Automatic Off-Line Signature Verification Systems: A Review

Srikanta Pal  
School of Information and Communication Technology, Griffith University, Queensland, Australia.  
+61-755529044  
srikanta.pal@griffithuni.edu.au

Michael Blumenstein  
School of Information and Communication Technology, Griffith University, Queensland, Australia.  
+61-755528271  
m.blumenstein@griffith.edu.au

Umapada Pal  
Computer Vision and Pattern Recognition Unit, Indian Statistical Institute, Kolkata-700108, India.  
+91-25752856  
umapada@isical.ac.in

ABSTRACT
The use of biometric technologies for human identity verification is growing rapidly in civilized society and showing its advancement towards the usability of biometrics for security. Off-line signature verification is considered as a behavioral characteristic based biometric trait in the field of security and the prevention of fraud. So, offline signatures are extensively used as a means of personal verification and identification. Manual signature-based authentication of a large number of documents is a very difficult and time consuming task. Consequently for many years, in the field of protected communication and financial applications, we have observed an explosive growth in biometric personal authentication systems that are closely connected with measurable physical unique characteristics (hand geometry, iris scan, finger prints or DNA). Human signatures also provide secure means for confirmation and authorization in legal documents. So nowadays, automatic signature verification becomes an essential component. In order to convey the state-of-the-art in the field to researchers, in this paper we present a survey of off-line signature verification systems.

General Terms: Systems, Forgeries, Methods, Skilled, Performance.
Keywords: Off-line Signature verification, on-line signature verification, biometrics, authentication systems.

1. INTRODUCTION
In conjunction with the recent and extraordinary growth of the Internet, automatic signature verification is being considered with renewed interest. Signature verification is not only a popular research area in the field of image processing and pattern recognition, but also plays an important role in many applications such as security, access control, contractual matters etc. The recognition of signatures is significantly concerned with the improvement of the interface between human-beings and computers [1, 2]. Research into signature verification has been vigorously pursued for a number of years and it is being explored specially in the off-line mode [3, 4]. A signature verification system and the associated techniques used to solve the inherent problems of authentication can be divided into two classes [5, 6]: (a) on-line method [7, 8] to measure the sequential data such as order of stroke, writing speed, writing time, pen pressure by utilizing intelligent machine algorithms [9, 10] and (b) off-line method [11, 12] that uses an optical scanner to obtain handwriting data written on paper. Off-line Signature verification deals with the verification of signatures, which are in a static format [13]. On-line signature verification has been shown to achieve much higher verification rates than off-line verification [11] as a lot of dynamic information is lost in the off-line mode. Hence, on-line signature verification is generally more successful. Signatures represent a particular writing style and are not considered as a collection of letters and words [14]. A person’s signature often changes depending on some elements such as mood, fatigue, time etc. Great inconsistency can even be observed in signatures according to country, habits, psychological or mental state, physical and practical conditions [15].

This paper is organised as follows: Section 2 discusses the signature verification concept, Section 3 introduces different types of forgeries, Section 4 introduces different methods of signature verification systems, Section 5 deals with non-English signature verification, Section 6 introduces a comparison of different approaches, Section 7 introduces our realization and future aspects. Finally, Section 8 concludes the paper.

2. SIGNATURE VERIFICATION CONCEPT
Signature verification (SV) systems seek to authenticate the identity of an individual, based on an analysis of his/her signature, through a process that discriminates a genuine signature from a forgery [16]. Signature verification is different to handwritten character recognition, because signatures are often unreadable, and they can simply appear as images with some particular curves that represent the writing style and pattern of an individual. Signatures are a special type of handwriting and very often are a combination of symbols and strokes.

In general to deal with the problem of off-line signature verification, researchers have investigated a commonly used approach which is based on two different patterns of classes, class1 and class2: Class1 represents the genuine signature set, and Class 2 represents the forged signatures set. For performance calculation usually two types of errors are considered. The False Rejection, which is called a Type-1 error and the False Acceptance which is called a Type-2 error. So there are two types of error rates: False Rejection Rate (FRR) which is the percentage of genuine signatures treated as forgeries, and False Acceptance Rate (FAR) which is the
percentage of forged signatures treated as genuine. When we deal with the experiments of a signature verification system, we consider FRR and FAR.

Feature extraction is also an essential component for contributing to the success of a signature verification system. An ideal feature extraction technique extracts a minimal feature set that maximizes interpersonal distance between signature examples of different persons, while minimizing intrapersonal distance for those belonging to the same person.

3. TYPES OF FORGERIES

There are usually three different types of forgeries to take into account. These three basic types of forged signatures are indicated below:
a. Random forgery. The forger has no access to the genuine signature (not even the author’s name) and reproduces a random one. A random forgery may also include the forger’s own signature.
b. Simple forgery. The forger knows the author’s name, but has no access to a sample of the signature. Thus, the forger reproduces the signature in his/her own style.
c. Skilled forgery. The forgery has access to one or more samples of the genuine signature and is able to reproduce it. Skilled forgeries can even be subdivided according to the level of the forger’s skill.

But based on the various skilled levels of forgeries, it can also be divided into six different subsets. The paper [22] shows various skill levels of forgeries and these are shown below:
1. A forged signature can be another person’s genuine signature. Justino et al. [17] categorized this type of forgery as a Random Forgery.
2. A forged signature is produced with the knowledge about the genuine writer’s name only. Hanmandlu et al. [19] categorized this type as a Random Forgery whereas Justino et al. [17] categorized this type as a Simple Forgery. Weiping et al. categorized this type as a Casual Forgery [18].
3. A forged signature imitating a genuine signature’s model reasonably well is categorized as a Simulated Forgery by Justino et al. [17].
4. Signatures produced by inexperienced forgers without the knowledge of their spelling after having observed the genuine specimens closely for some time are categorized as Unskilled Forgeries by Hanmandlu et al. [19].
5. Signatures produced by forgers after unrestricted practice by non-professional forgers are categorized as Simple Forgery/Simulated Simple Forgery by Ferrer et al. [20], and a Targeted Forgery by Huang and Yan [21].
6. Forgeries which are produced by a professional imposter or person who has experience in copying Signatures are categorized as Skilled Forgeries by Hanmandlu et al. [19].

4. DIFFERENT METHODS FOR OFF-LINE SIGNATURE VERIFICATION SYSTEMS

Many techniques have been developed in the field of off-line signature verification. Some convenient approaches and optimised schemes are discussed below:

Ismail et al. [23] developed an off-line signature identification method. A data base of 2400 signature images is considered. Chain code feature extraction is used to represent a boundary by a connected sequence of straight-line segments of specified length and direction. Seven different types of distance measure were used based on feature vectors derived from eigen-signatures. The highest accuracy of 96.2% is obtained with the Manhattan distance measure.

Justino et al. [24] proposed an off-line signature verification system based on Hidden Markov Models (HMMs) to detect random, casual, and skilled forgeries. Three features: a pixel density feature, a pixel distribution feature and an axial slant feature are extracted from a grid segmentation scheme. A database of 1600 genuine signatures is used to determine the optimal codebook size for detecting random forgeries. Signatures of 60 writers with 40 training signatures, 10 genuine test signatures, 10 casual forgeries, and 10 skilled forgeries per writer is used in another data set for experimentation. A False Acceptance rate of 2.83% is obtained and a False Rejection rate of 1.44%, 2.50%, and 22.67% are obtained for random, casual, and skilled forgeries, respectively. Some techniques involving off-line signature verification based on HMM are described in [25–32].

Armand et al. [33] presented a system based on the Modified Direction Feature. The feature extraction technique employs a hybrid of two other feature extraction techniques: Direction Feature (DF) and Transition Feature (TF). DF extracts the direction transitions based on the replacement of foreground pixels by their direction values. TF records the locations of the transitions between 1s and 0s in a binary image. A centroid feature and a trisurface feature are also used for enhancing the accuracy of the result. Two Neural Network classifiers are used to classify the signatures. A database totalling 2106 signatures is used and the highest accuracy obtained was 91.12%. Senol and Yildirim [34] presented an off-line signature verification system based on Neural Network. C. Oz [35] introduced an off-line signature verification system based on Artificial Neural Network. Techniques regarding off-line signature verification based on Neural Network are described in [36–38].

Oliveira et al. [39] developed an off-line signature verification system based on the Writer-Independent approach. Receiver Operating Characteristic (ROC) curves is used to improve the performance of the system. ROC graphs are two dimensional graphs in which true positive rate (TPR) and false positive rate (FPR) are plotted on the Y and X axis respectively. They used a two-fold technique. At first, different fusion strategies are analysed based on the ROC. Next, the result of the first stage is further improved by combining the classifiers without the need of joint training. They used two sets of data (160 genuine signatures, 40 forgery signatures and 1200 genuine, 300 forgery signatures). Support Vector Machine is used as a classifier and they obtained 91.80% as the highest recognition rate.

Ozgunduz et al. [40] used Support Vector Machines in order to detect random and skilled forgeries. To represent the signatures, they extracted global geometric features, direction features and grid features. In the experiments, a comparison between SVM and ANN is performed. Using a SVM with RBF kernel, an FRR of 0.02% and an FAR of 0.11% are obtained. Whereas the ANN, trained with the Back propagation algorithm, provided an FRR of 0.22% and an FAR of %0.16. In both experiments, skilled forgeries are used to train the classifier.

Nguyen et al. [41] presented an off-line signature verification system based on global features. In their paper, the
A combination of the Modified Direction Feature (MDF) with three global features: Feature from Energy Information, Maxima Feature, and Ratio Feature is reported. MDF feature extraction technique employs the location of transitions from background to foreground pixels and the direction at transitions in the vertical and horizontal directions of the boundary representation of an object. At each transition, the Location of the Transition (LT) and the Direction Transition (DT) values are recorded. A database of 12 genuine specimens and 400 random forgeries are taken from a publicly available database. The Support Vector Machine (SVM) classifier obtained an average error rate (AER) of 17.25%. Martinez et al. [42] and Motlf et al. [43] presented off-line signature verification systems based on Support Vector Machines.

Rigoll et al. [44] developed a system that systematically compares between off-line and on-line signature verification based on Hidden Markov Models. A database of 340 signatures is used. An angle between the strokes of two consecutive sample points is used for on-line verification. An additional feature i.e. a “Sliding bitmap” is also used for the on-line process. But for the off-line system, the difference between maximum and minimum coordinates of the signature is computed as a maximum height of the signature and the distance is subdivided into a certain number of squares, typically 6-10. Each square consists of approximately 10×10 pixels, and the grey value for each square is computed. The highest accuracies are 99.0% and 98.10% for the on-line and off-line verification systems respectively.

Prashanth et al. [45] proposed an off-line signature verification system based on standard scores correlation. Two types of features: Feature points based on vertical splitting, and feature points based on horizontal splitting are extracted here. The signature image is split with a vertical line passing through the geometric centre of the image to get its left and right parts. This geometric centre is obtained by locating a point where the number of black pixels is half of the total number of black pixels in the signature. The signature image is split with a horizontal line passing through the geometric centre to get the top and bottom parts of the image. The thirty feature points are extracted by following a similar procedure used for vertical splitting.

Schafer and Viriri [46] presented an off-line signature verification system based on the combination of feature sets. Some features are extracted such as: Aspect ratio, centroid feature, four surface features, six surface features, number of edge points, transition features etc. The verification of the signatures is accomplished by using the Euclidean distance. Depending on the threshold of the system, the signature will either be correctly identified as genuine or identified as a forgery. A data base of total 2106 signatures is used in 39 different sets. A success rate of 84.10% is achieved.

Larkins and Mayo [47] proposed a technique based on Adaptive Feature Thresholding (AFT) which is a novel method of person-dependent off-line signature verification. AFT enhances how a simple image feature of a signature is converted to a binary feature vector by significantly improving its representation in relation to the training signatures. The similarity between signatures is then easily computed from their corresponding binary feature vectors. Some important techniques involving off-line signature verification system are described in [48-56].

Kisku et al. [57] presented a system based on fusion of multiple matchers using SVMs for offline signature identification. In order to improve the performance of the system, a few preprocessing operations were carried out on offline signatures. To recognize a person correctly and identify imposters through offline signatures, image enhancement operations were performed on raw signature images. The proposed system uses three different statistical similarity measurement techniques applied to the extracted feature set consisting of geometric, global and local features separately. Matching scores are obtained from individual matchers and these different matchers or classifiers are fused using SVMs. Global signature features are extracted from the whole signature image. On the other hand, local geometric features are extracted from signature grids. Moreover, each grid can be used to extract the same range of global features. Combination of these two types of global and local features is further used to determine the identity of authentic and forged signatures successfully from the database. This set of geometric features is used as inputs to the identification system. The signatures are verified with the help of Gaussian empirical rules, Euclidean and Mahalanobis distance-based classifiers. Recognition of query signatures is performed by comparing these with all signatures in the database. The proposed system was tested on a signature database containing 5400 offline signatures of 600 individuals and the results were found to be promising. Similar types of works are described in [58-64].

Solar et al. [65] introduced a new approach for offline signature verification, based on a general-purpose wide baseline matching methodology. Wide baseline matching approaches based on local interest points are becoming increasingly popular and were experienced an impressive development in past years. In this approach, local interest points are extracted independently from both a test and a reference image, then characterized by invariant descriptors, and finally the descriptors are matched until a given geometric transformation between the two images is obtained. A Bayes classifier is employed to achieve a FRR of 16.4% and a FAR of 14.2%. The papers described in [66-73] indicate more or less same approaches.

Bertolini et al. [74] presented a system where two important issues of off-line signature verification are considered. The first one is in regards to feature extraction and on this basis a new graphometric feature set that considers the curvature of the most important segments of the signature is introduced. The second important aspect is the use of an ensemble of classifiers based on graphometric features to improve the reliability of the classification. The grid-based feature sets are used, i.e., the image of size 400 × 1000 is segmented using a grid and then the features are computed for each cell of the grid. In the system, four characteristics are introduced to train the classifiers, namely density, slant, distribution, and curvature. The first three are applied to signature verification with relative success [18], while the latter is a new feature set introduced as part of their research. The signature database used in this work was composed of 100 writers and it was divided into 40, 20, and 40 for training, validation, and testing, respectively. The error rates reported for simulated, random, and simple forgeries are 8.16%, 5.32%, and 4.48%, respectively. Some similar works are described in [75-78].

Biswas et al. [79] presented an off-line signature verification system using clustering techniques. In this system some
filtering techniques are used for removal of noises, and thinning of the signature images is undertaken in the pre-processing step. The region of interest detection and scaling is also performed here. In this interest detection and scaling step, the signature area within the image is identified i.e. the region of interest (ROI) is identified. The ROI is identified from both the sample signature and corresponding test signature. The scaling is performed on both the sample and test signature. So stretching is performed on the input signature in case it is smaller than the standard size or squeezing is undertaken when it is bigger. Normally all the signatures in the database are made to fit inside a rectangle of the same height and width To obtain the highest accuracy, the features such as: signature height-width ratio, signature occupancy ratio, distance ratio calculation at the boundary, the length and ratio of adjacency columns and number of spatial symbols within the signature image etc are extracted. Some similar techniques involving off-line signature verification are described in [80-86].

5. NON-ENGLISH OFF-LINE SIGNATURE VERIFICATION SYSTEMS

In the field of Signature verification, much of the research undertaken focuses on signatures of English script. Only a few non-English signature verification systems are reported and they are described below.

Lv et al. [87] developed a Chinese off-line signature verification system. A data base of 1100 signatures is considered. Support Vector Machines are used as a classifier. Four different types of features such as Moment feature, Direction feature, Gray distribution and Stroke width distribution feature are used here. Based on every feature, the accuracies are calculated separately and an average accuracy is also calculated based on all combined feature sets. An average error rate 5.10% is found using the combined feature sets. Ji et al. [88] proposed an off-line Chinese signature verification system using weighting factor on similarity computation. Some off-line Chinese signature verification techniques are developed by Ji and Chen [89], Tian and Qiao [90], Ye and Hou [91] and Ji et al. [92].

Ueda et al. [93] presented an off-line Japanese signature verification system using a pattern matching technique. A new pattern matching process is proposed for Japanese signature verification. In their modified pattern matching method, the strokes of the signatures are first thinned at a width of one pixel, and then the thinned signatures are blurred by a fixed point-spread function. A database totalling 2000 signatures is considered and an average error rate 9.1% is obtained.

Ghandali and Moghaddam [94] proposed an off-line Persian signature identification and verification system based on DWT (Discrete Wavelet Transform) and image fusion. In their paper, a new scheme to identify and verify off-line Persian signatures is proposed. In this method, DWT is employed to access high-frequency bands of signature shape. Then, different samples of a person’s signature are fused together based on high frequency bands to generate the signature patterns. This pattern is saved in the learning phase. A database consisting of 720 signatures is used. The error rate 9.9% and 10% are obtained in FRR and FAR respectively from an SVM classifier. Chen & Srichari [95] matched two signature contours using DWT before segmenting and extracting Zernike moments from the segments. Zoghi and Abolghasemii[96] presented an off-line Persian Signature Verification Using Improved Dynamic Time Warping-based Segmentation and Multivariate Autoregressive Modelling. Some techniques involving off-line signature verification based on DWT are discussed in [97-99].

Ismail et al. [100] proposed an off-line Arabic signature recognition and verification technique. In their paper, a system of two separate phases for signature recognition and verification is developed. In the first phase some features based on Translation, circularity feature, image enhancement, partial histogram, centres of gravity, global baseline, thinning etc. are extracted. In the second phase some more features are also extracted such as Central line features, Corner line features, Central circle features, Corner curve features and Critical point features. A set of signature data consisting of 220 genuine samples and 110 forged samples is used for experimentation. They obtained a 95.0% recognition rate and 98.0% verification rate from their system.

Table 1. Comparison of performances of diff. methods.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Approaches</th>
<th>FRR</th>
<th>FAR</th>
<th>Accurac y (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hierarchical Random Graph Model [101]</td>
<td>21.6</td>
<td>11.6</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Weighting Factor based Approach [102]</td>
<td>3.3</td>
<td>16.85</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Enhanced Modified Direction Feature[103]</td>
<td>2.88</td>
<td>1.71</td>
<td>91.21</td>
</tr>
<tr>
<td>4</td>
<td>Hybrid Statistical Modelling [104]</td>
<td>10.00</td>
<td>22.00</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>Writer-independent Approach[105]</td>
<td>-</td>
<td>-</td>
<td>91.80</td>
</tr>
<tr>
<td>6</td>
<td>Based on Fuzzy modeling [106]</td>
<td>12.7</td>
<td>12.7</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>Based on Neural Network [107]</td>
<td>0.01</td>
<td>0.02</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>Structure Feature Correspondence[108]</td>
<td>6.30</td>
<td>8.20</td>
<td>91.80</td>
</tr>
<tr>
<td>9</td>
<td>SVM based approach [109]</td>
<td>4.83</td>
<td>5.30</td>
<td>94.9</td>
</tr>
<tr>
<td>10</td>
<td>Exterior Contours and Shape Features[110]</td>
<td>6.50</td>
<td>6.90</td>
<td>93.80</td>
</tr>
<tr>
<td>11</td>
<td>Fuzzy Modeling Approach [111]</td>
<td>12.60</td>
<td>12.60</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td>Virtual Support Vector Machine [112]</td>
<td>16.00</td>
<td>13.00</td>
<td>-</td>
</tr>
<tr>
<td>13</td>
<td>Person verification based approach [113]</td>
<td>1.55</td>
<td>2.54</td>
<td>97.89</td>
</tr>
<tr>
<td>14</td>
<td>Based on Feature matching[114]</td>
<td>20.5</td>
<td>20.5</td>
<td>-</td>
</tr>
<tr>
<td>15</td>
<td>Based On Global Features[115]</td>
<td>5.40</td>
<td>4.60</td>
<td>-</td>
</tr>
<tr>
<td>16</td>
<td>Chinese Signature Verification [116]</td>
<td>9.49</td>
<td>6.93</td>
<td>-</td>
</tr>
<tr>
<td>17</td>
<td>Orientations Of Geometric Centroids [117]</td>
<td>14.66</td>
<td>25.11</td>
<td>-</td>
</tr>
<tr>
<td>18</td>
<td>Rotation Invariant Approach [118]</td>
<td>10.40</td>
<td>10.40</td>
<td>-</td>
</tr>
<tr>
<td>19</td>
<td>Based on Neural Network [119]</td>
<td>15.0</td>
<td>3.0</td>
<td>-</td>
</tr>
<tr>
<td>20</td>
<td>Contourlet-based method [120]</td>
<td>3.3</td>
<td>13.3</td>
<td>-</td>
</tr>
</tbody>
</table>

6. COMPARISON OF DIFFERENT APPROACHES WITH RESULT
The comparisons of different important methods with associated results are shown in Table 1.

In table 1, accuracy (%) denotes the average Identification rate of different databases. For verification, in the case of FAR some authors specify the rate of FAR separately for different levels of forgeries and the other authors specify the rate of FAR for all the different forgeries. In the table 1 the FAR is shown for all different forgeries. It is also noted that some authors show the verification result but do not show the identification result and vice versa in their paper. The results shows that very good high accuracy is still lacking from existing systems and hence further work is required in this area.

7. OUR REALIZATION AND FUTURE WORK

As we could observe, despite the vast amount of work performed thus far for signature verification, there are still many challenges in this research area. Signatures may be written in different languages and we need to undertake a systematic study on this. Also one problem of this area is, for security reasons, it is not easy to make a signature dataset of real documents (such as banking documents, for example) available to the signature verification community. Publicly availability signature datasets of real documents would make it possible to define a common experimentation protocol in order to perform comparative studies in this field. Researchers have used different features for signature verification. Combination of different classifiers as well as novel classifiers should be explored in future work to enhance performance. Accordingly in this survey we noted that all the published work is based on foreground information. A combination of background and foreground information may be considered for better results in the future.

8. CONCLUSION

To highlight the state-of-the-art to researchers in the field, this paper presents a brief survey of the recent works on off-line signature verification. Different existing approaches are discussed and compared along with their FAR, FRR and accuracies. The accuracy obtained so far from the available systems is not very high and more research on off-line signature verification, on-line signature verification as well as non-English signature verification is required.

9. REFERENCES


