International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (433-439), Impact Factor: 1.252, Available online at: www.erpublications.com

An Offline Handwritten Signature Verification System - A Comprehensive Review

Ms. Deepti Joon[1], Ms. Shaloo Kikon[2]

[1]M. Tech. Scholar, Dept. of ECE, P.D.M. College of Engineering, Bahadurgarh, Haryana
[2]Asst. Professor, Dept. of ECE, P.D.M. College of Engineering, Bahadurgarh, Haryana

Abstract: Handwritten signature is one of the oldest biometrics. Handwritten signature identification or verification is simple, fairly secure, inexpensive, nonintrusive and acceptable in society. Nevertheless, it has some drawbacks: lower identification rate with respect to other biometrics, non-linear changes with size changing and dependency to time and emotion. Another problem of processing the handwritten signature is the differences between signatures from different nationalities. Signature verification deals with the problem of identifying forged signatures of a user from his/her genuine signatures. The difficulty lies in identifying allowed variations in a user's signatures, in the presence of high intra-class and low interclass variability (the forgeries may be more similar to a user's genuine signature, compared to his/her other genuine signatures). The problem can be seen as a nonrigid object matching where classes are very similar.

Keywords: offline signature, gradients, handwritten, biometrics, verification.

Introduction

According to most financial institutions give preference to the use of the offline handwritten signature despite the fact that the online signatures have proved to be more reliable but however require more complex processing and high-tech gadgets which the offline signatures do not require. Offline signatures can be signed on a piece of paper, which as at today plays a very vital role in documentation despite the ongoing erevolution. Online signatures on the other hand, require special hardware such as digitizers and pressure tablets necessary to acquire the dynamic information such as pressure and speed of the signer, besides the static image of the signature.

Notwithstanding efforts toward the dematerialization of documents, the need for fast and accurate paper-based document authentication is still growing in our society. The field of biometrics is an important area of study as it offers many advantages over more commonly used authentication methods such as photo ID cards, magnetic strip cards etc. Nowadays, biometric technologies are increasingly and more frequently being used to ensure identity verification. Signatures often incorporate complex geometric patterns that make them a relatively secure means for authorization for high security environments.

Offline signature verification is one of most challenging area of pattern recognition. Many methods have been introduced in literature to find whether a given signature is genuine or forgery. The problem however is that the offline signature can be easily imitated or forged which could lead to false representation or fraud. Therefore, there is a need for adequate protection of personal signatures. Verification decision of offline handwritten signatures usually undergoes a series of processes which include pre-processing (where the local and global features of the handwritten signature is extracted), identification and verification of the extracted features against a standardized database. A good verification result can be derived by matching the robust features of the sample signature against the signature of the user through appropriate techniques or classifiers. However, most studies in this domain have often overlooked the impact of external influences such as duress and mind state of the signer when signing their signatures.

With the advent of highly advanced computers with unimaginable processing prowess, there is need for the development of a new technique and algorithm that can take into account some of these external factors when investigating or verifying a signature. This paper therefore attempts to address this challenge by proposing a new method for offline handwritten signature identification and verification through the use of a combination of techniques and methods such as adaptive window positioning technique for signature feature extraction, signer specific codebook for clustering and BPANN for matching. The rest of the paper is divided as follows: Section II looks at the related literature in this field, Section III discusses the methodology adopted for this study, Section IV presents and discusses the results of the study and Section V concludes the study.

International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (433-439), Impact Factor: 1.252, Available online at: www.erpublications.com

Depending on the signature acquisition method used, automatic signature verification systems can be classified into two groups: online (dynamic) and offline (static). A static signature image, generally scanned at a high resolution (e.g. 600 dpi), is the only input to offline systems. Verification of signatures found on bank cheques and vouchers are among important applications for offline systems. An example set of offline signatures is shown in Figure 1. In addition to the signature image, time dimension is also available for dynamically captured signatures that are acquired using pressure sensitive tablets or smart pens. These input devices sample the signature at a high frequency, resulting in a time ordered sequence of signature's trajectory points. An example online signature capturing device is shown in Figure 2. Each point is associated with a corresponding acquisition time stamp and a location coordinate, besides other dynamic features such as pressure and pen inclination angles that can be captured subject to the hardware used.

Figure 1: An example set of public figures collected from the web.

Figure 2: An example online signature capturing device.

Online signature verification is generally used for access control and electronic document authentication types of applications. Due to the differences in the input, preprocessing, feature extraction and classification methods used; online and offline systems show significant variations in their approaches, specifically in representation, preprocessing and matching steps. Offline signature verification can be said to be more challenging compared to online signature verification. While variations among a user's signatures and easy to forge signatures pose a challenge in both cases, dynamic information available in online signatures make the signature more unique and more difficult to forge. In particular, imitating both the shape and dynamic information of an online signature seems to be difficult except for very simple signatures. In contrast, it is possible in some real life situations, for an impostor to trace over a genuine offline signature and obtain a high quality forgery. Furthermore, the availability of the signature's trajectory also makes it easier for online verification systems to align two signatures and detect differences.

Various Models of Handwritten signature

The field of off-line signature verification has enjoyed a great deal of attention over the past few decades. In this chapter we present a collection of verification systems proposed over the years. Although some of these systems may seem dated, they represent noteworthy efforts in the field and also provide the reader with a historical perspective regarding advances made in recent years. For a comprehensive discussion regarding the current state of the art, the reader is referred to Impedovo and Pirlo (2008). Unfortunately, there exists at present no standard library of off-line signatures for verification purposes, and therefore no truly objective benchmark regarding results obtained by any of the systems mentioned. Results reported by the various authors do nonetheless provide the reader with a general idea regarding the effectiveness of their proposed feature extraction techniques and verification strategy. The discussion of each system is chronologically categorised according to the primary method used for verification, and includes the year of publication and author(s) associated. Each of the possibly numerous features considered is also discussed. Where possible, the nature and composition of the data sets used for training and testing are mentioned, as well as the verification results reported.

Simple distance classifiers

A simple distance classifier (SDC) models each pattern class with a probability density function (PDF), typically Gaussian, and subsequently relies on the distance computed between a test pattern and such a PDF in order to make a classification. Fang et al. (2001) propose a method based on the so-called smoothness criterion, since the authors suggest that the cursive segments of forgeries are generally less smooth than those of genuine signatures. Two approaches are proposed for extracting such a smoothness feature. The crossing method involves comparing each stroke segment to its smoothed version, obtained by performing a second-order cubic spline smoothing operation. The second method employs the fractal dimension of each stroke segment to evaluate its smoothness. The obtained smoothness feature is then combined with various global shape features. These include the signature aspect ratio, baseline shift of the vertical projection, the percentage of positively slanted border pixels, as well as the percentage of vertically slanted border pixels.

The database considered consists of 1320 genuine signatures and 1320 amateur skilled forgeries. An FRR of 18.1% and FAR of 16.4% is reported. Majhi et al. (2006) implement a novel feature extraction method based on geometric centres. Features are obtained by recursively dividing a signature image into sub-images along horizontal and vertical axes located on the geometric centre of the parent image. Geometric centres of the final sub-images subsequently form the feature vector. An Euclidean distance model is used for classification on a database containing 30 genuine signatures, 10 random forgeries, 10 simple forgeries and 10 skilled forgeries per writer. The number of writers considered during testing is not disclosed. The authors reportedly achieve FARs of 2.08% (random forgeries), 9.75% (simple forgeries) and 16.36% (skilled forgeries), associated with an FRR of 14.58%.

Hidden Markov Model

An HMM models each pattern class using a sequence of observations, along with the relationship between individual observations within such a sequence, and is discussed further in Section 4.4 and Appendix B. Coetzer et al. propose the combination of an HMM-based verifier with DRT based features. By constructing an HMM utilising a ring topology, rotation invariance is achieved. The system is tested on the Stellenbosch data set (as discussed in the previous section), as well as Dolfing's data set (as considered in this study). Experiments performed on the Stellenbosch data set reportedly yield EERs of approximately 18% and 4.5% when skilled and simple forgeries are considered, respectively. An EER of 12.2% is reported when considering only amateur skilled forgeries from Dolfing's data set.

Considering only professional skilled forgeries from Dolfing's data set reportedly yields an EER of 15%. Oliveira et al. (2005) investigate the use of grid segmentation in conjunction with the graphological features pixel density, pixel distribution, progression, slant and form. Experiments are performed on a database collected from 60 individuals, including 2400 genuine signatures, 1200 random forgeries, 600 simple forgeries and 600 skilled forgeries. Feature-specific EERs of 7.87% (pixel density), 7.65% (pixel distribution), 7.92% (slant), 9.15% (progression) and 11.30% (form) are reported. Wen et al. combine the efforts of a ring-structured HMM with a set of ringperipheral features based on a transformation-ring-projection. The system is evaluated on a data set containing 2640 signatures, of which 1320 are skilled forgeries, representative of 55 individual writers. The authors report an EER of 11.4%. Furthermore, the system is also tested using a sub-corpus of the MCYT bimodal database, containing 2250 signatures from 75 individuals, resulting in an EER of 15.02%.

Feature Extraction in Handwritten Signature Systems

Feature extraction step reduces the dimension of original signature images while preserving and extracting the important information encoded in the image. A carefully selected set of features will transform the images so that it becomes easier to distinguish between genuine and forgery classes. Weaker features will increase the load on the classifier. In this section, common features that have been used in offline signature verification problem are summarized.

Contourlet transform:

Contourlet transform as introduced by Do and Vetterli [79] is an efficient tool for capturing smooth contours. It has five significant features: 31 Multiresolution, localization, critical sampling, directionality and anisotropy. It is a double filter bank: Laplacian Pyramid (LP) is followed by a Directional Filter Bank (DFB). It is also named pyramidal directional filter bank (PDFB). LP at each level decomposes input image into down sampled lowpass sub-band (coarse image) and one bandpass sub-band. DFB is then applied to bandpass sub-band. By repeating this scheme iteratively on the coarse image resulted from LP at each level, a fine to coarse representation of the input image is obtained. Contourlet transform is applied to offline signature verification problem by Pourshahabi et al. Reported EER values are 14% for a private Persian dataset and 23% for a private English dataset, with skilled forgeries.

Local binary patterns:

Local binary pattern (LBP) is a powerful feature proposed to capture the texture in objects. In the basic LBP method, a gray scale image is processed such that a binary code is generated for each pixel in the image. This code encodes whether the intensities of the neighboring pixels are greater or less than the current pixel's intensity. So, for instance in a 3x3 neighborhood with the current pixel being the center, a binary code of length 8 is generated consisting of 0s and 1s, according to the relative intensities of the neighbors. A histogram is then computed to count the number of occurrences of each binary code, describing the proportion of common textural patterns. LBP is very suitable for offline signature verification and has been utilized in several works.

The reason is that, LBP encodes neighboring patterns of pixels well. There are many LBP variants proposed in the literature. However, there are few works for LBP pattern selection proposed so far. An important drawback of the original LBP method is the sparse histogram generated, for example of size 256 for 3 by 3 neighborhood. Much of these patterns would never be seen on a small image sample. An example LBP histogram selection is applied to color texture classification by Porebski et al. It consists in assigning to each histogram a score which measures its efficiency to characterize the similarity of the textures within the different classes. The histograms are then ranked according to the proposed score and the most discriminant ones are selected. Selection is based on one of the simplest available methods according to the authors. It is a within-class histogram intersection similarity measure. Accuracy rates are reported to increase less than 0.5% in different color spaces.

Cartesian grids:

First and most common choice is the use of rectangular grids in Cartesian coordinates. The grids may be overlapping to capture the signature at grid boundaries, or non-overlapping. A sample signature, overlaid with 10×20 = 200 non-overlapping rectangular grids is shown in Figure 3. A sample signature with 20% overlapping 6×6 = 36 grids is shown in Figure 4, grids are shown altogether. We use overlapping grids which are found to perform better.

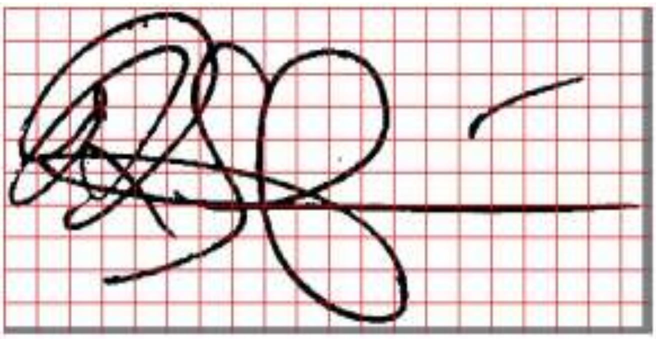

Figure 3: Cartesian non-overlapping grids.

International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (433-439), Impact Factor: 1.252, Available online at: www.erpublications.com

Figure 4: Cartesian 6x6 20% overlapping grids shown altogether

Signature Modelling and Verification System

In this study, we explain how these feature based signature representations may be used to construct writer-dependent models used for signature verification, thereby completing the classification phase, as well as the underlying pattern recognition process, introduces several key concepts regarding the writer-dependent approach to signature verification. Previous Section focus on the base classifiers developed in this study and show that they employ two fundamentally different classification techniques.

We explain the advantages of using the DTW-based approach to vector matching as an alternative to other popular distance measures. The second classifier, a discrete observation left-right HMM, is also presented. We explain the general advantages of utilising an HMM-based approach to signature modelling, as well as the reasoning behind the specific HMM design considered in this study. Detailed discussions of the theoretical background required for DTW and HMM development are reserved for Appendices A and B, respectively. Although the topics discussed in these appendices are of vital importance to the successful implementation of the DTW and HMM base classifiers, they are not deemed central within the context of this chapter.

Modelling

The act of signature creation is a dynamic, time-varying process, since it is physically impossible for any writer to exactly duplicate a signature in successive attempts. Certain variations therefore become evident in the feature sets of different genuine signatures belonging to a single writer. This phenomenon is commonly referred to as intra-class variability. Consequently, it becomes essential for any efficient verification system to sufficiently understand and compensate for such variations. In general, given a set of training signatures, the construction of a writer-dependent signature model is based on a certain predefined reference entity. In this study, for example, the reference entities used by the DTW and HMM base classifiers are represented by a signature pattern Xk (see Section 4.3.2) and hidden Markov model λ (see Section 4.4.4), respectively.

Following possible model optimisation, any signature pattern subsequently submitted for verification is matched against such a reference entity, thereby yielding an appropriate classifier score. In order to compensate for the intra-class variability associated with writer ω, certain writer-specific statistics are also included in the signature model. The most popular statistics are undoubtedly $\mu\omega$ and $\sigma\omega$, denoting the mean and standard deviation, respectively, of the classifier scores obtained from the training set of writer ω. Whilst $\mu\omega$ represents a benchmark for the classifier score obtained from a typical genuine signature belonging to writer ω, the measure of tolerable score variability obtained from the training set is quantified by $\sigma\omega$. These statistics are therefore also said to estimate the confidence distribution1 of genuine signatures belonging to writer ω, as illustrated in Figure 4. In an ideal scenario, this estimated distribution would include any and all genuine signatures produced by writer ω, whilst excluding all forgeries. As shown in the next section, however, this is generally not a valid assumption.

We experimentally confirm the contributions made in this study. The results are compared to the results reported for previous systems proposed in the literature.

The signature database considered in this study contains 4837 signatures obtained from 51 different writers. This data set, originally captured on-line, is referred to as Dolfing's data set, as it was originally utilised by Dolfing (1998) for the purpose of developing an on-line signature verification system. Dolfing's original data set has since been converted into an off-line data set, thereby rendering it suitable for the evaluation of the classifiers developed in this study. For a detailed discussion regarding the conversion algorithm, the reader is referred to Coetzer (2005). Since Dolfing's data set was originally captured on-line, the resulting off-line representation can be viewed as an ideal data set, in the sense that none of the signature images suffer from the presence of background noise. In addition, each signature image contained in the data set has a uniform stroke width of approximately 5 pixels.

During the acquisition of Dolfing's data set, each of the 51 writers submitted 30 signature samples, contributing a total of 1530 genuine signatures. A total of 3000 amateur skilled forgeries and 307 professional skilled forgeries were subsequently collected. Only the set of amateur skilled forgeries are considered in this study. In order to gain further insight into the nature of Dolfing's data set, we present a collection of samples, one genuine signature for each of the 51 writers, in Figure 5. From these samples, it is clear that the signatures comprising Dolfing's data set represent a wide variety of handwriting styles, as well as greatly varying levels of intricacy regarding signature design.

Figure 5: Typical examples of signature images contained in Dolfing's data set. Each image represents a genuine signature belonging to one of the 51 enrolled writers.

Conclusion

The proposed signature verification system is been based on some special features extraction. Global features included connected component, height width ratio, number of end points and type of end point line. It uses a compact and memory efficient storage of feature points, which reduces memory overhead and results in faster comparisons of the data to be verified. From intuition, the statistics on the positional variations of the features or strokes of signature samples should be useful for verification. The present study was aimed at evaluating the usefulness of the method. Although it is not the best among all existing methods, there is the possibility of combining it with other methods to achieve better results. Similar to other real world problems, no single approach may solve the signature verification problem perfectly, and practical solutions are often derived by combining different approaches. This technique can be added with any existing verification system for better result.

References

[1]. K. Saeed, M. Tab_dzki, M. Adamski, "A New Approach for Object Feature Extract and Recognition", 9th International Conference on Advanced Computer Systems – ACS'02, pp. 389-397, Miedzyzdroje, 23-25 October 2002.
[2]. J. F. Vargas, M. A. Ferrer, C. M. Travieso, and J. B. Alonso, "Off-line signature verification based on grey level information using texture features," Pattern Recogn., vol. 44, pp. 375–385, February 2011.
[3]. G. S. Spagnolo, C. Simonetti, and L. Cozzella, "Superposed strokes analysis by conoscopic holography as an aid for a handwriting expert," Journal of Optics A: Pure and Applied Optics, vol. 6, pp. 869–874, 2004.
[4]. A. Kholmatov and B. Yanıko˘glu, "Identity authentication using improved online signature verification method," Pattern Recognition Letters, vol. 26, no. 15, pp. 2400–2408, 2005.

[5]. R. Plamondon and G. Lorette, "Automatic signature verification and writer identification – the state of the art," Pattern Recognition, vol. 22, no. 2, pp. 107–131, 1989.
[6]. J. -P. Drouhard, R. Sabourin and M. Godbout, "A neural network approach to off-line signature verification using directional PDF" Pattern Recognition, Volume 29, Issue 3, pp 415-424, March 1996.
[7]. Marco Desira, W Kenneth P. Camilleri, "Handwritten Signature Verification by Independent Component Analysis" ICT08 Conference Programme, 2007.
[8]. Karanja Evanson Mwangi, "Offline Handwritten Signature Verification Using Sift Features", Faculty of Computing and Information Technology, Makerere University, 2008.
[9]. Javier Ruiz-del-Solar, Christ Devia, Patricio Loncomilla, and Felipe Concha, "Offline Signature Verification Using Local Interest Points and Descriptors", LNCS 5197, pp. 22–29, 2008. Springer-Verlag Berlin Heidelberg 2008.
[10]. N. Otsu, "A threshold selection method from gray-level histogram," IEEE Transactions on System Man Cybernetics, Vol. SMC-9, No. 1, 1979, pp. 62-66.
[11]. Bence Kovari, "Time-Efficient Stroke Extraction Method for Handwritten Signatures", 7th WSEAS International Conference on APPLIED COMPUTER SCIENCE, Venice, Italy, November 21-23, 2007.
[12]. Khalid Saeed and Marcin Adamski, "Extraction of global features for off line signature recognition", Faculty of Computer Science, Bialystok Technical University, Wiejska 45A, 15-351 Bialystok, Poland.
[13].
[14]. R. Sabourin, R. Plamondon, and G. Lorette, "Off-line identification with handwritten signature images: survey and perspectives," Structured Document Image Analysis, pp. 219–234, 1992.
[15]. M. A. Ferrer, F. Vargas, A. Morales, and A. Ordonez, "Robustness of offline signature verification based on gray level features." IEEE Transactions on Information Forensics and Security, vol. 7, pp. 966–977, 2012.
[16]. F. Vargas, M. A. Ferrer, C. M. Travieso, and J. B. Alonso, "Off-line handwritten signature GPDS-960 corpus," in IAPR 9'th International Conference on Document Analysis and Recognition, September 2007, pp. 764–768.