistan

[2] Department of Computer Science, Iqra National University, Peshawar, Pakistan

[3] Department of Computer Engineering, Bahria University, Islamabad, Pakistan

Published online: 28 August 2017

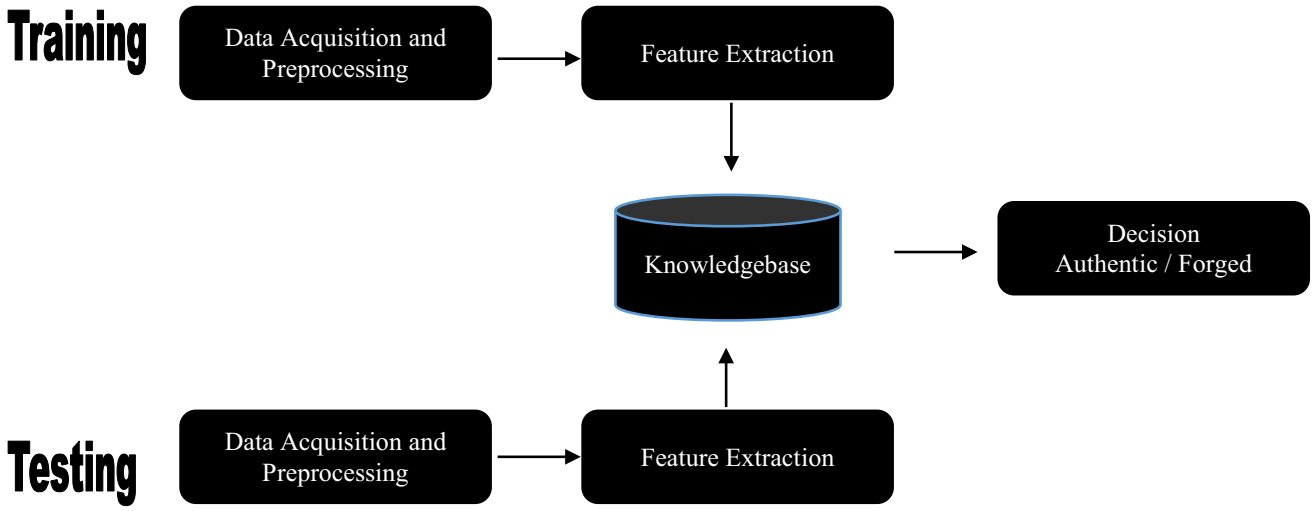


Fig. 1 Generic architecture of online signature verification system

as noise removal etc. Later, features are extracted from this data which are stored in knowledgebase. During the testing phase a target signature is presented to the system whose features are extracted and matched with the features stored in the knowledgebase. Decision regarding the authenticity/forgery is made on the basis of similarity score of these features.

Online signature verification systems either employ model based techniques or distance based techniques [2]. Model based approaches use generative classifiers such as HMM, GMM etc [6] while distance based techniques use dynamic programming techniques to calculate a score for similarity/dissimilarity. Examples of distance based technique are Euclidean distance, City block distance and dynamic time warping (DTW) etc. Even the genuine signatures of a user are different from each other due to various psychological and economical conditions [7]. In such situations, distance based techniques which employ exact matching techniques such as Euclidean distance provide poor results. On the other hand, elastic matching techniques such as DTW provide better results for the situations like signature verification [8].

In online signature verification system the data is captured as a time series signal from digital signature of a person drawn on a graphic tablet. Due to the fact that the two signatures of a person cannot exactly be the same, it is necessary to capture several sample signatures for a single person to be used as training data. The captured signal vectors would either be different in length or different in time domain. So, it is necessary to align these signals before calculating the magnitude of similarity or dissimilarity between two signals. DTW is a technique which measures the similarity of two time series signals which differ in phase or timing [9]; thus becomes an ideal candidate to be used for signature verification.

This paper presents a DTW based signature verification scheme which only uses basic features i.e. X and Y coordinates of the captured signals. The proposed approach uses DTW to align the signatures which are different in length or phase. From the training dataset the best candidate is selected as a template signature and a generic signature envelope is created on the basis of the template and other signatures available in training set. The signature envelope serves as the boundary for taking decision of authentic/forged signatures. The beauty of the scheme is that it is very simple and uses only basic features which result in low resources requirement. The results obtained are superior to the schemes which use the same dataset for evaluation purpose. Key contributions of this research work can be summarized as follows:

- A novel generalized envelope is created for signature identification which serves as decision boundary.
- The scheme is simple in the sense that it uses only basic features and thus consumes minimal possible resources.
- The accuracy of the proposed scheme is the highest among the schemes which have used same dataset.

The remainder of the paper is organized as follows. Section 2 describes the related work. Section 3 provide details of the proposed approach while Sect. 4 describes the dataset used for evaluation purpose. Section 4 further discuss the results obtained through experiments and elaborate the reasoning of why the proposed method outperforms other state of the art methods. Section 5 concludes the discussion and investigates possible future avenues for the subject purpose.

2 Related work

Handwritten signatures are used for centuries to establish a person's authentication in his absence. With the digital revolution the same signatures are used for a person's iden-

tification. Online signature verification based schemes use a digital tablet for obtaining a user's signature and extracting and storing the features from this signature [10]. The same features are later matched with the features of a given signature for verifying the signature [10]. Online signature verification is an active research area for last four decades. Subsequently, detail surveys of various schemes can be found in [3,10–13]. Like any pattern recognition system, signature verification systems are based on feature extraction i.e., global and local features. Global features are the ones which are extracted from the signature as a whole. These include signature trajectories, average of the signing speed, Fourier descriptors of the signature etc [5]. On the other hand local features extract information from each sample point. These include distance and trajectory changes between two successive samples points, pressure applied on each point etc [5].

Feature extraction is followed by classification stage where signature is classified either based on some form of distance or on some model. One such scheme is based on the use of City block distance [4]. In distance based scheme DTW is most widely used scheme as it allows alignment of two signatures with different length [14,15]. Some researchers employed classical distance scheme such as Euclidean distance [16] and Mahanabolis distance [17]. Another distance based scheme employed for signature verification include longest common subsequence (LCSS) [18].

Model based schemes on the other hand tryto estimate statistical model which represent most important features of the signature. Model based schemes include Hidden Markov Model (HMM) [6,19] and Gaussian mix model (GMM) [20,21]. Other model based techniques employed for signature verification include Support Vector Machine (SVM) [22], Artificial neural networks [1] etc.

There are other methods as well which perform transformations such as fast Fourier transform (FFT), discrete cosine transform (DCT) or discrete wavelet transform (DWT). Features are extracted from signatures through WT and are passed through DCT for dimensionality reduction and are later classified through LPD in [23]. The authors of [24] used FFT and then used the Euclidean distance between these descriptors in their proposed scheme. Proposed scheme in [25] uses DCT on 44 extracted features for performing signature verification. Similarly, a slightly modified version of DCT, discrete fractional cosine transform (DFrCT) is used in [26] for feature extraction and the distance between the descriptors is used as criteria for signature verification. Other schemes such as [27] use clustering techniques to extract important features which describe characteristics of a user and later use various classifiers for signature verification. Similarly, discrete Fourier transform is applied on signature data for feature extraction which is followed by DTW based distance measurement in [28].

The proposed scheme in this paper is based on DTW. Hence it would be imperative to provide an insight in to DTW based signature verification schemes. Rest of the section describes some recent work on DTW based scheme.

DTW is a dynamic programming technique and is a computationally expensive process.DTW works by taking two input signals $I = (i_1, i_2, \ldots, i_a)$ and $J = (j_1, j_2, \ldots, j_b)$ with length a and b, respectively.DTW align these signals in such a way that one point of first signal vector is aligned with the best matching point in second signal vector. It effectively computes a distance matrix which provides alignment between two best matching points I_x, J_y [8]. DTW can be described by the following equation:

$$D(x, y) = d(i_x, j_y) + \{minD(x-1, y-1), D(x-1, y-2), D(x-2, y-1)\} \quad (1)$$

Many researchers have proposed modification in original DTW to improve its performance. Improvement of performance of DTW for signature verification is the focus of [29]. The focus of [30] is use of a modified version of DTW, EADTW which accelerates the verification process. A Multidomain verification system is proposed in [31] which use DTW for selection of a prototype signature. Normalization of scores obtained through DTW is the focus of [32]. Another scheme is discussed in [33] which employ DTW for matching. Improvement of DTW score is also discussed in [34] which use vector quantization generated code and fuse these with DTW score for improving the overall results. Use of code vectors generated through vector quantization is advocated in [34]. The score obtained from this code vector is fused with the score obtained through DTW is used for signature verification [34]. The authors in [7] extracted the features through GMM model and used these features with DTW for verification the signatures. Signatures are also used for locking/unlocking of mobile device, so the similar verification process can also be used for mobile devices and the same is used in proposed scheme in [35] which discusses capturing signature by tracking the finger movement instead of a tablet and then applying DTW to signature verification process. Recently, Kinematics based studies are also applied for signature verification, one such case is [2] where DTW is used along with Sigmalog-normal analysis, which is extracted from human kinematics model, for signature verification [2]. In this paper, a scheme based on DTW and a bounded envelope is proposed, such as lower bounding [8]. To the best of our knowledge the said technique is yet to be used for signature verification.

3 Proposed scheme

Two signatures of a person show dissimilarities because of various physical and psychological characteristics. Hence

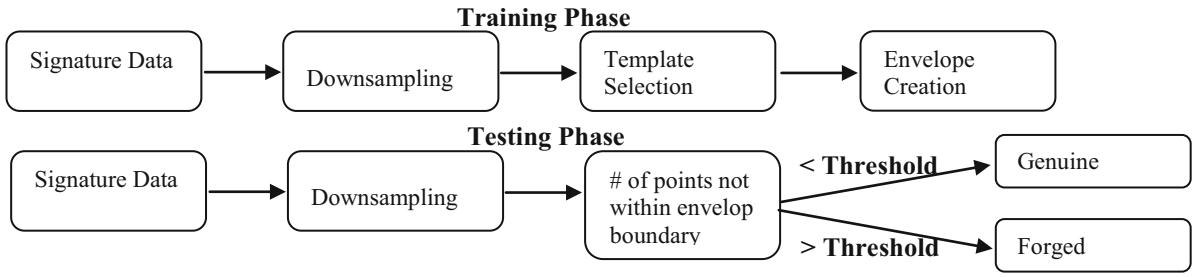


Fig. 2 Architecture of proposed scheme

Table 1 Pseudo code for preprocessing stage of proposed method

Pseudo Code VERSIG

```
//Preprocessing stage
Dataset = read(all_signatures_data);
FOREACHsample in Dataset
sample = down-sample(sample);
FOR EACH x,y coordinates pair in sample
    sample (x,y) =  Centroid(sample(x,y));
END FOR
END FOR
Training_dataset = extract_trainingdata(Dataset);
Testing_dataset = extract_testingdata(Dataset);
```

simple matching algorithms which provide one to one matching of points perform poorly in signature verification. DTW is an elastic matching technique which is used to align two time series signals of different wavelength with each other. Since signatures are obtained through a graphic tablet or other such device in an online signature verification system the signatures are treated as two different time series signals. This makes DTW an ideal choice for designing a solution for this problem [17]. Once the signatures are aligned one need to have a decision boundary for deciding the authenticity of a given signature. This decision boundary is provided by the signature envelop derived from the training signature.

Figure 2 shows a graphical representation of the proposed scheme. First, the signature data obtained from the tablet is down-sampled and centroid of each signal point is calculated which has the characteristics of both X and Y domains. Then a template signature is selected from the training set which exhibits best characteristics of the signature. Cost matrix approach (discussed below) is used for selection of template signature. A signature envelope is created by using DTW of template signature with all the other samples in training set. This envelope creates a decision boundary on the basis of which decision regarding authentic/forged signature is made.

The pseudo code of the proposed scheme is provided in Table 1. *Training_dataset* and *Testing_dataset* both are initialized by applying preprocessing steps as presented in Table 1. Loop iterates over the complete dataset to down-sample the given signature and centroid for each sample point is calculated.*sample(x,y)* holds the centroid of the down-sampled data. Table 2 shows the pseudo code of training phase. In training phase, two phase loop is used where outer loop calculates *dist_matrix* (distance matrix) which calculates the distance of each sample in the *Training_dataset* with all the other samples. The *Template_index* holds the index of the sample which shows minimum distance in the distance vector and is selected as Template signature. Afterwards, the inner loop calculates the *Upper_Boundary(person)* and *Lower_Boundary(person)* of the envelop by using the template signature. The discussion on how these boundaries are formed may please be found in subsequent subsections.

In the testing phase as described in Table 3, each sample of a user is aligned with the template signature. The distance vector is compared to *Upper_Boundary* and *Lower_Boundary* of envelope. The number of points which fall outside the boundary of envelope are counted. If the points exceeds a certain *Allowed_Threshold* then this signature is labeled as Forged, otherwise it is labeled as Authentic. Table 4 provides the information about the notations used in the proposed scheme and the subsequent subsections provide detail of various components of proposed scheme which is an extension of previous scheme proposed by the authors.

Table 2 Pseudocode for training stage of proposed method

```
//TRAINING PHASE//
k = 0;
FOR EACH person in distinct_person(Training_dataset)
  Template_of_person (k) = {};
  Train_sample_person = get_training_Data(person)
FOR i=1 to length(Train_sample_person)
FOR j=1 to length(Train_sample_person)
IF i==j THEN dist_matrix [i,j]= inf;
ELSE
Sample_i = Train_sample_person (i);
Sample_j = Train_sample_person (j);
dist_matrix [i,j]= distance_based_on_DTW((Sample_i, Sample_j);
END IF
    END FOR
Total_distance_of_sample(i) = \sum_{j=1}^{length(Training\_samples\_of\_person)} dist\_matrix[i,:]
END FOR
Template_index = index_of_min_value(Total_distance_of_sample);
  Template_of_person (k) = Train_sample_person(Template_index);
  Template = Template_of_person(k);  TrainSample = Train_sample_person;
[Upper_Boundary(person)] = Upper_Envelope(Template, TrainSample);
  [Lower_Boundary(person)] = Lower_Envelope(Template, TrainSample);
k++;
END FOR
```

Table 3 Pseudocode for testing stage of proposed method

```
//TESTING PHASE//
k = 0;
FOR EACH person in distinct_person(Testing_dataset)
  Test_sample_person = get_testing_Data(person)
FOR i=1 to length(Test_sample_person)
FOR j=1 to length(Test_sample_person)
IF i==j THEN dist_matrix [i,j]= inf;
ELSE
Sample_i = Test_sample_person(i);Sample_j = Template_of_person(person);
dist_vector [i]= DTW((Sample_i, Sample_j);
      END IF
    END FOR
Points_Above_Boundary  =  (dist_matrix[i] >Upper_Boundary(person));
Points_Below_Boundary  =  (dist_matrix[i] <Lower_Boundary(person));
Total_Points_Exceeding = Points_Above_Boundary  + Points_Below_Boundary ;
IF Total_Points_Exceeding>Allowed_Threshold
            THEN Class_predicted = Forged;
ELSE
            Class_predicted = Authentic;
END IF
IF Class_predicted ==actual_class_label (Test_sample_person (i))
THEN Total_Accurate_prediction++;
END IF
Total_Testing_Samples++;
END FOR
k++;
END FOR
Total_Accuracy = Total_Testing_Samples / Total_Accurate_prediction;
```

Table 4 Notation used in the proposed scheme

Abs(x)	This function returns the absolute value of 'x' given as parameter
Mean(x)	This function returns the average value of a vector 'x' containing floating values given as parameter
Centroidcalc(p1,p2)	This represents the centroid value of two points: p1 and p2
Sqrt(x)	Square root of 'x' given as parameter
DTW	Dynamic time warping
dist_vector	Distance vector containing values of difference between two sample vectors after applying DTW
X	A vector containing all the x-coordinate values of a sample signature
Y	A vector containing all the y-coordinate values of a sample signature
Inf	Infinity
distinct_person(Training_dataset)	Number of total distinct persons whose signature data is stored in the training dataset
get_training_Data(person)	Retrieve training data of person (given as parameter) from the database
Template_index	Index of the sample selected as template
Upper envelope	A vector contains maximum points obtained from all the DTW aligned signatures of a person
Lower envelope	A vector contains minimum points obtained from all the DTW aligned signatures of a person

3.1 Down sampling

The dataset Japanese handwritten signature set, used for experimentation purpose, is collected using the tablet which has a resolution of 200 Hz. With this resolution even the smallest signature has points in the range of 2500 × 1400 (2500 points in X dimension and 1400 points in Y dimension). Since DTW is a computationally expensive process, alignment of signatures require a very long processing time. In order to reduce this time, one need to down sample the data. However, on the other hand, down sampling may lead to loss of significant information about the signature. In order to balance both the conditions, each signature in dataset is down-sampled in such a way that every fifth element, in both X and Y dimensions of a signature, is selected. During the experimental testing the authors used both the approaches, i.e., raw data without down sampling and data which is down sampled. The results show that down-sampled approach outperformed the raw data approach not only in terms of execution time but in terms of accuracy as well.

3.2 Centroid selection

The dataset provides information about X and Y coordinates and Pressure. One approach to apply DTW over a signature is to align the signature in X and Y domains separately by assigning weights to each domain and later on combining the score for decision making. The other approach, which is employed in the proposed method, is to take Centroid of a signature on the basis of both the domains. Following equation is used for calculation of Centroid of a signature:-

$$Centroidcalc = abs(sqrt\left((X - mean\,(X)).^2 + Y - mean\,(Y)\right).^2 \tag{2}$$

Figures 3, 4, and 5 shows a signature sample in X domain, Y domain and Centroid of the same signature, respectively. From the figures, it is evident that centroid contain features of both the domains and thus is a better representation of a signature. This approach is used previously by other researchers as well [36].

3.3 Selection of a template signature

The most important task for the proposed method is the selection of a template signature from the given training set. It is well known that two signatures of a person are not similar and shows variations at different points.

Time series signal of two signatures of a same person is shown in Fig. 6. From the figure, it is clear that even the genuine signatures of a person are not always similar. If more samples are collected the signatures show variation on different points making the process more difficult.

The given dataset provide 12 samples of genuine signatures of a person. An ideal template signature would be the one which capture all the important characteristics of a gen-

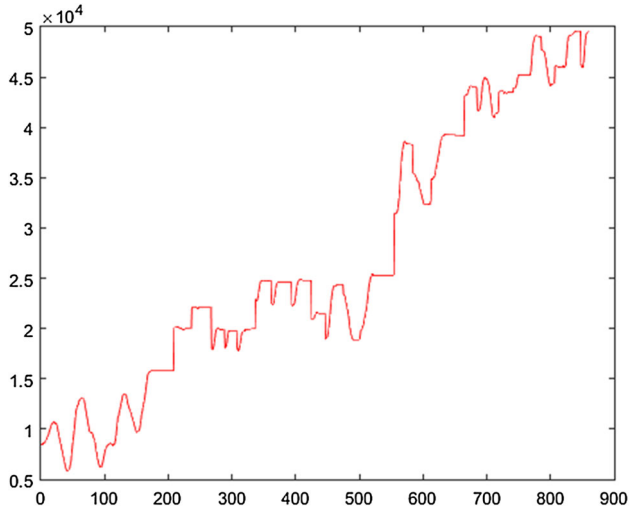


Fig. 3 X Coordinates of signature

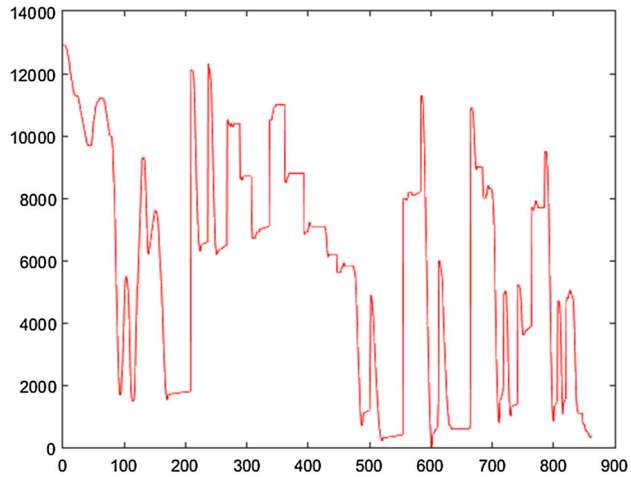


Fig. 4 Y Coordinates of signature

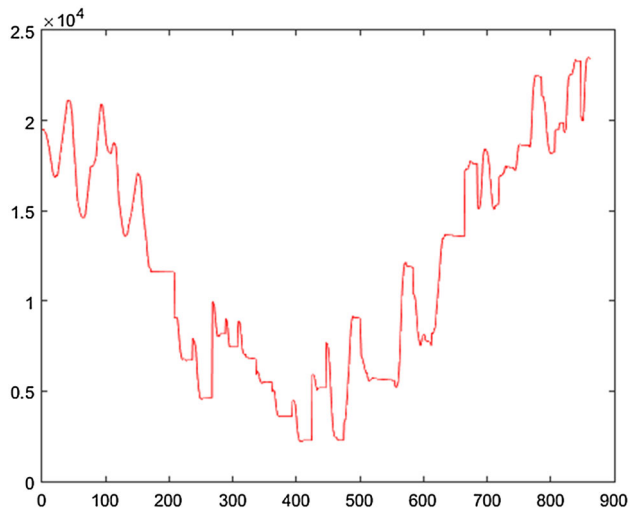


Fig. 5 Centroid of signature

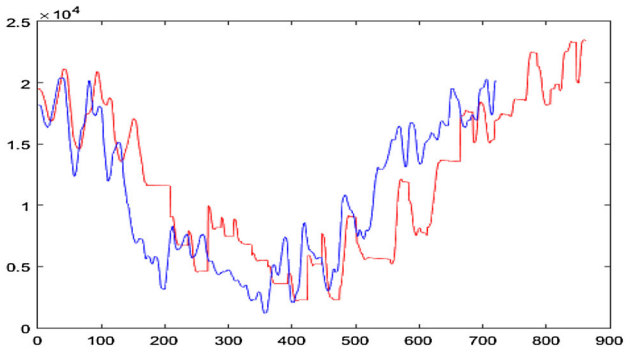


Fig. 6 Two signatures of a person

uine signature. In order to select a template signature a cost matrix based approach is used in the proposed method. In the proposed approach DTW alignment of each signature available in the training set is taken with the rest of the signatures in the dataset effectively creating a 12×12 matrix with dimension. The working of DTW is elaborated in Equation 1. The selected template signature is the one which shows minimum cost across the opposite corners of the matrix. The template signature obtained is used for creation of envelope in the next step.

3.4 Envelope creation

As described in the previous section, two signatures of a same person exhibit variations and in some cases significant variations, due to physical and psychological issues etc. This variation creates difficulties in classification of genuine and forged signatures. The crux of proposed scheme is creation of a generalized envelope which covers all the variations of person's available signatures in the training set.

The envelope is created by aligning the signatures of training dataset with the Template signature. This alignment results in providing 11 equal length vectors providing 11 values at each point of signature. The envelope is created by simply taking the maximum and minimum values of each point, effectively creating a decision boundary which covers all the variations of a signature. All the samples of a person available in the training set falls within this envelope and so this envelope can be used as a decision boundary for forgery detection. Following equations are used for this purpose.

$$Upper\_Boundary\_Envelope\,(x) = \max(x_i, x_{i+1}, \ldots, x_n) \quad for\ i = 1, \ldots, n \tag{3}$$

$$Lower\_Boundary\_Envelope\,(x) = \min(x_i, x_{i+1}, \ldots, x_n) \quad for\ i = 1, \ldots, n \tag{4}$$

where x is set of vectors of all DTW aligned signatures in training set and n is the no. of signatures of each person in the

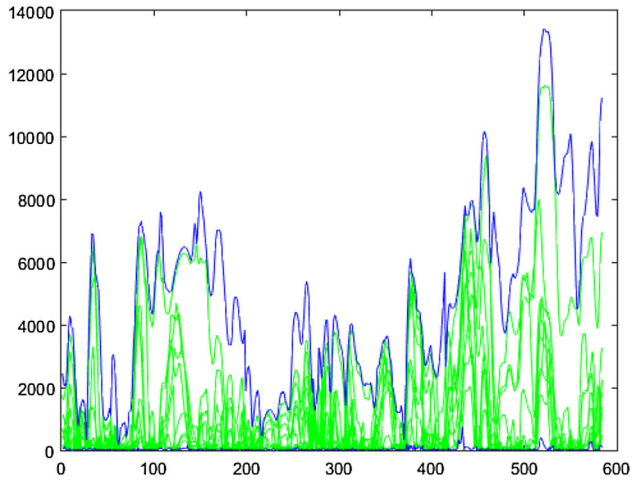


Fig. 7 Creation of signature envelope

training set. An envelope created in such a way is depicted in the Fig. 7.

3.5 Decision criterion

The envelope created in the previous step serve as a basis for decision regarding the authentic/forged signature. However, due to signature variations it is still possible that a genuine signature fall outside the signature envelope which will label a genuine signature as a forged one. To avoid such situation, a threshold value is used in the proposed method which calculates that how many points may be allowed to fall outside the signature envelope. Moreover, the magnitude of this deviation is also calculated. Together with the number of points where the deviation is noticed and the magnitude of deviation, decision regarding authenticity of the signature is made.

Figure 8 show authentic signatures of a person in testing dataset (red lines show signature envelope and blue lines show signatures of the same person in testing dataset). While Fig. 9 shows forged signatures of the same person in testing dataset (red lines show signature envelope and green lines show forged signatures of the same person in testing dataset).

Figures 8 and 9 clearly show that genuine signatures exhibit minor deviations from the envelope whereas forged signatures show a lot of deviation from the envelope.

In a system where user exhibits very minor change in signatures obtained at different times, a very tight envelope can be used where small deviation will lead to conclusion that signature is forged. However, it is observed that there are users which have a large variation at same points even in the training set. Thus a user dependent threshold for decision making can be used. Alternatively, a generalized threshold for all the users can also be used. In this work, a generalized threshold value is used after trial and error method.

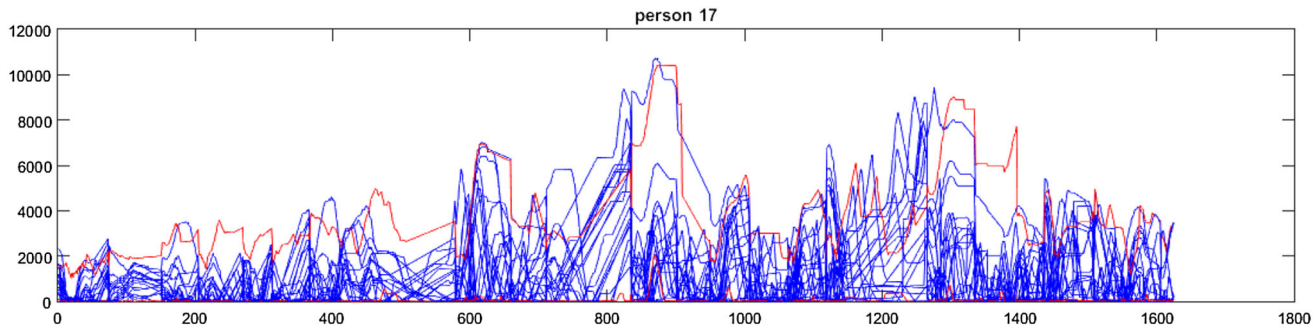


Fig. 8 Authentic signatures in testing dataset

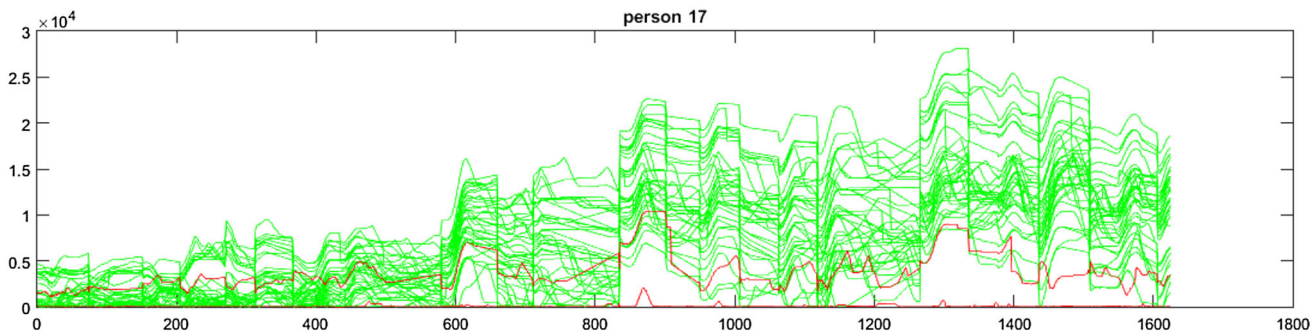


Fig. 9 Forged signatures in testing dataset

Table 5 ICDAR 2013 Japanese signature dataset

No. of users	Genuine samples	Forged samples
Training dataset		
11	462	396
Testing dataset		
20	592	684

4 Dataset

The dataset used for evaluation is a standardized dataset consisting of Japanese signatures and is used for signature verification competition as a part of ICDAR 2013 [37]. Signatures obtained in the dataset are collected by HP Elitebook 2730p tablet PC and collection software developed by Microsoft. Sampling rate of the tablet was 200 Hz. Dataset contained both the training and evaluation sets. 11 persons took part in training set whereas 20 persons took part in evaluation set. The sets provide information about X and Y coordinates and pen up and down values. Training set contained 462 genuine and 396 forged samples whereas evaluation set contained 592 genuine and 684 forged samples. Dataset contained samples of random forgery, where the forger have no information about the original signature of a person, and skilled forgery where the forger had seen the original signature of the person. The information regarding dataset is given in Table 5.

4.1 Results and discussion

Qatar University [37] submitted an online signature verification in ICDAR 2013 competition which used X and Y coordinates, Pressure, Directions, Angles, Speed and Angular speed features for verification at signal level. Moreover, it also computed histogram of reference and signature in question, for verification process.

Sabanciuniversity submitted two DTW based systems. First one used features such as X and Y coordinates, curvature difference between two coordinates and pressure [24]. Second system submitted by the same university [37] used DTW and all the features of previous system except Pressure information. The later system performed better then the former one showing that Pressure information is not a significant feature to be used.

Various schemes have been proposed for online signature verification which provides different accuracy results. However, the results are not only dependent on type of method the scheme used but more importantly dataset they use.

Since the proposed scheme used ICDAR 2013 signature dataset which consist of Japanese signatures. It is only logical to evaluate the schemes which used the same dataset. The results are summarized in Table 6 and it is evident from the table that the results obtained from proposed approach are best among the schemes which used the same dataset.

Table 6 Results of approaches used ICDAR 2013 subset

Approach proposed by	Method used	Accuracy	FAR	FRR
Qatar University [37]	Histogram level features	70.55	29.56	30.22
Sabanci University [37]	DTW	72.55	27.56	27.36
Sabanci University [37]	DTW	72.47	27.56	27.50
Usman et al. [38]	DWT and Fourier transform	73.49	27.48	25.54
Madiha et al. [33]	Euclidean distance and DTW	78.57	28.22	16.06
Proposed approach	DTW	79.80	27.35	15.18

5 Conclusion and future work

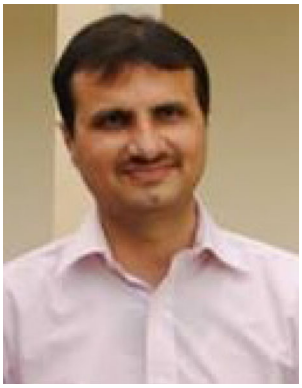
A novel online signature verification scheme is proposed which is based on selecting an ideal template through DTW and then creation of a signature envelope which can be effectively used for forgery detection. The proposed scheme is evaluated on Japanese signature dataset, compared with other schemes which used the similar dataset, and showed promising results. It is planned to implement the same scheme on other well known signature verification datasets to evaluate the accuracy of the scheme. Moreover, it is intended to create a user dependent threshold for each user which will improve the overall results of the scheme.

References

1. Iranmanesh, V., et al.: Online handwritten signature verification using neural network classifier based on principal component analysis. Sci. World J. (2014). doi:10.1155/2014/381469
2. Fischer, A., Plamondon, R.: Signature verification based on the kinematic theory of rapid human movements. IEEE Trans. Human Mach. Syst. **47**(2), 169–180 (2017)
3. Plamondon, R., Lorette, G.: Automatic signature verification and writer identification–the state of the art. Pattern Recognit. **22**(2), 107–131 (1989)
4. Feng, H., ChoongWah, C.: Online signature verification using a new extreme points warping technique. Pattern Recognit. Lett. **24**(16), 2943–2951 (2003)
5. Richiardi, J., Ketabdar, H., Drygajlo, A.: Local and global feature selection for on-line signature verification. In: 2005 Proceedings Eighth International Conference on Document Analysis and Recognition. IEEE (2005)
6. Muramatsu, D., Matsumoto, T.: An HMM online signature verifier incorporating signature trajectories. In: 2003 Proceedings Seventh

International Conference on Document Analysis and Recognition. IEEE (2003)
7. Diaz, M., et al.: Dynamic signature verification system based on one real signature. In: IEEE Transactions on Cybernetics (2016)
8. Keogh, E.: Exact indexing of dynamic time warping. In: Proceedings of the 28th International Conference on Very Large Data Bases. VLDB Endowment (2002)
9. Mueen, A., Keogh, E.: Extracting optimal performance from dynamic time warping. In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM (2016)
10. Leclerc, F., Plamondon, R.: Automatic signature verification: the state of the art—1989–1993. Int. J. Pattern Recognit. Artif. Intell. **8**(03), 643–660 (1994)
11. Impedovo, D., Pirlo, G.: Automatic signature verification: the state of the art. IEEE Trans. Syst. Man Cybern. Part C **28**(5), 609–635 (2008)
12. Mohammed, R.A., et al.: State-of-the-art in handwritten signature verification system. In: 2015 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE (2015)
13. Plamondon, R., Srihari, S.N.: Online and off-line handwriting recognition: a comprehensive survey. IEEE Trans. Pattern Anal. Mach. Intell. **22**(1), 63–84 (2000)
14. Bashir, M., Kempf, J.: Area bound dynamic time warping based fast and accurate person authentication using a biometric pen. Digit. Signal Process. **23**(1), 259–267 (2013)
15. Kholmatov, A., Yanikoglu, B.: Identity authentication using improved online signature verification method. Pattern Recognit. Lett. **26**(15), 2400–2408 (2005)
16. Guru, D.S., Prakash, H.N.: Online signature verification and recognition: an approach based on symbolic representation. IEEE Trans. Pattern Anal. Mach. Intell. **31**(6), 1059–1073 (2009)
17. Qiao, Y., Wang, X., Xu, C.: Learning Mahalanobis distance for DTW based online signature verification. In: 2011 IEEE International Conference on Information and Automation (ICIA). IEEE (2011)
18. Gruber, C., et al.: Online signature verification with support vector machines based on LCSS kernel functions. IEEE Trans. Syst. Man Cybern. Part B **40**(4), 1088–1100 (2010)
19. Fierrez, J., et al.: HMM-based on-line signature verification: feature extraction and signature modeling. Pattern Recognit. Lett. **28**(16), 2325–2334 (2007)
20. Richiardi, J., Drygajlo, A.: Gaussian mixture models for on-line signature verification. In: Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications. ACM (2003)
21. Sharma, A., Sundaram, S.: A novel online signature verification system based on GMM features in a DTW framework. IEEE Trans. Inf. Forensics Secur. **12**(3), 705–718 (2017)
22. Fauziyah, S., et al.: Signature verification system using support vector machine. In: 2009 ISMA'09 6th International Symposium on Mechatronics and its Applications. IEEE (2009)
23. Nanni, L., Lumini, A.: A novel local on-line signature verification system. Pattern Recognit. Lett. **29**(5), 559–568 (2008)
24. Yanikoglu, B., Kholmatov, A.: Online signature verification using Fourier descriptors. EURASIP J. Adv. Signal Process. **2009**, 12–24 (2009)
25. Rashidi, S., Fallah, A., Towhidkhah, F.: Feature extraction based DCT on dynamic signature verification. Sci. Iran. **19**(6), 1810–1819(2012)
26. Arora, M., Singh, K., Mander, G.: Discrete fractional cosine transform based online handwritten signature verification. In: 2014 Recent Advances in Engineering and Computational Sciences (RAECS). IEEE (2014)
27. Manjunatha, K.S., et al.: Online signature verification based on writer dependent features and classifiers. Pattern Recognit. Lett. **80**, 129–136 (2016)
28. Mlaba, A.S.P., Gwetu, M.V., Viriri, S.: A distance-based approach to modelling reference signature for verification. In: Conference on Information Communication Technology and Society (ICTAS). IEEE (2017)
29. Rashidi, S., Fallah, A., Towhidkhah, F.: Similarity evaluation of online signatures based on modified dynamic time warping. Appl. Artif. Intell. **27**(7), 599–617 (2013)
30. Ding, L., et al.: Based on EADTW on-line handwriting signature handwriting signature verification system design and implementation. In: Applied Mechanics and Materials. Vol. 556. Trans Tech Publications, Zurich (2014)
31. Giuseppe, P., et al.: Multidomain verification of dynamic signatures using local stability analysis. IEEE Trans. Human Mach. Syst. **45**(6), 805–810 (2015)
32. Fischer, A., et al.: Robust score normalization for dtw-based online signature verification. In: 2015 13th International Conference on Document Analysis and Recognition (ICDAR). IEEE (2015)
33. Tahir, M., Akram, M.U., Idris, M.A.: Online signature verification using segmented local features. In: 2016 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube). IEEE (2016)
34. Sharma, A., Sundaram, S.: An enhanced contextual DTW based system for online signature verification using vector quantization. Pattern Recognit. Lett. **84**, 22–28 (2016)
35. Fang, Y., et al.: A novel video-based system for in-air signature verification. Comput. Electr. Eng. **57**, 1–14 (2017)
36. Muramatsu, D., Matsumoto, T.: Effectiveness of pen pressure, azimuth, and altitude features for online signature verification. Adv. Biom. 503–512 (2007)
37. Malik, M.I., et al.: ICDAR 2013 competitions on signature verification and writer identification for on-and offline skilled forgeries (SigWiComp 2013). In: 2013 12th International Conference on Document Analysis and Recognition (ICDAR). IEEE (2013)
38. Tahir, M., Akram, M.U.: Online signature verification using hybrid features. In: 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec). IEEE 2015

Mehr Yahya Durrani is serving as Assistant Professor at COMSATS Institute of Information Technology, Pakistan. He graduated in the field of information Technology and later received Masters degree in Computer Science. Currently, he is pursuing Doctorate in the field of Pattern Recognition.



Salabat Khan received his Doctorate from National University FAST Pakistan. He is currently working as Assistant Professor at COMSATS Institute of Information Technology, Pakistan. His areas of expertise include Machine Learning, Data Mining and Evolutionary Computing. He has contributed more than 20 research articles in international journals.

Shehzad Khalid is a Professor and Head of Department at Department of Computer Engineering, Bahria University, Pakistan. He is a qualified academician and researcher with more than 200 international publications in conferences and journals. Dr. Shehzad has graduated from Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Pakistan, in 2000. He received the M. Sc. degree from National University of Science and Technology, Pakistan in 2003 and the Ph.D. degree from the University of Manchester, U.K., in 2009.