J. Appl. Environ. Biol. Sci., 4(9S)342-347, 2014

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

A Review of Offline Signature Verification Techniques

Muhammad Nazakat, Dr. Shehzad Khalid, Dr. Imran Siddiqi

Department of Computer Engineering Bahria University

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

ABSTRACT

Among various biometric modalities, signature verification remains one of the most widely used methods to authenticate the identity of an individual. Signature verification, the most important component of behavioral biometrics, has attracted significant research attention over the last three decades. Despite extensive research, the problem still remains open to research due to the variety of challenges it offers. The high intra-class variations in signatures resulting from different physical or mental states of the signer, the differences that appear with aging and the visual similarity in case of skilled forgeries etc. are only a few of the challenges to name. This paper is intended to provide a review of the recent advancements in offline signature verification with a discussion on different types of forgeries, the features that have been investigated for this problem and the classifiers employed. The pros and cons of notable recent contributions to this problem have also been presented along with a discussion of potential future research directions on this subject.

KEYWORDS*:* Behavioral Biometrics, Signature Verification, Forgeries, False Rejection Rate, False Acceptance Rate, Feature Extraction, Classification

1 INTRODUCTION

The security requirements in today's world have placed biometrics at the center of an ongoing debate concerning its key role in a multitude of applications. Biometrics measures individuals' unique physical or behavioral characteristics with the aim of recognizing or authenticating the claimed identity. Physical biometrics includes modalities like fingerprints, retina, iris, DNA and facial patterns etc. Behavioral biometrics, on the other hand, exploits the behavioral characteristics of an individual like signature, voice, keystroke pattern or gait etc. to determine the identity. These diverse biometric modalities have received significant research attention of the pattern classification community over the last three decades and mature verification/authentication systems are available for modalities like face, iris, voice and signature etc. Among these diverse biometric verification modes, signature verification is undoubtedly the most wide used and accepted attribute for identity verification and is also the subject of our study. Despite significant research, the problem of signature verification remains open due to the wide diversity of challenges it offers. This paper is intended to provide a review of the recent signature verification techniques proposed in the literature along with the pros and cons of each and a comparative overview in terms of performance. The paper also summarizes the types of forgeries and the general steps involved in verification of signatures.

Handwritten signature verification is simple, secure, cheap and acceptable all over the world. It is frequently employed to approve the transfer of resources of millions of people in the form of bank checks, credit card payments and other financial documents. Other official and legal documents requiring signatures can also be validated using signature verification techniques [15]. Signature verification, like all other pattern classification problems, is typically categorized into traditional phases of preprocessing, feature extraction and classification. Among different problem scenarios offered by signature verification, discriminating a sample of genuine signature from a skilled forgery is known to be the most challenging task. This paper reviews the signature verification problem from different perspectives. We first present the categories of signature verification from the view point of data acquisition followed by a discussion on the common types of forgeries. We then present a general discussion on the phases of preprocessing, feature extraction and classification steps in a signature verification system followed by a review of some recent and significant research contributions to this problem. Finally, we conclude our discussion summarizing potential research directions on this subject.

* **Corresponding Author:** Muhammad Nazakat, Department of Computer Engineering Bahria University. jawadchughtai@gmail.com

2. TYPES OF SIGNATURE VERIFICATION

As a function of data acquisition, signature verification techniques are categorized into two classes – online and offline. In online verification systems, signature data is obtained from an electronic tablet which, in addition to the signature shape, also captures the dynamic information like pressure, velocity and number/order of strokes etc. Offline signature verification relies on digitized images of signatures generated by scanning or photographing a paper based signature. Since offline signatures only capture the shape and lack dynamic information, they are generally considered less informative as opposed to online signatures and hence their verification is relatively more difficult. A major proportion of signature encountered in the real world, however, are offline.

3. TYPES OF FORGERIES

This section presents the different types of forgeries encountered in signature verification problems. Traditionally, forgeries are categorized into three groups as listed in the following

3.1. Skilled Forgery. Skilled forgery includes imitating the original signature and is the most difficult type of forgery to detect. The forger has knowledge of the original signature and attempts to imitate the original signature after several practice sessions.

3.2. Random Forgery. Random forgery refers to the scenario where the forger has no knowledge about the name or signature of the original signer and randomly generates a signature pretending to be the original signer.

3.3. Casual Forgery. In casual forgeries, the forger has knowledge of the name but not of the signature of the original signer. The forger attempts to generate a random signature using the name of the original signer.

An ideal signature verification should be able to handle skilled forgeries and at the minimum any signature verification system must at least detect random forgeries [21].

After having discussed the types of forgeries, we present the general steps involved in an offline signature verification system in the following section.

4. OFFLINE SIGNATURE VERIFICATION STEPS:

As discussed earlier, signature verification comprises the three traditional phases of preprocessing, feature extraction and classification. A general discussion on each of these steps with respect to verification problem is presented in the following while an overview of the process is illustrated in Figure 1.

4.1 Preprocessing. Preprocessing is carried out to convert the raw images to a standard form appropriate for the next phase of feature extraction [20]. Depending upon the type of signatures encountered in an application, preprocessing may involve one or more of the following steps.

Size Normalization: As a function of the features employed for verification, all signatures may require a re-sampling to a predefined size. This normalization is carried out in a way as to preserve the aspect ratio of the signature.

Segmentation: If the verification system directly works on documents (for example checks etc.), the signature block may require segmentation from rest of the document. Segmentation may also involve elimination of the border [14] or removal of background (if any).

Enhancement: Image enhancement techniques are typically applied to the signature image for contrast enhancement and/or noise removal prior to feature extraction. Traditional image enhancement filters are generally used for this purpose.

Binarization: In some cases, signature verification systems extract features from binarized images of signatures. These systems require a binarization step where the signature image is converted into binary using global or local thresholding algorithms.

Feature extraction: Feature extraction is the process of extracting the representative characteristics of signatures which allow discriminating different signature classes [21]. Like any other shape matching problem, features extracted from signatures could be structural or statistical. Since rich classifiers are available for statistical features, most of the studies on signature verification are based on statistical features which are further categorized into global and local features.

Global Features: These features are computed from the complete signature as a whole and typically include attributes like aspect ratio, density, edge points, distribution of orientations, transformations and topology etc. [2].

Local Features: Local features are extracted from small regions of the signature image which are obtained using a logical or component based segmentation of signatures.

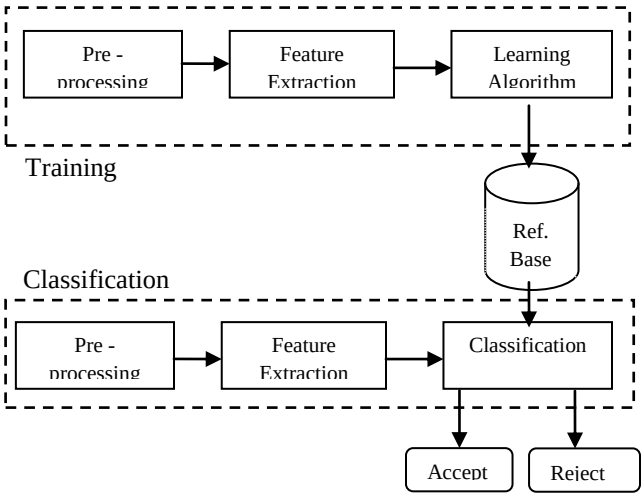

Figure 1: General steps in offline signature verification

Classification Classification includes making a decision about the authenticity of a query signature. Classification involves extracting features from the signature in question and feeding them to a classifier trained on the reference signature base. The classifier classifies the query signature as genuine or forged. Typical classifiers applied to signature verification include artificial neural networks (ANN), support vector machine (SVM) and hidden Markov models (HMM) etc. [3].

4.4 Evaluation Metrics Like any other biometric authentication system, signature verification also employs the well-know False Acceptance Rate (FAR) and False Rejection Rate (FRR) for performance evaluation. FAR represents the percentage of forged signatures falsely accepted as genuine while FRR refers to the percentage of genuine signatures wrongly classified as forged. Generally, the verification systems rely on a threshold to reject or accept a signature and changing the threshold results in increasing one of the errors and decreasing the other. Consequently, another measure, the Equal Error Rate (EER) is also used to quantify the performance of verification systems. The system threshold is fixed to a value where the FAR is equal to the FRR, the particular value of error being termed as EER.

After having discussed the general steps in a signature verification system and the evaluation metrics employed, we present notable recent research contributions to this problem in the following section.

5. A REVIEW OF SIGNATURE VERIFICATION APPROACHES

Signature verification is one of the most researched pattern classification problems. The techniques developed for verification of signatures are generally divided into three categories, template matching, statistical approaches and structural approaches. We discuss the different verification methods proposed under each of these classes in the following.

5.1 Template Matching Template matching [10] is considered the simplest technique to match two signatures. A signature in question is matched with the templates stored in the reference base. The matching is directly carried out on signatures rather than on features. Dynamic Time Warping (DTW) has been most widely used for this purpose [4]. Shanker et al. [18] modified the DTW algorithm for matching signatures and realized better results than the traditional DTW. The authors claim that the improved DTW reports an EER of 2% as compared to 29% with original DTW on the same data set. In [1], authors employ raw pixels and consider signature verification as a graph matching problem. EERs of 26.7% and 5.7% are achieved on skilled and random forgeries respectively. Kennard et.al [24] developed an algorithm for 2D geometric warp and obtained an EER of 26%. Liwicki et.al [25] evaluated their proposed template matching approach on offline and online Dutch and Chinese signatures and obtained acceptably good verification performance.

5.2 Statistical Approaches Statistical approaches are based on a set of statistical features extracted from the signature images. These features are then fed to a learning algorithm to learn to discriminate between

different signature classes. Classifiers like ANN, SVM and HMM have been extensively used for this problem.

Among well-known statistical signature verification techniques, Dehghan et.al [5] used a set of shape descriptors and a combination of multiple neural networks as classifier. Velez et al. [12] employed a number of statistical measures as features and a compression NN as classifier to realize a FAR of 2.1% and FRR of 0%. A number of other studies also use a combination of statistical features and an artificial neural network for signature verification [26, 27, 28].

An interesting and novel Gabor filter based feature (G-Surf) has been introduced by Pal et al. in [19]. Features extracted from signature images are used to train a support vector machine which discriminates between different signature classes. In [2], authors investigate the combination of multiple features for signature verification. The features considered in their study include shape descriptors, Fourier Mellin transform, Envelope histogram of oriented gradients, and Envelope curve coding. In [11], authors employ discrete radon transform and hidden Markov models realizing equal error rates of 18% on skilled forgeries and 4.5% on casual forgeries.

Hai Rong et al. [16] extract interesting points from signature images including turning, intersection and isolated points etc. and use these points to partition the signature into small grids. Features extracted from the grids are then fed to HMM for training/classification. Other recent studies based on HMM [13, 14] have also shown promising performance on the verification task.

Barbantan et al. [9] carry out a study on the discriminating power of different well-known features and employ a feature selection mechanism to find the optimal set of features for verification of signatures. In [29], Kumar et al. use a set of shape and texture based features to characterize signatures and employ two different classifiers for verification, ANN and SVM. Özgündüz et al. [22] extract directional and grid based features from signature images and compare the performance of these features on SVM and ANN classifiers. SVM outperforms ANN achieving a true classification rate of around 95%. Ferrer et al. [7] compare the performance of basic local binary patterns (LBP) against the variants of LBP and GLCM based features using SVM as classifier and report that the basic version of LBP is more robust to noise and distortions in comparison to its extensions.

After having discussed the signature verification techniques based on statistical features, we present an overview of few verification approaches based on structural features

5.3 Structural Approaches Structural approaches represent the signatures using trees, graphs, strings and other similar structures which are the compared through matching algorithms to perform the verification task. Among well-known structural approaches, Zafar et al. [23] represent the signature by a polygon formed by joining the end points of the signature. A set of structural features extracted from the approximating polygon are then used to characterize the signature. In [30], authors compute structural descriptors to characterize signatures while in [32] structural features extracted from the contours of signature images are used to train a neural network. In [31], authors employ grid based features and evaluate them using eight different classifiers. The classifiers are then combined using score based as well as decision based fusion and improved verification results are realized.

6. DISCUSSION

This section presents a comparative analysis of the signature verification techniques discussed earlier. The simplest of these approaches is template matching which performs acceptably good on random forgeries but cannot handle skilled forgeries. Dynamic time warping (DTW) addresses most of the issues with basic template matching by allowing comparison of signals (features) which are not aligned in space/time. DTW, however, suffers from high computational cost in terms of memory as well as time. Neural networks and their variants are easily the most widely used classifiers for this problem. Hidden Markov models have also been effectively applied for verification of signatures but they require significant number of training samples of each class (individual) for learning. Verification techniques based on SVM also realize performances which are comparable and, in some cases, better than the traditional classifiers. These state-of-the-art classifiers work with statistical features and the availability of this rich pool of classifiers for these features make them an attractive choice for pattern classification problems in general and signature verification in particular. Verification techniques based on structural features have also been proposed. While structural features better capture the shape and geometrical information in signatures, matching of structural features is not straight forward. Consequently, techniques based on statistical features outnumber those based on structural features.

A quantitative comparison in terms of equal error rates (EER) of few of the techniques discussed in this paper is summarized in Table 1. In most cases, the verification performance is reported on custom developed databases making it hard to objectively compare different methods. It can be noticed from Table 1 that in majority of cases, acceptably low equal error rates are reported.

It is also important to mention that despite 30 years of research, offline signature verification is still an open problem. This argument is supported by regular organization of International competitions on signature verification in conjunction with a number of reputed International conferences. The participation of a large number of research groups around the globe in these competitions speaks about the kind of research interest this problem has still maintained.

Table 1: Performance comparison of different signature verification techniques
(G = Genuine Signatures, F = Forged Signatures, SF=Skilled Forgeries, CF = Casual Forgeries)

SNo	Approach	Database	Signer	ERR%
1	HMM / DRT [10]	Stellenbosch / Dolfing	Users: 73 F:22 G:51	SF:18% CF: 4.5%
2	ANN [27]	Custom	Users:300 G: 150 F: 150	0.415%
3	G-SURF [19]	GPDS	Users:50 F:30 G:24	0.95%
4	HMM [16]	Custom	Users: 200 G:25 F:55	6.4%
5	GWA [24]	Custom/ SigCom2011	G=192 F=256 / G=764 F=1005	4.02% 20%/26%

7. CONCLUSION

This paper presented a review of some notable contributions to offline signature verification along with a discussion on the pros and cons of these techniques. This review, by no means is exhaustive and for comprehensive reviews on this subject the readers may refer to a number of interesting survey papers [20] on this problem. The idea of this paper is to give novice researchers a quick review of the problem domain and the different approaches that have been developed over the years. Some interesting areas which could be further explored in offline signature verification include investigation of relevance of different features for this problem and the combination of different classifiers to achieve near to 0 error rates. Adaptation of these features and classifiers for online signature verification where the memory and processing resources are limited, could also be an interesting track to explore.

REFERENCES

1. Abuhaiba, Ibrahim SI. "Offline signature verification using graph matching. "Turkish Journal of Electrical Engineering & Computer Sciences 15.1 (2007): 89-104.
2. Hassan, Ehtesham, et al. "Off-line hand written input based identity determination using multi kernel feature combination." Pattern Recognition Letters 35 (2014): 113-119.
3. Arya, Meenakshi S., and Vandana S. Inamdar. "A preliminary study on various off-line hand written signature verification approaches." International Journal of Computer Applications 1.9 (2010): 50-56.
4. Impedovo, Donato, and Giuseppe Pirlo. "Automatic signature verification: the state of the art." Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on 38.5 (2008): 609-635.
5. Dehghan, Mehdi, Karim Faez, and Mahmood Fathi. "Signature verification using shape descriptors and multiple neural networks. "Proceeding of IEEE Region. Vol. 10. 1997.
6. Ozgunduz, Emre, TulinSenturk, and M. ElifKarsligil. "Off-line signature verification and recognition by support vector machine." (2005).
7. Ferrer, Miguel A., et al. "Robustness of offline signature verification based on gray level features." Information Forensics and Security, IEEE Transactions on7.3 (2012): 966-977.

8. Ferrer, Miguel A., Jesus B. Alonso, and Carlos M. Travieso. "Offline geometric parameters for automatic signature verification using fixed-point arithmetic. "Pattern Analysis and Machine Intelligence, IEEE Transactions on 27.6 (2005): 993-997.
9. Barbantan, Ioana, Camelia Vidrighin, and Raluca Borca. "An offline system for handwritten signature recognition." Intelligent Computer Communication and Processing, 2009. ICCP 2009. IEEE 5th International Conference on. IEEE, 2009.
10. Inglis, Stuart, and Ian H. Witten. "Compression-based template matching." Data Compression Conference, 1994. DCC'94. Proceedings. IEEE, 1994.
11. Coetzer, Johannes, Ben M. Herbst, and Johan A. du Preez. "Offline signature verification using the discrete radon transform and a hidden Markov model. "EURASIP Journal on Applied Signal Processing 2004 (2004): 559-571.
12. Velez, Jose F., Angel Sanchez, and A. Belén Moreno. "Robust off-line signature verification using compression networks and positional cuttings." Neural Networks for Signal Processing, 2003. NNSP'03. 2003 IEEE 13th Workshop on. IEEE, 2003.
13. Justino, Edson JR, et al. "An off-line signature verification system using hidden markov model and cross-validation." Computer Graphics and Image Processing, 2000. Proceedings XIII Brazilian Symposium on. IEEE, 2000.
14. Kovari, Bence, and Hassan Charaf. "A study on the consistency and significance of local features in off-line signature verification." Pattern Recognition Letters 34.3 (2013): 247-255.
15. Kumar, Rajesh, J. D. Sharma, and Bhabatosh Chanda. "Writer-independent off-line signature verification using surroundedness feature." Pattern Recognition Letters 33.3 (2012): 301-308.
16. Lv, Hai Rong, Wen Jun Yin, and Jin Dong. "Off-line Signature Verification based on deformable grid partition and Hidden Markov Models." Multimedia and Expo, 2009. ICME 2009. IEEE International Conference on. IEEE, 2009.
17. Hanmandlu, Madasu, Mohd Hafizuddin MohdYusof, and Vamsi Krishna Madasu. "Off-line signature verification and forgery detection using fuzzy modeling." Pattern Recognition 38.3 (2005): 341-356.
18. PiyushShanker, A., and A. N. Rajagopalan. "Off-line signature verification using DTW." Pattern Recognition Letters 28.12 (2007): 1407-1414.
19. Pal, Srikanta, et al. "Off-line Signature Verification using G-SURF." 12th International Conference on Intelligent Systems Design and Applications (ISDA). http://dx. doi. org/10.1109/ISDA. 2012.6416603, 2012.
20. Hou, Weiping, Xiufen Ye, and Kejun Wang. "A survey of off-line signature verification." Intelligent Mechatronics and Automation, 2004. Proceedings. 2004 International Conference on. IEEE, 2004..
21. Al-Omari, Yazan M., SitiNorul Huda Sheikh Abdullah, and Khairuddin Omar. "State-of-the-art in offline signature verification system." Pattern Analysis and Intelligent Robotics (ICPAIR), 2011 International Conference on. Vol. 1. IEEE, 2011.
22. Ozgunduz, Emre, Tulin Senturk, and M. ElifKarsligil. "Off-line signature verification and recognition by support vector machine." (2005).
23. Zafar, Sohail, and Rashid Jalal Qureshi. "Off-line signature verification using structural features." Proceedings of the 7th International Conference on Frontiers of Information Technology. ACM, 2009.
24. Kennard, Douglas J., William A. Barrett, and Thomas W. Sederberg. "Offline signature verification and forgery detection using a 2-D geometric warping approach." Pattern Recognition (ICPR), 2012 21st International Conference on. IEEE, 2012.
25. Liwicki, Marcus, et al. "Signature verification competition for online and offline skilled forgeries (SigComp2011)." Document Analysis and Recognition (ICDAR), 2011 International Conference on. IEEE, 2011.
26. Chhabra, Sakshi, et al. "OFF-LINE Signature Verification Using Neural Network Approach." International Journal of Computer Trends and Technology (IJCTT) ,2013.
27. Jarad, Mujahed, Nijad Al-Najdawi, and Sara Tedmori. "Offline handwritten signature verification system using a supervised neural network approach. "Computer Science and Information Technology (CSIT), 2014 6th International Conference on. IEEE, 2014.
28. Alam, Md, and Aisha Hassan Abdalla. "An evaluation on offline signature verification using artificial neural network approach." Computing, Electrical and Electronics Engineering (ICCEEE), 2013 International Conference on. IEEE, 2013.
29. Kumar, Rajesh, J. D. Sharma, and Bhabatosh Chanda. "Writer-independent off-line signature verification using surroundedness feature." Pattern Recognition Letters 33.3 (2012): 301-308.
30. Huang, Kai, and Hong Yan. "Off-line signature verification using structural feature correspondence." Pattern Recognition 35.11 (2002): 2467-2477.
31. Swanepoel, Jacques P., and Johannes Coetzer. "Off-line signature verification using flexible grid features and classifier fusion." Frontiers in Handwriting Recognition (ICFHR), 2010 International Conference on. IEEE, 2010.
32. Armand, Stephane, Michael Blumenstein, and Vallipuram Muthukkumarasamy. "Off-line signature verification using the enhanced modified direction feature and neural-based classification." Neural Networks, 2006. IJCNN'06. International Joint Conference on. IEEE, 2006.