Off-line Signature Verification Using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines

Vu Nguyen, Michael Blumenstein, Vallipuram Muthukkumarasamy Graham Leedham
School of ICT, Griffith University, Queensland, Australia *UNSW (Asia), Singapore*
{Vu.Nguyen2, M.Blumenstein, V.Muthu}@griffith.edu.au *G.Leedham@unswasia.edu.sg*

Abstract

As a biometric, signatures have been widely used to identify people. In the context of static image processing, the lack of dynamic information such as velocity, pressure and the direction and sequence of strokes has made the realization of accurate off-line signature verification systems more challenging as compared to their on-line counterparts. In this paper, we propose an effective method to perform off-line signature verification based on intelligent techniques. Structural features are extracted from the signature's contour using the Modified Direction Feature (MDF) and its extended version: the Enhanced MDF (EMDF). Two neural network-based techniques and Support Vector Machines (SVMs) were investigated and compared for the process of signature verification. The classifiers were trained using genuine specimens and other randomly selected signatures taken from a publicly available database of 3840 genuine signatures from 160 volunteers and 4800 targeted forged signatures. A distinguishing error rate (DER) of 17.78% was obtained with the SVM whilst keeping the false acceptance rate for random forgeries (FARR) below 0.16%.

1. Introduction

Signatures are still widely used in many areas in society. Automatic systems can be used to validate cheques, financial and legal documents. In terms of a signature's reproducibility, Guest indicates that the signature does not differ with age [1].

Automated signature identification/verification is a research field that attempts to create reliable on-line or off-line machines, which can identify or verify human signatures. The on-line recognition process is often conducted using a digitizing tablet or a pen with information about velocity, stroke order, pressure, etc., whilst the off-line process uses a static image of the signature only. The off-line signature recognition problem is more challenging than the on-line one as much valuable information such as the pen's velocity, pressure and stroke order is not available. Thus, while on-line signature verification has been fruitful and has many real world applications, results from the off-line equivalents are still limited.

Signature Identification is the procedure of determining to whom a particular signature belongs to. In this process, features of a signature are first extracted. This information is then used as a key to look up the signature database. The process of determining whether a particular signature is authentic or is a forgery is called verification.

Particular problems facing off-line signature verification are the small number of genuine samples that may be used for the training process and the system's ability to distinguish a genuine signature from different types of forgeries (random, simple, simulated, etc.) [2]. Skilled forgeries are particularly difficult to distinguish from genuine samples.

1.1. Forgery Types

Although research into signature verification has been carried out for many years, the categorization of forged signatures is not standardized. Varying skill levels of forgeries are listed as follows:

1. A forged signature can be another person's genuine signature. Justino *et al.* categorized this type of forgery as a *Random Forgery* [3].
2. A forged signature is produced with the knowledge about the genuine writer's name only. Hanmandlu *et al.* categorized this type as a *Random Forgery* [4]. Justino *et al.* categorized this type as a *Simple Forgery* [3]. Weiping *et al.* categorized this type as a *Casual Forgery* [5].
3. A forged signature imitating a genuine signature's model reasonably well is categorized as a *Simulated Forgery* by Justino *et al.* [3].
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.* [4].

5. Signatures produced by forgers after unrestricted practice by non-professional forgers are categorized as *Simple Forgery/Simulated Simple Forgery* by Ferrer *et al.* [6], and a *Targeted Forgery* by Huang and Yan [7].
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.* [4].

In this research, a random forgery refers to the 1st type and a targeted forgery refers to the 5th type.

2. Methodology

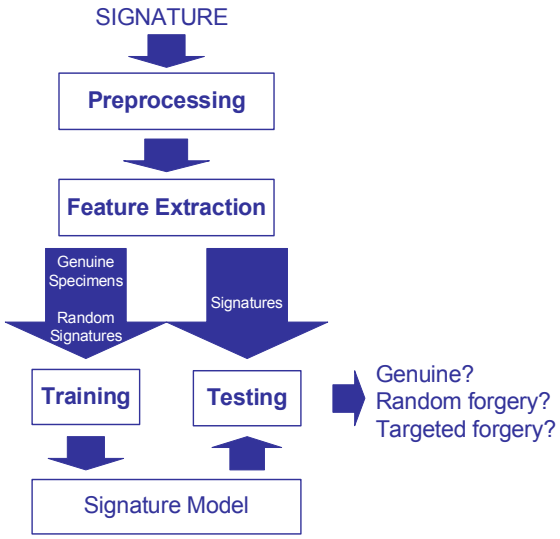

Figure 1. Verification process for signatures

It is sensible not to use targeted forgeries to train classifiers as the collection of such forgeries is impractical despite the potential of achieving higher accuracy. Figure 1 illustrates a general automated off-line signature verification system (AOSVS) that does not use targeted forgeries for training. This research employs a similar system in which an enhanced version of the MDF is integrated in the feature extraction process. In addition, a system that uses targeted forgeries for training is also investigated to evaluate the importance of targeted forgeries quantitatively.

2.1. Signature Database

The gpdsSIGNATURE [6] database which is publicly available for download at the URL: http://www.gpds.ulpgc.es/download/index.htm was employed to perform experiments in this research. It contains 160 signature sets of 24 genuine and 30 targeted signatures for each set. For each signer, all genuine specimens were collected in a single day's writing session. To produce forged signatures, the signers were allowed to practice their forgeries as long as he/she wished with static images of genuine specimens. Each of them imitated 3 signatures of 5 signers in a single day's writing session. The genuine signature shown to each forger was chosen randomly from the 24 genuine ones. Therefore for each genuine signature there are 30 skilled forgeries made by 10 forgers, using 10 different genuine specimens. Figure 2 shows some genuine samples and their imitations from the gpdsSIGNATURE database.

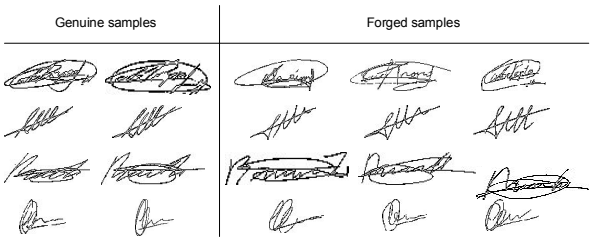

Figure 2. Genuine and Forged samples taken from the gpdsSIGNATURE database

2.2. Modified Direction Feature

The Modified Direction Feature (MDF) [8] utilizes the location of transitions from background to foreground pixels in the vertical and horizontal directions of the boundary representation of an object. For each transition, the Location of the Transition (LT) and the Direction Transition (DT) values are stored (as illustrated in Figure 3). An LT is calculated by taking the ratio between the position where a transition occurs and the distance across the entire image in a particular direction, whilst the DT is obtained by examining the stroke direction of an object's boundary at the position where a transition occurs. Finally, a local averaging process is applied to the LT and DT values obtained in each of the four possible traversal directions to reduce the feature vector size.

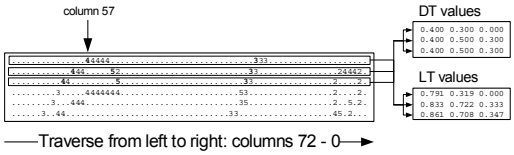

Figure 3. The extraction of LT and DT values along the left to right direction

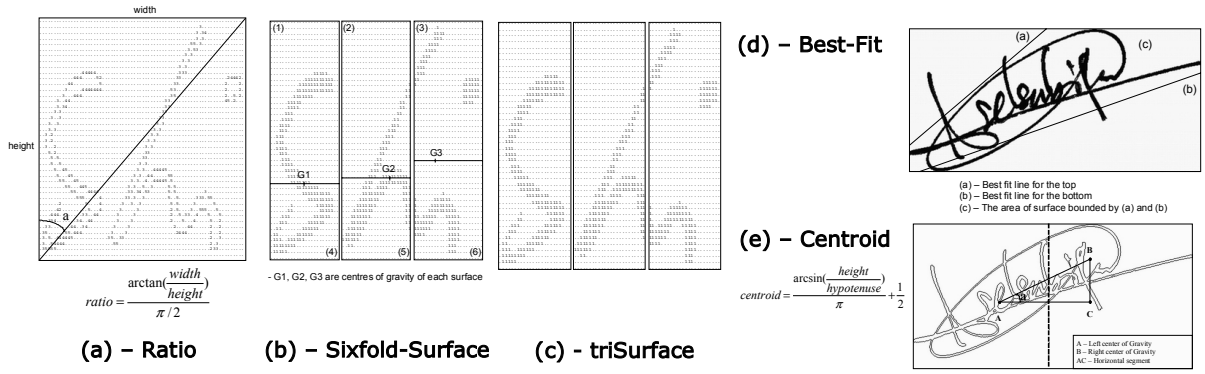

Figure 4. Extra features extracted for EMDF

2.3. Extra Features

Additional geometric features examined in this research are the Ratio [8], Length, Centroid, triSurface, Best-Fit, and the Sixfold-Surface feature [9].

The Ratio is a global feature that considers the proportion of the height and the width of the image of the signature as shown in Figure 4(a).

To obtain the Sixfold-Surface feature set, the signature image is first divided into three equal parts vertically. The centre of gravity is then calculated for each part to determine a horizontally separating line for each part. These separating lines divide each component into two domains. Six feature values are finally calculated by dividing the surface covered by the signature in a particular domain by the domain's area.

The triSurface is similar to the Sixfold-Surface feature except that the parts are not divided further into domains by horizontal separating lines.

In order to obtain an approximation for the signature's skew for the Best-Fit feature, a linear regression was applied to the minima and the maxima point sets of the signature to determine top and bottom best-fit lines. The angles created by these two lines with the horizontal formed the first two features after normalization. The signature surface area enclosed between these two lines became the third feature.

The Centroid feature relates to the dominant angle of the signature's pixel distribution. To determine the Centroid feature, the signature image is first divided into two equal parts. The position of the centre of gravity of each part is then determined. The angle which is created by the line that crosses these two points and the horizontal line (See Figure 4e) is then normalized for use in the feature vector.

The Length feature provides a contribution to the feature vector using the width of the signature following a normalization process.

2.4. Classifiers

Two types of neural networks, the MLP trained using Resilient Backpropagation and the Radial Basis Function network, were employed as classifiers in this research. Besides the main purpose of comparing the performance of classifiers in the absence of targeted forgeries in the training process, it is also of interest to see how the involvement of targeted forgeries in the training process would affect verification accuracy.

Another type of classifier, which was also investigated in this research is the Support Vector Machine (SVM), the relatively new statistical learning technique developed by Vapnik [10]. They implemented the idea of mapping the input vectors into a high-dimensional feature space through some nonlinear mapping. In such space, the optimal separating hyperplane is then searched. It is also based on a structural risk minimization principle (SRM). Two main objectives of the SRM induction principle are to control the empirical risk on the training samples and to control the capacity of the decision functions used to obtain that risk value.

A decision function of an SVM has the form of:

$$f(x) = sign(w \cdot x + b)$$

Given a set of training vectors S with l pairs (x_i, y_i) of samples:

$$S_l = ((x_1, y_1), \ldots (x_l, y_l)) \quad x_i \in \Re^n, y_i \in \{-1, +1\}$$

Each of these samples belongs to either two classes, $W_1(y_i = +1)$ or $W_2(y_i = -1)$.

SVM finds the hyperplane with the maximum Euclidian distance from the training set. According to the SRM principle, there will be only one optimal hyperplane (Figure 5) with the maximal margin δ defined as the distances from the hyperplane to the closest points of the two classes.

Dealing with non-separable training sets, the ith misclassified sample is assigned with a slack variable ξ_i representing the magnitude of the classification error.

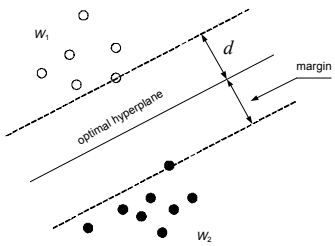

Figure 5. Optimal separating hyperplane maximizes the margin

The SVM solution for a non-separable training set can be found by keeping the upper bound on the Vapnik - Chervonenkis dimension minimized [11] and by minimizing an upper bound on the empirical risk with the following minimization:

$$\text{Minimise}_{\xi,\, w,\, b} \quad \langle w \cdot w \rangle + C\sum_{i=1}^{l} \xi_i$$

$$\text{Subject to} \quad y_i(\langle w \cdot x_i \rangle + b) \geq 1 - \xi_i, i = 1,...,l,$$

$$\xi_i \geq 0, i = 1,...,l.$$

C is the regularization constant determining the trade-off between the empirical error and the complexity term. The parameters are experimentally chosen by the user. A large C means a higher penalty for misclassifications.

The choice of kernel varies among classification problems and feature extraction techniques. With respect to the off-line signature verification problem, Ferrer *et al.* and Lv *et al.* reported their best results were achieved with the RBF [6] kernel whilst Justino *et al.* achieved their best results with the linear kernel [3]. In this research, three types of kernel were investigated: linear kernel, polynomial kernel, and RBF kernel.

All the experiments with SVM in this research were conducted using SVM^{light} version 6.01 created by Joachims [12].

2.5. Experimental Settings

Four different experimental settings were used. The number of random forgeries used in the training and the testing process were identical amongst the settings. The number of each type of signatures used for the training and the testing process of settings I and II are the same as settings III and IV respectively, except that the targeted forgeries were removed from the training process in settings I and II. Table 1 contains detailed information about the experimental settings.

The 400 random forgeries used to train each classifier were chosen from 100 randomly selected writers, four genuine signatures for each. 59 genuine signatures were chosen from the remaining 59 writers to represent random forgeries for testing.

2.6. Error Rate Decomposition

Table 1. Experimental settings for signature verification with and without using targeted forgeries for training

Setting	Phase	# Genuine	# Random	Targeted
I	Training	12	400	N/A
	Testing	12	59	15
II	Training	20	400	N/A
	Testing	4	59	5
III	Training	12	400	12
	Testing	12	59	15
IV	Training	20	400	25
	Testing	4	59	5

The accuracy of an AOSVS is usually measured by two types of error rate: False Rejection Rate (FRR) and False Acceptance Rate (FAR). However, systems can be challenged by random forgeries and targeted forgeries. Although it is much easier to detect and reject random forgeries, Justino *et al.* [13] reported that the forgeries detected in 95% of cases are random forgeries. As a consequence, the measurement of false acceptance rate for each type of forged signature, random forgery (FARR) and targeted forgery (FARG) is necessary.

The core problem of signature verification is to distinguish the genuine signatures from the targeted forged signatures. In this research, we use the Distinguishing Error Rate (DER), which is the average of FRR and FARG, as a metric to compare classifiers.

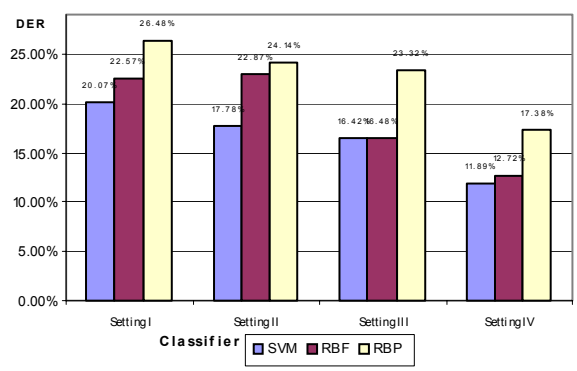

Figure 6. Performance of classifiers with different settings using the MDF-R feature set

3. Results and Analysis

As mentioned earlier, we used three types of kernel, linear, polynomial, and RBF, in our experiments with SVM. Kernel parameters were experimentally chosen and the best configurations were used for comparison purposes. It is observed that the RBF kernel had produced the best results.

Figure 6 shows the results of classifiers using

different settings and the MDF-R feature set. The results show that the use of targeted forgeries sufficiently assists the classifiers to provide better verification accuracy. For all the settings, SVM produced the better results as compared to RBF and RBP. The best results were obtained with Setting IV with the DER as low as 11.89%.

Following the introduction of targeted forgeries into the training process, it is noted that the performance of RBF was significantly improved (from 22.87% with Setting II down to 12.72% with Setting IV).

The FARR rates in experiments with SVM were also well under 1% (0.16% with Setting II) and are comparable to FARR rates reported by Justino *et al.* [3] and Ferrer *et al.* [6]. Taking this type of error into account, the proposed system is comparable to that of Ferrer *et al.* [6]. Meanwhile, a direct comparison to the research proposed by Justino *et al.* [3] is not feasible as the definition of forgeries and their collection process were not identical to that proposed in this research.

Figure 7 summarizes results employing the MDF-R plus extra features (MDF-R-CTLFS). The results achieved with the SVM classifier approximate to those achieved using the MDF-R feature set. Using the RBP classifier, the enhanced MDF feature set assisted in reducing the DER significantly. The best result (DER: 9.21%) employing the MDF-R-CTLFS feature set was achieved with Setting IV using the RBF classifier.

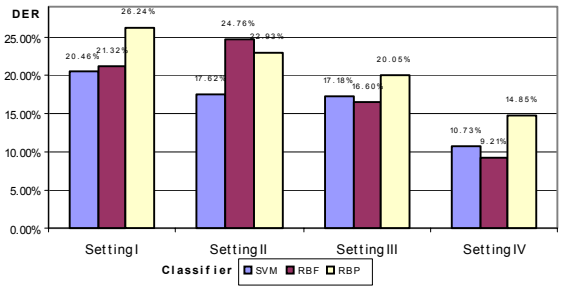

Figure 7. A comparison amongst classifiers with different settings using the MDF-R-CTLFS feature set

4. Conclusions

This research compared the performance of RBF, RBP neural networks, and SVM as classifiers in an AOSVS employing an enhanced MDF technique under two specific conditions. One condition is the distribution of samples used for training and the other is the use of targeted forgeries in the training process. Under both conditions, the results obtained using SVM were more favorable than RBF and RBP.

Further work will involve the investigation of other machine learning techniques as well as the addition of rotation invariant geometric global features for enhancing the verification process.

References

[1] R. Guest, "Age dependency in handwritten dynamic signature verification systems," *Pattern Recognition Letters*, vol. 27, pp. 1098-1104, 2006.

[2] R. Sabourin, G. Genest, and F. J. Preteux, "Off-line signature verification by local granulometric size distributions," *PAMI, IEEE Transactions on*, vol. 19, pp. 976-988, 1997.

[3] E. J. R. Justino, F. Bortolozzi, and R. Sabourin, "A comparison of SVM and HMM classifiers in the off-line signature verification," *Pattern Recognition Letters*, vol. 26, pp. 1377-1385, 2005.

[4] M. Hanmandlu, M. H. M. Yusof, and V. K. Madasu, "Off-line signature verification and forgery detection using fuzzy modeling," *Pattern Recognition*, vol. 38, pp. 341-356, 2005.

[5] H. Weiping, Y. Xiufen, and W. Kejun, "A survey of off-line signature verification," in *Intelligent Mechatronics and Automation, 2004. Proceedings. 2004 International Conference on*, 2004, pp. 536 - 541.

[6] M. A. Ferrer, J. B. Alonso, and C. M. Travieso, "Offline geometric parameters for automatic signature verification using fixed-point arithmetic," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 27, pp. 993-997, 2005.

[7] K. Huang and H. Yan, "Off-line signature verification using structural feature correspondence," *Pattern Recognition*, vol. 35, pp. 2467-2477, 2002.

[8] M. Blumenstein, X. Y. Liu, and B. Verma, "A Modified Direction Feature for Cursive Character Recognition," in *International Joint Conference on Neural Networks*, 2004, pp. 2983-2987.

[9] S. Armand, M. Blumenstein, and V. Muthukumarasamy, "Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural-based Classification," in *Intl. Joint Conference on Neural Networks*. Sheraton Vancouver Wall Centre, Vancouver, BC, Canada, 2006, pp. 1663-1670.

[10] V. Vapinik, *Statistical Learning Theory*. New York: Wiley, 1998.

[11] C. J. C. Burges, "A Tutorial on Support Vector Machines for Pattern Recognition," *Data Mining and Knowledge Discovery*, vol. 2, pp. 121-167, 1998.

[12] T. Joachims, "Optimizing search engines using clickthrough data," in *The 8th ACM SIGKDD intl. conf. on Knowledge discovery and data mining*. Edmonton, Alberta, Canada ACM Press, 2002, pp. 133-142.

[13] E. J. R. Justino, A. E. Yacoubi, F. Bortolozzi, and R. Sabourin, "An Off-line signature verification using Hidden Markov Model and Cross-Validation," in *13th Brizilian Symposium on Computer Graphics and Image Processing*. Gramado, Brazil, 2000, pp. 105-112.