J. Appl. Environ. Biol. Sci., 4(9S)303-308, 2014

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Online Signature Verification: A Review

Jawad-ur-Rehman Chughtai, Dr. Shehzad Khalid, Dr. Imran Siddiqi

Department of Computer Engineering Bahria University

Received: September 12, 2014
Accepted: November 23, 2014

ABSTRACT

From the last few decades, online signature verification (OSV) has become a hot research topic and have been employed in many application areas such as banking, law enforcement, industry, and security control etc. The growing security needs of today's society exert a pull on researchers to work in this area. A number of techniques along with their variations have been proposed in the realization of a fool proof & reliable signature verification system. Dynamic Time Warping (DTW), Hidden Markov Model (HMM), Support Vector Machine (SVM) and Neural Networks (NN) are the most promising approaches amongst the others. In this paper, we have presented a review of research carried out in recent past in the field of online signature verification and made a qualitative analysis of these state-of-the-art approaches.
KEYWORDS*:* Biometrics, Online Signature Verification, DTW, HMM, SVM, NN, Forgery

1 INTRODUCTION

Today's society demands secure means for person's authentication. Traditional authentication methods are based on the knowledge (password, Personal Identification Number) or on the possession of a token (Identification card, keys), which can be forgotten or stolen. This fact makes biometrics to take its place as an alternative method for person's authentication and identification. Besides many other verification methods like fingerprints, iris, etc. Signature verification, a behavioral trait is one of the promising way to authenticate a person's identity. This paper is focus on the qualitative study about the signature verification techniques.

The term biometrics refers to an individual's recognition based on personal distinctive characteristics. Two types of biometrics can be defined by taking into account the personal traits which are physical or behavioral. The physical are about catering the biological traits of users, for instance, fingerprint, face, hand geometry, retina, and iris. The latter takes into account the behavioral traits of users, such as voice or handwritten signature. Biometric system is an advanced method to induce security and is mainly employed for personal authentication. Handwritten signature comes into sight as the most socially undertaken and renowned method for individual verification among all other existing biometric authentication systems [14].

A signature is a handwritten depiction of someone's name or some other mark of identification that a person writes on documents or a device as a proof of identification. The formation of signature varies from person to person or even from the same person due to physical & mental condition at that time, geographical location, age and other factors. The primary focus of a signature verification system is the detection of forged and imitated signatures (variations) generated by imposters, for instance, unskilled and skilled forgery. The intention behind signature verification systems is to minimize the false acceptance rate (FAR) and false rejection rate (FRR) but the two terms are inversely proportional.

Signature verification can be viewed as offline or static signature verification & online or dynamic signature verification from data acquisition standpoint. In offline signature verification, signatures are recorded as images on paper which can later on be transformed into computer by means of a scanner and processed using offline verification stages. Offline signature verification is carried out on static features like shape, style variation, distortion, rotation variation, etc. on the other hand, Online signature verification makes use of dynamic features e.g. pressure, velocity ,stroke length, pen up/down time, etc. along with the shape of the signature [12].One of the key requirement of a verification system i.e. accuracy, can be achieved with greater precision due to the availability of dynamic information in online signature verification system as compared to offline signature verification systems. OSV is accepted far and wide by the communities for verification purposes as its more secure method than already available methods in use. It's difficult for imposters to copy all attributes (speed, pressure) along with the shape as it's present in the genuine signature [7]. Due to the increasing popularity of the input capturing devices e.g. tablets, PDA's

*** Corresponding Author:** Jawad-ur-Rehman Chughtai, Department of Computer Engineering Bahria University. jawadchughtai@gmail.com

etc., data acquisition in OSV is no more a major problem. That's also one of the reason which attracted the researchers to work in this area.

Worldwide acceptance of mobile devices these days apparently challenges the future of online handwritten signature verification. A very little research is reported in this area up till now [25], [13]. Researchers are now shifting their focus towards the security of mobile applications to address the challenges reported so far e.g. signing in different context (sitting or standing, holding the mobile at various angles and orientations etc.).

A wide range of techniques and methods have been proposed for the implementation of robust online signature verification systems to date. The most renowned approaches found in literature are Dynamic Time Warping (DTW) [17],[18],[12],[1],[22],[3],[19], Hidden Markov Model (HMM) [10],[26],[24], Neural Networks (NN) [6],[7],[5],[4], and Support Vector Machine (SVM) [9],[11],[16]. Starting with an introduction about phases of a typical online signature verification system as a whole, and continues with a comparison of benefits and shortcomings of the most renowned signature verification techniques and their performance evaluation, rounded up by a conclusion and future directions. More specifically, Section II shed lights on the typical steps followed by an online signature verification system and gives a brief introduction of these steps. Section III highlights the verification approaches followed by their pros and cons in Section IV. Section V outlines the system's performance evaluation for online signature verification stated in recent literature. An insight on the most promising future research directions are reported in Section VI, followed by the conclusions of this paper at the end.

2. STEPS IN ONLINE SIGNATURE VERIFICATION

A typical online signature verification system follows the phases of data acquisition, preprocessing, feature extraction, and classification (training and verification), as shown in Fig. 1. However some researchers ignored preprocessing phase in order to keep the temporal information as shown in a recent research [2].

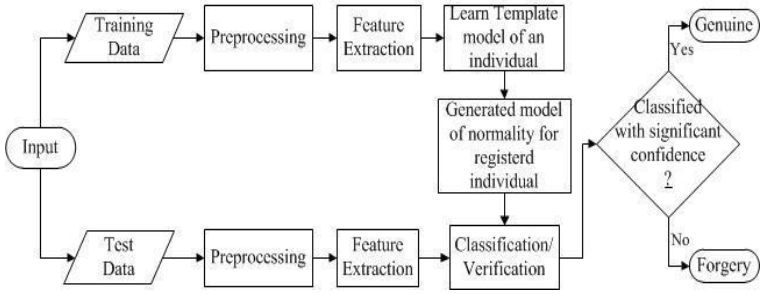

Figure 1:Phases of an online signature verification system

2.1. Data acquisition. The signature to be processed by an online signature verification system comes from either some freely available database (e.g. SVC2004, MCYT, etc.) or recorded by means of any electronic device (e.g. digitizing tablets, PDAs, smart-phones, data glove, etc.).

2.2. Preprocessing Since, the training and testing signatures may contain noise & length variability, there is a need to preprocess these signatures before moving to next stages. The degree of signature's preprocessing needs to be carefully done. Preprocessing is performed in such a way that the signature temporal information, endpoints of strokes and points where the signature trajectory changes are not affected. Noise and additional jerks in the signatures are removed as well if necessary.

2.3. Feature Extraction. One of the most important processes in signature verification is feature extraction. Since, the data in online signature verification is represented as a series of points, features are extracted from a sequence of points. After preprocessing, features such as x & y coordinates, pen status, pressure etc. are extracted from the input signatures for each segment. New features such as velocity of x (vx) and velocity of y (vy) etc. can be derived from these signatures. The features that are not reverse engineered by any imposter, & maximize the interpersonal variability and minimizes the intrapersonal variability, need to be selected and saved in the database as reference signature along with the calculated threshold value.

2.4. Classification. After the preprocessing and feature extraction phase, a comparison between the features of test and genuine/trained signature is carried out, and a decision on the basis of

acceptance/rejection criteria (threshold value) is made as genuine or forged. Some of the most relevant approaches to online signature verification are shown in Fig. 2.

3. METHODS FOR ONLINE SIGNATURE VERIFICATION

3.1. Dynamic Time Warping. Dynamic Time Warping is the most popular & commonly used template matching approach for conducting online signature verification. DTW takes two signature sequences as input and find out the optimal matches (similarity) in those sequences. It can efficiently determine the most optimal distance between the given sequences even if there is a variation in the signature's length in time. Dynamic programming strategy is used in DTW to handle length variability [19]. The capability of fast similarity computation takes DTW at the top in the hierarchy of signature verification approaches. One of the characteristic that DTW exhibit is that it does not requires large amount of training data. However, the problem with DTW is its time complexity, which is O (n2) where n represents the number of points of a signature sequence. VQ-DTW, a variation of DTW is introduced to speed up DTW computations where Vector Quantization has the ability to group together the points that lies within the same region hence, trimming down algorithmic time complexity [8]. A recent approach called Area bound dynamic time warping (AB_DTW) to speed up DTW computations has been reported in the literature [3].

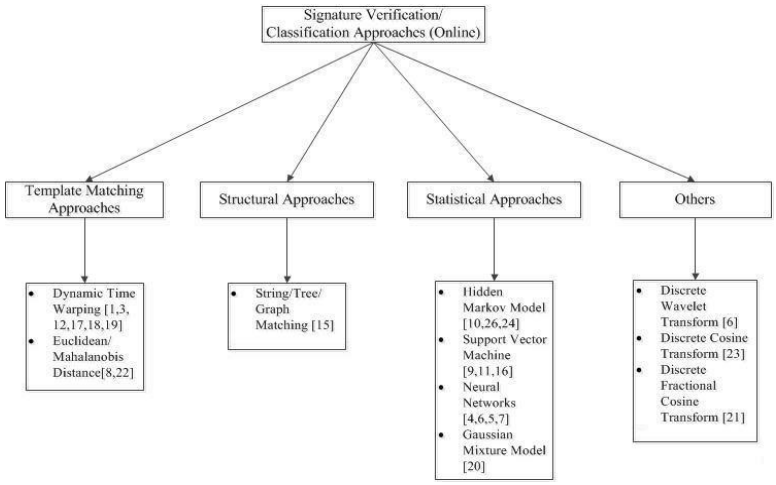

Figure 2: Signature verification approaches

3.2. Hidden Markov Model. HMMs have been used in a multitude of application areas such as signal processing, speech recognition, pattern recognition and is successfully implemented in signature verification as well. HMM is an effective statistical modeling approach in which an observable sequence is generated by the underlying process. HMM, a generalization of Markov Model is a robust method for modeling the variability of distinct time random signals if the time information is accessible [10]. Since, HMM can handle time duration signals variation, for instance, signatures speech etc., it is prominent for signature and speech recognition applications [8]. In HMM, the division of signing process into multiple states is made that makes up a Markov chain. A sequence of probability distributions of the different features are taken that are implied in the verification task and matching is performed on it. Signature's likelihood is the measure used in these verification systems to determine the verification score which is then normalized to get a threshold value. It shows whether a given signature (test) is genuine or forged [24]. The model using HMM in signature verification consist of States (genuine or forged) and Observations (x, y coordinates, pressure etc.). The drawback of applying HMM in signature verification is that it needs huge features to be set in huge number. Also, the amount of data in training the model is very large thus resulting in a very high time complexity.

3.3. Neural Networks. Neural network is a supervised statistical modeling approach that can learn from the training samples and solve number of problems (e.g. pattern recognition) based on that information. [7] In signature verification, the model learns using a number of genuine and forged signatures which are stored in the database and test signature is judged as genuine or forged. To identify the variation in the test signature, NN is trained to learn weights in accordance with the reference signature. NN is used in prior

research because of its ability to generalize but the major shortcoming of using NN in online signature verification is that it needs a lot of time while training the model [6]. Neural Network is used as follows in modeling of a signature verification system: In the training phase, a vector of n number of sensors is used where n is the number of features of the signature taken for verification. The training is conducted using Back-propagation algorithm. The similarity of the target feature with respect to genuine signature sample's feature is predicted by means of these vectors. A multilayer feed forward neural network is used for the purpose which contains n number of input units, one output unit revealing genuine or forged, and some units in one or more hidden layer(s).

3.4. Support Vector Machine. Support vector machines are supervised learning models whose foundations stem from statistical learning theory. The support vector machine works by using a set of data sample as input. Then, it predicts the associated output class for each input sample that makes it a non-probabilistic binary linear classifier. SVM has been considered a good choice for solving the signature verification problem as it is frequently used for pattern recognition applications, classification and regression problems [11]. An SVM maximally separates hyper plane that determines clusters by mapping input vectors to a higher dimensional space [16]. An SVM takes a set of input data and determines to which of the two classes the input data belongs.

3.5. Others. Discrete Wavelet Transform [6] and Discrete Cosine Transform [23], [21] are also reported as promising verification approaches in past. DWT coefficients of user genuine signatures that are mostly similar are chosen as candidates for signature authentication features [6]. The advantage of using the DCT is the ability to compactly represent an online signature using a fixed number of coefficients, which leads to fast matching algorithms [23]. Gaussian Mixture Model is another mature statistical model, and is used in similarity measurement of signatures found in [20]. A new method of online signature verification is proposed in [15], which employed graph representation of data along with graph matching techniques. Two types of graph representation for on-line signatures were presented, and a sub-optimal graph matching algorithm is used to compute the distance between graphs.

4. COMPARISON OF THE APPROACHES

In this section, we are presenting the approaches discussed in sections III-A, III-B, III-C and III-D.

4.1. Benefits & Shortcomings of Approaches. DTW is employed to estimate the similarity or dissimilarity between two time varying sequences which have intra-individual variations [3]. If the number of sample data is very large then DTW becomes computationally expensive. Hence, to speed up computations DTW can be employed with slight variation such as area bound DTW (AB_DTW) [3], VQ_DTW [8]. The variation in the signature due to, weather condition, emotional condition etc. and can be addressed using DTW. DTW uses dynamic programming algorithm to find out the similarity between two sequences of sample signature.

Hidden Markov model are the most popular statistical methods applied in signature verification. An HMM is a double stochastic process in which one unobservable state can be predicted through a set of observations. Many topologies are used in implementing HMM; the most frequently used is left-to-right HMM [10].

Support Vector Machine is another major statistical approach found in online signature verification that uses kernel functions to find out the resemblance and similarity of two sample sets [11]. Besides these, Neural Network approaches, MLP networks in particular, are widely used in online signature verification systems because it is very simple to train them, very fast to use in pattern recognition and achieves high recognition rate [7].

5. PERFORMANCE EVALUATION WITH RESULTS

The performance of biometric verification systems is usually expressed in terms of False Acceptance Rate (FAR) and False Rejection Rate (FRR). A false acceptance occurs when a forger's sign/invalid user is approved by the system & a false rejection occurs when a genuine sign/valid user is rejected by the system. Both FAR & FRR are related to each other so that a variation in one of the rates will have an inverse effect on the other. Another alternative used commonly to evaluate the system's performance is to compute the equal error rate (EER). The performances of various techniques with results are shown in Table I

Table 1: PERFORMANCE EVALUATION OF VARIOUS METHODS

S.No	Method	Performance EER%
1	Dynamic Time Warping[22]	3.71
2	Hidden Markov Model[24]	2.27, 3.07
3	MLP-NN[7]	3.0
4	DCT-Parzen Window[23]	3.61, 2.04 1.49
5	SVM-LCSS[11]	6.84
6	Graph Edit Distance[15]	5.80, 2.46

6. CONCLUSION AND OUR INSIGHTS

An online signature is a consequence of complex psychological procedure due to certain factors such as mood, environment, etc. and hence it's not easy as pie to measure it with the help of any approach therefore, it is imperative to uncover the most optimal technique that caters the distinctive features of a signature and employ it for an individual's verification. This paper gives an overview of the most popular state-of-the-art techniques used in online signature verification. The pros and cons of these techniques are presented which gives an approximation of the best method used in a particular scenario. The most commonly used approaches are similarity finding by Dynamic Warping and Hidden Markov Model. Dynamic warping approaches give a flexible matching of the local features while HMM performs stochastic matching of a model and a signature using a sequence of probability distributions of the features along the signature.

J. kempf's [3] work can be extended to multivariate time series to achieve promising results. Since, there exist more than hundred features, it is still an open question that what are the best features selected together to achieve greater verification accuracy. Also, with the increasing popularity and social acceptance of smart-phones, security challenges open up new ways of research [13], [5], and [4]. We expect our finding will broaden the concept of online signature verification results in recommendation for devising new methods specifically for handling smart-phone's challenges and open up new directions for the researchers.

REFERENCES

1. H. Lim A. G. Reza and Md. J. Alam. "an efficient online signature verification scheme using dynamic pro-gramming of string matching". In Proceedings of the 5th International Conference on Convergence and Hy-brid Information Technology, ICHIT 11, pages 590–597, 2011.
2. S. RohillaandA. Sharma and R.K. Singla. "online signature verification at sub-trajectory level". In Ad-vanced Computing, Networking and Informatics- Volume 2, volume 28, pages 369–374. Springer International Publishing, 2014.
3. M. Bashir and J. Kempf. "area bound dynamic time warping based fast and accurate person authentication using a biometric pen". Digital Signal Processing, 23 (1):259 – 267, 2013.
4. K. Cpalka and M. Zalasinski. "online signature verifica-tion using vertical signature partitioning". Expert Systems with Applications, 41(9):4170 – 4180, 2014.
5. K. Cpalka, M. Zalasinski, and L. Rutkowski. "new method for the online signature verification based on horizontal partitioning". Pattern Recognition, 47(8):2652 – 2661, 2014.
6. M. Maged M. Fahmy. "online handwritten signature verification system based on dwt features extraction and neural network classification ". Ain Shams Engineering Journal, 1(1):59 – 70, 2010.
7. A. Fallah, M. Jamaati, and A. Soleamani. "a new online signature verification system based on combining mellin transform, mfcc and neural network ". Digital Signal Processing, 21(2):404 – 416, 2011.
8. M. Faundez-Zanuy. "online signature recognition based on vq-dtw". Pattern Recognition, 40(3):981 – 992, 2007.

9. S. Fauziyah, O. Azlina, B. Mardiana, A. M. Zahariah, and H. Haroon. "signature verification system using support vector machine". In 6th International Symposium on Mechatronics and its Applications, 2009, pages 1–4, Mar 2009.
10. J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez. "hmm-based on-line signature verification: Feature extraction and signature modeling". Pattern Recognition Letters, 28(16):2325 – 2334, 2007.
11. C. Gruber, T. Gruber, S. Krinninger, and B. Sick. "online signature verification with support vector machines based on lcss kernel functions". Trans. Sys. Man Cyber. Part B, 40(4):1088–1100, Aug 2010.
12. Z. Gingl H. Bunke, J. Csirik and E. Griechisch. "online signature verification method based on the acceleration signals of handwriting samples". In CIARP 2011, volume 7042, pages 499–506. 2011.
13. N. Houmani, S. Garcia-Salicetti, B. Dorizzi, and M. El-Yacoubi. "online signature verification on a mobile platform". In Mobile Computing, Applications, and Services, volume 76, pages 396–400. Springer Berlin Heidelberg, 2012.
14. V. Govindaraju K. W. Boyer and N. K. Ratha. "introduc-tion to the special issue on recent advances in biometric systems". Trans. Sys. Man Cyber., 37(5):1091–1095, Oct 2007.
15. Z. Zhang K. Wang, Y. Wang. "online signature verifica-tion using graph representation". In Sixth International Conference on Image and Graphics (ICIG), 2011, pages 943–948, Aug 2011.
16. B. Kar and P. K. Dutta. "svm based signature verification by fusing global and functional features". International Journal of Computer Applications, 60(16):34–39, Dec 2012.
17. M. Khalil, M. Moustafa, and M. H. Abbas. "enhanceddtw based on-line signature verification". In Proceedings of the 16th IEEE International Conference on Image Processing, pages 2685–2688, 2009.
18. D.lLemire. "faster retrieval with a two-pass dynamic-time-warping lower bound ". Pattern Recognition, 42(9): 2169 – 2180, 2009.
19. M. G. Lopez, R. L. Ramos., O. H. Miguel, and E. N. Canto. "embedded system for biometric online signature verification". 10(1):491–501, Feb 2014.
20. M. Lopez-Garcia, R. Ramos-Lara, O. Miguel-Hurtado, and E. Canto-Navarro. "embedded system for biometric online signature verification". IEEE Transactions on Industrial Informatics,, 10(1):491–501, 2014.
21. M.Arora, K. Singh, and G. Mander. "discrete fractional cosine transform based online handwritten signature ver-ification". In Recent Advances in Engineering and Com-putational Sciences (RAECS), 2014, pages 1–6, March 2014.
22. Y. Qiao, Wang Xingxing, and C. Xu. "learningmaha-lanobis distance for dtw based online signature verifica-tion". In IEEE International Conference on Information and Automation (ICIA),, pages 333–338, June 2011.
23. S. Rashidi, A. Fallah, and F. Towhidkhah. "feature extraction based dct on dynamic signature verification ". ScientiaIranica, 19(6):1810 – 1819, 2012.
24. E. A. Rua and J.L.A. Castro. "online signature verifi-cation based on generative models". 42(4):1231–1242, Aug 2012.
25. N. Sae-Bae and N. Memon. "online signature verification on mobile devices". 9(6):933–947, June 2014. L. Zhang J. Zheng and E. Zhan. "online handwriting signature verification based on parameters optimization of hmm". In 2nd International Conference on Informa-tion Engineering and Computer Science (ICIECS), 2010, pages 1–4, Dec 2010.