

Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural-based Classification

Stéphane Armand, Michael Blumenstein and Vallipuram Muthukumarasamy

Abstract—Signatures continue to be an important biometric for authenticating the identity of human beings. This paper presents an effective method to perform off-line signature verification using unique structural features extracted from the signature's contour. A novel combination of the Modified Direction Feature (MDF) and additional distinguishing features such as the centroid, surface area, length and skew are used for classification. A Resilient Backpropagation (RBP) neural network and a Radial Basis Function (RBF) network were compared in terms of verification accuracy. Using a publicly available database of 2106 signatures (936 genuine and 1170 forgeries), verification rates of 91.21% and 88.0% were obtained using RBF and RBP respectively.

I. INTRODUCTION

Within the field of human identification, the usage of biometrics is growing because of its unique properties such as hand geometry, iris scan, fingerprints or DNA. The use of signatures has been one of the more convenient methods for the identification and verification of human beings. A signature may be termed a behavioural biometric, as it can change depending on many elements such as: mood, fatigue, etc. The challenging aspects of automated signature identification and verification have been, for a long time, a true motivation for researchers. Research into signature verification has been vigorously pursued for a number of years [1] and is still being explored (especially in the off-line mode) [2]. On-line verification must be differentiated from off-line verification, as the number of features, which may be extracted from on-line mediums, exceed those obtained from off-line verification i.e. time, pressure and speed can be extracted from on-line modes of verification [3]. Previous approaches, such as that based on fuzzy modeling and the employment of the Takagi-Sugeno model, have been proposed using angle features extracted from a box approach to verify and identify signatures [4]. Also, The GSC (Gradient, Structural and Concavity) feature

extractor provided results as high as: 78% for verification and 93% for identification [5]. Various classifiers, such as Support Vector Machines (SVMs) and Hidden Markov Models (HMMs), have also been successful in off-line signature verification; SVMs providing an overall better result than the HMM-based approach [6]. Research into person identification/verification, including physical traits, fingerprint and signature analysis has also been investigated [7].

In the field of pattern recognition, choosing a powerful set of features is crucial for both the application and the classifier. H. Lv *et al* used the direction distribution, moment feature, stroke width distribution and grey distribution to conduct signature verification [8].

Previous work using the Modified Direction Feature (MDF) generated encouraging results, reaching an accuracy of 81.58% for cursive handwritten character recognition [9]. As an extension to previous work, the research in this paper adapts, extends and investigates MDF with signature images. Specifically, a number of features have been combined with MDF, to capture various structural and geometric properties of the signatures being investigated. The verification process implies the usage of forged signatures, discriminating the genuine from the forged. In this paper, we present experimental results for signature verification using MDF, and propose some modifications of the features extracted.

S. Armand is with the School of Communication and Information Technology, Griffith University, Gold Coast Campus, PMB 50, Gold Coast Mail Centre, Queensland 9726, Australia. (phone: +61 7 5552 8271; fax: +61 7 5552 8066; e-mail: stephane.armand@student.griffith.edu.au)

M. Blumenstein is with the School of Communication and Information Technology, Griffith University, Gold Coast Campus. (e-mail: m.blumenstein@griffith.edu.au)

V. Muthukumarasamy is with the School of Communication and Information Technology, Griffith University, Gold Coast Campus. (e-mail: v.muthu@griffith.edu.au)

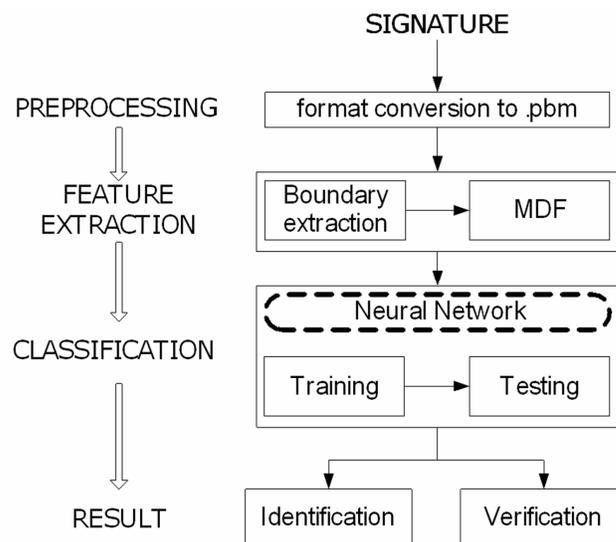


Figure 1: Procedure to identify/verify a signature from a database

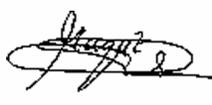
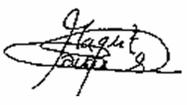
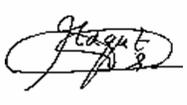
GENUINE SAMPLES	FORGED SAMPLES		
			
			
			
			

Figure 2: Signature Samples

II. METHODOLOGY

To perform verification or identification of a signature, several steps must be performed. After preprocessing all signatures from the database by converting them to a portable bitmap (PBM) format, their boundaries are extracted to facilitate the extraction of features using MDF. Verification experiments are performed with neural-based classifiers. Figure 1 illustrates the signature verification process.

A. Signature Database

Experiments have been performed with the “Grupo de Procesado Digital de Senales” (GPDS) signature database [10]. The results provided in this research used a total of 2106 signatures.

From those 2106 signatures, we used 39 sets of signatures and, for each set, 24 samples of genuine and 30 samples of forgeries.

Samples of the genuine and forged signatures are displayed in Figure 2.

B. Boundary Extraction

The boundary of each signature must be extracted prior to the feature extraction process. As we are using neural classifiers, the amount of data used as input to perform verification is an important parameter. Having a large input vector size could dramatically increase the complexity and training time of the classifier, in addition to potentially decreasing the accuracy of the system. Thus, the binary image of each signature is processed, and the contour is extracted, providing the first step in the process of reducing the amount of data describing each pattern. Figure 3 shows the extraction of a signature's boundary [9].

C. Feature Extraction with MDF

The features extracted must be appropriate for both the application and the classifier used. MDF has been used to extract features for the signature verification problem. Related work using MDF is described in [9]. This technique employs a hybrid of two other feature extraction techniques, Direction Feature (DF) and the Transition Feature (TF).

DF extracts direction transitions (DT), based on the replacement of the foreground pixels by their direction

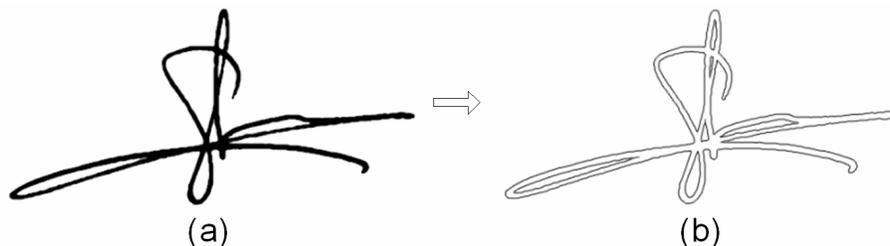


Figure 3: Example of boundary extraction from a signature: (a) original signature, (b) following boundary extraction

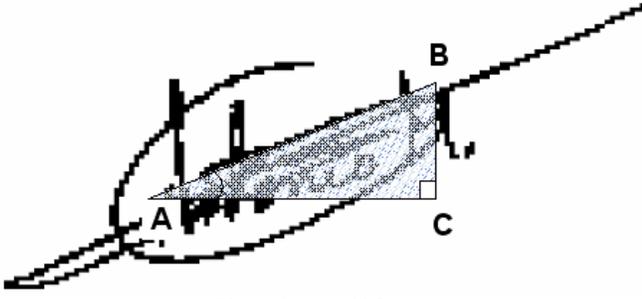


Figure 4: centroid feature

values, which are categorized by five different direction numbers: vertical direction value = 2, right diagonal value = 3, horizontal direction value = 4, left diagonal value = 5 and intersections = 9. The feature vector is extracted by zoning and computing the most representative direction values in a given zone.

TF records the locations of the transitions (LTs) between foreground (1s) and background (0s) in binary digital images. The image is traversed from the following directions: left to right, right to left, top to bottom and bottom to top. Each time a change from '0' to '1' or from '1' to '0' occurs, the ratio between the location of the transition and the length/width of the image traversed is recorded as a feature. An averaging algorithm is used to obtain a feature vector of appropriate size in order to decrease the training/classification time. These are based on the extraction technique present in TF.

Not only are the locations of the transitions calculated, but also the corresponding direction values are determined, facilitating the storage of LTs and DTs. The width to height ratio feature was also included to comprise MDF.

D. The Centroid Feature

Another feature was considered in this research relating to the dominant angle of the signature's pixel distribution, the 'centroid'.

First, the signature image was separated into two equal parts. The position of the centre of gravity in each part was calculated (A and B in Figure 4). The angle between the horizontal axis and the line obtained by linking the two centres of gravity was the feature added. To convert this angle in the range of 0 to 1, calculations were performed with the coordinates of the centres of gravity. A right triangle was considered using the centres of gravity as the extreme points of its hypotenuse, the row of the first centre of gravity and the column of the other, intersecting to form the right angle.

To obtain the 'centroid' feature, the angle α was first considered in the left part of the triangle, and then a calculation was performed, in order to restrict the value in the range of 0 and 1. Equations (1) and (2) are followed to get this value. The concept is shown in Figure 4. The angle α is illustrated at point A.



Figure 5: triSurface feature

$$\alpha = \frac{\arcsin\left(\frac{\text{height}}{\text{hypotenuse}}\right)}{\pi} \quad (1)$$

$$\text{centroid} = \alpha + \frac{1}{2} \quad (2)$$

E. The TriSurface Feature

The surface area of two visually different signatures could be the same. For the purpose of increasing the accuracy of a feature describing the surface area of a signature, the 'triSurface' feature was investigated, as an extension, in which the signature was separated into three equal parts, vertically.

The surface area feature is the surface covered by the signature, including the holes contained in it. The total number of pixels in the surface was counted, and the proportion of the signature's surface over the total surface of the image was calculated.

This process was used for the three equal parts of the signature, giving three values between 0 and 1. Figure 5 illustrates this concept.

F. The Length Feature

The length feature represents the length of the signature, after scaling all the signatures from the database to the same height. In order to obtain a value between 0 and 1, the minimum signature length obtained in the whole database was considered as 0, and the maximum signature length was considered to be 1. The remaining signature lengths were then converted to values between this minimum and maximum range.

G. The Sixfold-Surface Feature

This feature is different from the TriSurface feature mainly in two ways. Firstly, the number of feature values obtained is doubled to six with the Sixfold Surface.

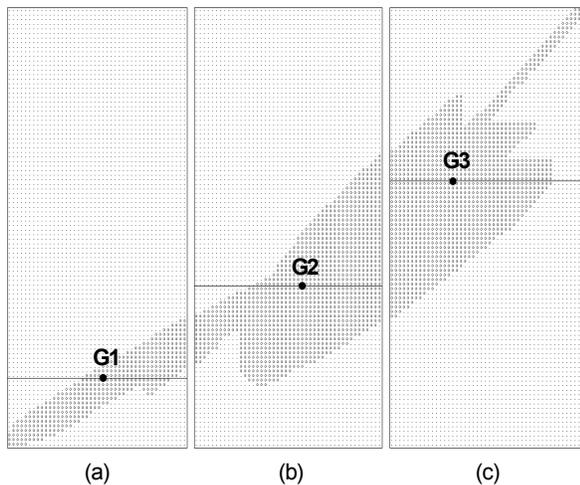


Figure 6: SixFold Surface feature. G1, G2 and G3 are the center of gravity for the respective sections (a), (b) and (c)

Secondly, centers of gravity are determined to assist in the calculation of the six-fold surface features.

The signature image is first divided into three parts vertically. The center of gravity is calculated for each of the three parts and the signature surface above and below the horizontal line of the center of gravity (giving two sub sections for each part) was calculated. The result was a set of six feature values, corresponding to the surface of the six sub-sections as illustrated in Figure 6.

H. The Best-fit Feature

The line of best fit usually attempts to represent a scatter of points in an area. In order to obtain an approximation for the signature's skew, the line of best fit using minima and maxima from the bottom edge of the signature was calculated. Similarly the line of best fit from the top of the signature was also calculated. In each case, this calculation was performed after determining the slope of the line. The angles between each of these lines and the X-axis were calculated, giving two features. The surface area enclosed between the two lines became the third feature. Figure 7 depicts the concept.

I. Neural Network Classifier

Two neural network classifiers were used to verify the signatures: the Resilient Backpropagation (RBP) neural network and the Radial Basis Function (RBF) network. The database was split into two parts, to perform the training and testing components. From the genuine set, 18 samples of each signature were used for training, and 6 for testing. We used 22 samples of each signature for training the forged signatures and 8 for testing purposes. Parameters such as the number of iterations and hidden units were varied extensively for RBP during experimentation; also the number of centres was varied between 40 and 10000 for the RBF network. Both of the classifiers used 40 outputs to classify the signatures: 39 outputs for each different set of signatures, and the last output for the forgeries.

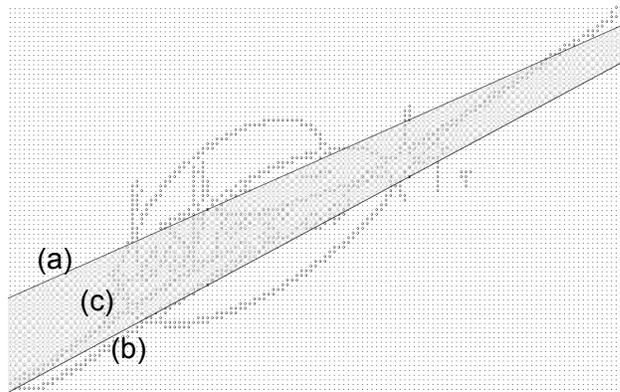


Figure 7: Best-Fit features. (a) and (b) are respectively the line of best fit for the top and the bottom, (c) represents the surface between the two lines.

III. EXPERIMENTS

The signatures were firstly converted into a Portable Bitmap (PBM) format in order to facilitate processing as binary images. Subsequently, their boundaries were extracted for further processing.

An adapted version of MDF (including the new features described in the previous sub-sections) was used for feature extraction. The features were values scaled between 0 and 1, to facilitate neural network training for experimentation. C, Java and the Matlab environment were used for implementing and investigating the proposed techniques.

A. Verification with MDF

Using MDF, a total of 121 values were obtained. Modifications of the MDF technique have been proposed to improve classification accuracy, with the hypothesis that adding distinguishing features could improve the verification rate. Experiments with MDF merged with each new feature, or a combination of new features were conducted separately, increasing the feature vector up to 126 inputs.

B. 4-Fold Validation

Four-fold cross validation was used in this research. The signatures from the database were partitioned into four equal sections in their related type (genuine or forged). Thus, four sections for the genuine, and four sections for the forged, resulted from this partition. Three sections of each were used for training, and testing was performed with the remaining unseen signature sets. As a result, four training and testing sets were obtained, and experiments were run four times with the different sets, obtaining varying results. By doing so, the results for signature verification were suitably validated.

IV. RESULTS AND DISCUSSION

The verification process is different from identification, as forged signatures are also part of the database in the former;

TABLE I
RESULTS USING THE RBP NEURAL NETWORK CLASSIFIER

	Verification Rate [%]				
	Set 1	Set 2	Set 3	Set 4	Sets Avg.
MDF	83.33	88.64	87.18	85.16	86.08
MDF-C	84.07	87.91	89.56	87.73	87.32
MDF-T	85.53	86.45	87.55	87.91	86.86
MDF-L	84.43	88.10	89.01	85.35	86.72
MDF-S	83.88	83.52	88.46	86.26	85.53
MDF-F	83.33	87.36	88.28	84.98	85.99
MDF-CT	84.43	87.36	88.46	89.56	87.45
MDF-CL	82.23	87.73	84.98	86.45	85.35
MDF-TL	82.97	86.63	87.18	89.19	86.49
MDF-CS	84.62	89.01	88.28	88.64	87.64
MDF-CF	83.15	88.64	87.18	85.90	86.22
MDF-TF	83.52	87.00	87.91	87.18	86.40
MDF-TS	79.85	89.01	88.46	87.91	86.31
MDF-LF	83.15	86.63	87.00	87.18	85.99
MDF-LS	83.70	88.46	88.83	85.16	86.54
MDF-FS	87.36	87.91	88.64	86.63	87.64
MDF-CTL	81.68	87.36	87.36	87.18	85.90
MDF-CLF	83.15	87.36	89.19	87.36	86.77
MDF-CTLF	87.36	87.73	89.74	87.18	88.00
MDF-CTLFS	83.52	86.63	90.66	87.55	87.09

C = centroid, T = TriSurface, L = length, S = Sixfold-Surface,
F = Best-fit

the classifier was required to distinguish between genuine and forged signatures. Optimally, results should show a high acceptance rate for the genuine and a high rejection rate for forged signatures. In the following experiments, 1560 signatures for training and 546 signatures for testing were used to conduct verification.

This section describes the results obtained experimenting as follows: MDF in its original version, or with one or more of the extra features: centroid (C), triSurface (T), length (L), sixfold-surface (S) and the best-fit (F). As shown in Table I and Table II, MDF merged with other features outperformed the original version of MDF, for most of the experiments. Using RBP, the best result obtained reached 88% verification rate (v. r.), with MDF-CTLF. Using RBF, MDF-CTLFS obtained the best result, reaching 91.21% v. r.

A. Comparison between RBP and RBF

Using the RBF classifier, the results obtained were better overall in comparison with the RBP classifier. Using different algorithms, and having different configurations, the comparison between RBP and RBF is made only on the basis of the best results obtained, upon conducting the experiments. Table I and Table II displays the results obtained. The results obtained with RBF were always higher than the RBP results. However, to conduct the RBF experiments, an allocation of more memory was needed. Figure 8 illustrates the comparison between RBP and RBF.

TABLE II
RESULTS USING THE RBF NEURAL NETWORK CLASSIFIER

	Verification Rate [%]				
	Set 1	Set 2	Set 3	Set 4	Sets Avg.
MDF	87.91	90.48	89.74	90.29	89.61
MDF-C	88.10	89.74	90.11	89.93	89.47
MDF-T	87.73	90.48	89.93	90.11	89.56
MDF-L	89.01	91.21	90.66	90.66	90.38
MDF-S	89.38	90.11	91.03	91.03	90.38
MDF-F	88.28	90.66	90.11	90.66	89.93
MDF-CT	88.28	90.29	90.11	89.74	89.61
MDF-CL	88.10	90.84	89.74	90.29	89.74
MDF-TL	89.38	87.91	89.38	88.46	88.78
MDF-CS	88.10	90.29	90.66	90.11	89.79
MDF-CF	88.28	91.39	90.11	90.11	89.97
MDF-TF	88.10	90.29	90.84	91.21	90.11
MDF-TS	88.46	90.84	90.29	90.84	90.11
MDF-LF	89.38	91.21	90.84	91.94	90.84
MDF-LS	89.74	91.03	90.48	91.21	90.61
MDF-FS	90.11	89.93	90.84	91.03	90.48
MDF-CTL	89.19	91.76	91.94	91.58	91.12
MDF-CLF	88.83	91.58	90.84	91.39	90.66
MDF-CTLF	88.10	91.94	91.94	92.31	91.07
MDF-CTLFS	88.83	92.31	91.94	91.76	91.21

B. Comparison between MDF and MDF-CTLFS using RBF

In order to evaluate which of the feature configurations were the most successful between MDF and MDF combined with all the features investigated (MDF-CTLFS), it is possible to directly compare the best results obtained. As shown in Table II, MDF provided a verification rate of 89.61%, and MDF-CTLFS gave a verification rate of 91.21%. However, it is not accurate to conclude that MDF-CTLFS is definitely better than MDF, based only on these figures. Another way is to conduct hypothesis testing.

By observing the results obtained from identical network configurations, MDF-CTLFS performed better in terms of providing a better recognition rate. It is hypothesised that the population mean recognition rate of MDF-CTLFS is higher than the population mean recognition rate of MDF.

Hypothesis testing is formulated as such: let μ_d be the population mean verification accuracy between MDF and MDF-CTLFS; let \bar{d} be the sample mean of the difference between MDF and MDF-CTLFS. The testing was performed at a 0.1% significance level using the matched pairs method. Let X1 denote each data point obtained by MDF-CTLFS and X2 each data point from MDF.

Important figures can be obtained from the matched pairs. They are 1) the number of data points, denoted by n , 2) the difference between two matched pairs, $d = X1 - X2$, 3) the sample standard deviation of the differences between two sets of data. The difference between each matched pair value is displayed in Table III.

TABLE IV
ANALYSIS OF THE RATES OBTAINED WITH MDF-CTLFS

		Test Set Recognition [%]					
		Set 1	Set 2	Set 3	Set 4	Sets Avg.	
GENUINE	Accepted ⁽¹⁾	85.04	89.32	90.17	90.17	88.68	
	Rejected as Forged ⁽²⁾	11.97	9.40	9.83	10.26	10.36	
	Misclassified as another Genuine ⁽³⁾	2.99	1.28	1.28	1.28	1.71	
FORGERIES	Rejected ⁽⁴⁾	91.67	94.55	93.27	94.87	93.59	
	Misclassified as its Genuine ⁽⁵⁾	4.49	2.88	3.21	3.53	3.53	
	Misclassified as a Genuine ⁽⁶⁾	3.85	2.56	3.53	1.60	2.88	
GENUINE AND FORGERIES		Total Corrects	88.83	92.31	91.94	91.76	91.21

(1) percentage of genuine accepted signatures, (2) percentage of genuine signatures rejected as forgeries, (3) the percentage of genuine misclassified as another genuine, but not as a forgery, (4) A rejected forgery is the desired result from a forgery test. The number displayed is the rate of forgeries correctly rejected, (5) percentage of forgeries classified as their equivalent genuine signatures, (6) denotes a forged signature misclassified as a genuine, which is not the forged genuine

16 data points were taken to perform the calculation, and a result of 1.454 was found for the sample mean.

$$\bar{d} = 1.454 \quad (3)$$

$$S_d = \sqrt{\frac{\sum (d - 1.454)^2}{n - 1}}$$

$$S_d = 1.178 \quad (4)$$

And the hypothesis testing steps are:

Step 1) $H_0 : \mu_d = 0$

$H_{alt} : \mu_d > 0$

Step 2) $n = 16, \bar{d} = 1.454, S_d = 1.178$

Step 3) Critical values:

Degrees of freedom = 15

$t_{0.001} = 3.733$

Step 4) Test statistic

$$t = \frac{\bar{d} - \mu_d}{S_d / \sqrt{n}} = \frac{1.454 - 0}{(1.178 / \sqrt{16})} \quad (5)$$

$t = 4.934$

Step 5) According to the calculation, t was found superior to $t_{0.001}$, as shown in Figure 9. The statistical test used, provides sufficient evidence to conclude that MDF-CTLFS has a higher verification accuracy on average than MDF (for the database used) at a 0.1% significance level. In other words, there is 99.9% confidence that on average, MDF-CTLFS outperforms MDF.

C. Analysis of the rates obtained with MDF-CTLFS

An advantage of using 40 outputs (39 for the genuine set of signatures, one for the forged sets) for neural verification is the possibility of analyzing the output obtained following experimentation. In Table IV, different rates obtained for each set are shown as a result of experimentation with the highest performing feature and classifier combination (MDF-CTLFS and RBF).

Amongst the genuine signatures, on average, 88.68% of these were correctly verified, and 93.59% forged were correctly rejected. No more than 12% of genuine signatures were rejected as forged signatures. A maximum of 3% of the genuine signatures were misclassified as another genuine category. From one perspective, it may be observed that it could be preferable to have a signature rejected, rather than

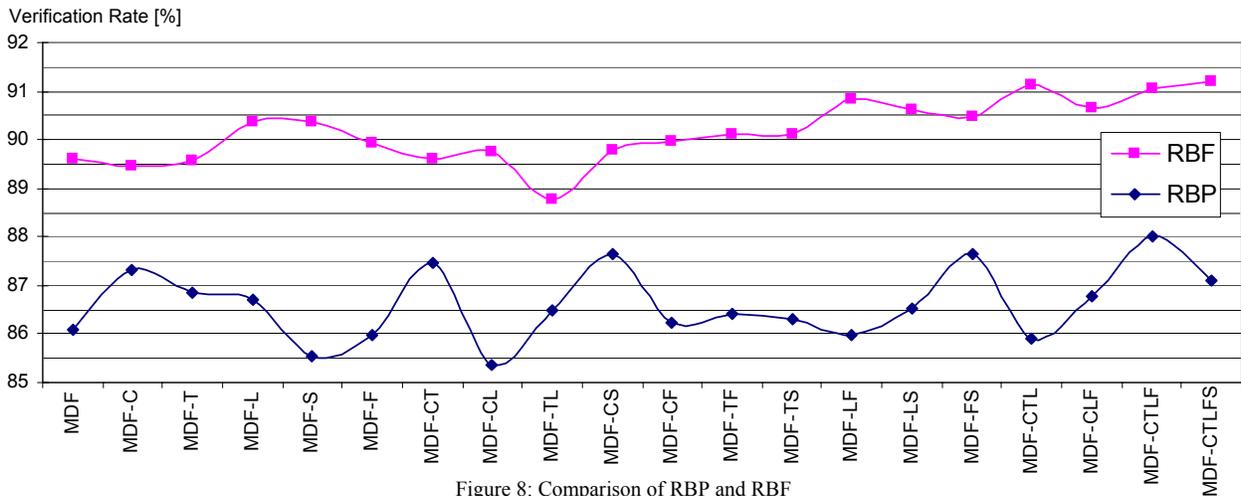


Figure 8: Comparison of RBP and RBF

TABLE III

OBTAINING VALUES FOR HYPOTHESIS TESTING

X1	X2	d = X1-X2
84.07	82.42	1.65
86.45	86.08	0.37
87.36	87.55	-0.18
87.00	87.00	0.00
87.73	86.81	0.92
90.29	89.01	1.28
91.94	88.46	3.48
89.74	86.81	2.93
88.10	87.91	0.18
91.58	91.21	0.37
92.86	90.11	2.75
92.67	89.56	3.11
88.83	87.91	0.92
92.31	90.48	1.83
91.94	89.74	2.20
91.76	90.29	1.47

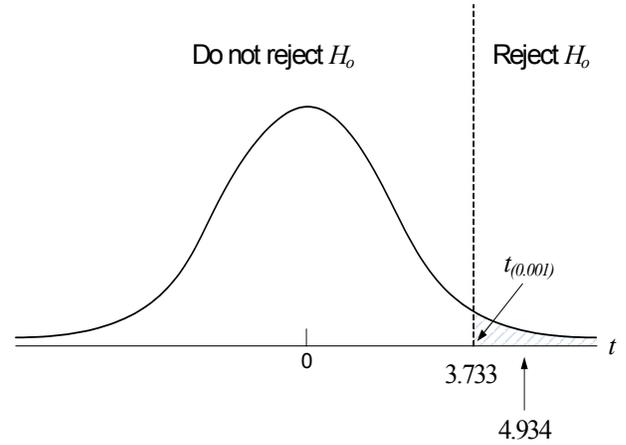
misclassified as another genuine signature.

Amongst the forged signatures, an average of 93.59% were correctly rejected. 4.49% was the maximum rate for the forgeries misclassified as their genuine signature equivalents. A maximum of 3.85% were misclassified as another genuine signature.

D. Comparison of verification rate with other researchers

It is difficult to compare the results obtained in this paper with those of other researchers as many have used different databases for experimentation. However, a general comparison can be performed with the researchers that proposed the GPDS database. As mentioned previously, the database used in the current research contains 39 sets of signatures from the GPDS database; this was the only subset available when the experiments were conducted. The full GPDS database contains a total of 160 sets of signatures.

The proposed system, using a single neural network classifier for training and testing, reached a verification accuracy of 91.21%. In their research, Martinez *et al* obtained their best results with HMMs, showing a 2.2% error rate using random forgeries, and a 14.1% error rate using simple forgeries. The objective of their verification system was to differentiate the genuine from the forgeries. Using a random forgery meant that the signature sample belonged to a writer, which was different to those used in the signature model. In this paper, each single signature from the testing set was presented to the trained neural classifier for verification. Consequently, a tested signature, genuine or forged, is not assumed to be known before being classified. Hence, although it is difficult to directly compare the results in this paper with those presented by Martinez *et al.* (due to the difference in experimental methodology and database size), it is possible to observe that the results are

Figure 9: Area of the right-tailed hypothesis: $t > t_{0,001}$

favourable in comparison.

V. CONCLUSIONS

The principal objective of this paper was to investigate the efficiency of the enhanced version of the MDF feature extractor for signature verification. Investigations adding new feature values to MDF were performed, assessing the impact on the verification rate of the signatures, using 4-fold cross validation. Two different neural classifiers were used. Most of the experiments conducted with MDF that were merged with the new features obtained better results than the original MDF. Using RBP, MDF reached an 86.08% v. r., and MDF-CTLF reached 88% v. r. The RBF classifier provided better results than the RBP classifier overall. The best v. r. obtained reached 91.21% with MDF-CTLFS, the combination of all the features described in this paper.

In future research, investigations will be conducted to enhance the feature extraction process. These include further combinations and investigations of the features. In addition, a larger signature database will be collected, including multilingual signatures, to investigate the techniques proposed in this paper. Finally, additional classifiers will be investigated including Support Vector Machines (SVMs) for verifying the signatures.

REFERENCES

- [1] K. Han, and I.K. Sethi, "Handwritten Signature Retrieval and Identification", *Pattern Recognition* 17, 1996, pp. 83-90.
- [2] S. Chen, and S. Srihari, "Use of Exterior Contour and Shape Features in Off-line Signature Verification", *8th International Conference on Document Analysis and Recognition (ICDAR '05)*, 2005, pp. 1280-1284.
- [3] A. Kholmatov, and B. Yanikoglu, "Identity Authentication using improved online signature verification method", *Pattern Recognition Letters*, 2005, in press.
- [4] M. Hanmandlu, M.H.M. Yusof, and V.K. Madasu, "Off-line Signature Verification using Fuzzy Modeling", *Pattern Recognition* 38, 2005, pp. 341-356.
- [5] M.K. Kalera, S. Srihari, and A. Xu, "Off-line signature verification and identification using distance statistics", *International Journal of Pattern Recognition and Artificial Intelligence* 18(7), 2004, pp. 1339-1360.

- [6] 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* 26, 2005, pp. 1377-1385.
- [7] H. Srinivasan, M. J. Beal and S.N. Srihari, "Machine Learning approaches for Person Identification and Verification", *SPIE Conference on Homeland Security*, 2005, pp. 574-586.
- [8] H. Lv, W. Wang, C. Wang and Q. Zhuo, "Off-line Chinese Signature Verification based on Support Vector Machines", *Pattern Recognition Letters* 26, 2005, pp. 2390-2399.
- [9] M. Blumenstein, X.Y. Liu, and B. Verma, "A Modified Direction Feature for Cursive Character Recognition", *International Joint Conference on Neural Networks (IJCNN '04)*, 2004, pp. 2983-2987.
- [10] L.E. Martinez, C.M. Travieso, J.B. Alonso, and M. Ferrer, "Parametrization of a forgery Handwritten Signature Verification using SVM", *IEEE 38th Annual 2004 International Carnahan Conference on Security Technology*, 2004, pp. 193-196.