Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-8, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

A Feature group based approach to Offline Signature Verification using Neural Networks and Support Vector Machines

Mrs. Yogita Praful Gawde [1] & Dr. Balaji G. Hogade.[2]
[1]Electronics and Telecommunication Department ARMIET, Asangaon, Mumbai University, India
[2] Electronics and Telecommunication Department, Terna College of Engineering, Nerul navimumbai India

Abstract: *Handwritten signatures form the most natural technique of authenticating a individual's identity in banking process. People with malicious intention do forge the signatures for getting undue benefit. This work looks at the process of automating the identification process of signature authentication using computers. The techniques used are based on Artificial intelligence (AI) based methods of Neural Networks (NN) and Support vector Machines (SVM). The work herein presents a method of using both of the above for the purpose with support from Image Processing (IP) techniques. The work makes use of Spatial and transform domain techniques from IP for signature feature generation and evaluates 16 different feature combinations for the signature verification task. At the end the better one of them is identified using Accuracy as the performance measure.*

1. Introduction

Banking user signature verification in general is divided in two types - off line and online signature verification. The off-line signature verification is designed with a view to decide whether a signature originates from a given user of the banking system, it uses a scanned image of the users signature to be verified along with a set of users original signature images. The online verification system needs a setup of specialised signature acquisition hardware. The off-line signature verification can be implemented easily after the regular signing process, and so is less intrusive and more user friendly, but lacks the availability of signatures dynamic features like stroke information, pressure and velocity available from the stylus (pen)tip.[1]

The aim of off-line signature verification is to decide, whether a signature originates from a given signer based on the scanned image of the signature and a few images of the original signatures of the signer. Unlike on-line signature verification, which requires special acquisition hardware and setup, off-line signature verification can be performed after the normal signing process, and is thereby less intrusive and more user friendly. The past approaches in offline signature verification systems indicate that the human experts exhibit an error rate of about 1% in distinguishing between the forged and valid signatures whereas the best systems designed for the purpose deliver a error rates in range of 5%. [2].

Generally signature verification system follow an approach which has three phases. First one is of extracting certain features from the images of signatures, then they evaluate them as a indicator of a certain class and lastly, make use of some kind of classifier to declare whether a given signature is an original or a forgery [3].

A good amount of effort has been done in applying neural networks (NN) to signature verification (SV) have been undertaken in past with a varying degree of success [4,5]. This work is based on evaluating the opportunities in the second and final phase of signature verification. In this work, we are concerned with the design of an Offline Signature Verification System that could be used in practice. For this reason, we restrict our analysis to methods that do not rely on skilled forgeries for the users enrolled in the system, since this is not the case in practical applications. We do consider, however, that a dataset consisting of genuine signatures and forgeries that will differentiate among the signature images depending on feature sets.

A complete neural network based classification method is demonstrated to show how some of the limitations of off-line signature verification can be overcome to make them have performance nearing those of human experts. Experimental results are provided to evaluate a variety of features being used with the neural network based classification system. Multiple signature features (e.g., height, width, axis of signature, number of breaks in signature etc.) are extracted from the signature image and used to train the NN and SVM. The NN and SVM models are developed and then tested and their accuracy is compared for various signature feature groups.

2. Objective

The present work has following objectives:

- Design a system to prove genuineness or authentication of a person's signature using Neural network and SVM based models.
- Identify some features of a genuine signature to distinguish it from the forged one.
- Analyze the skilled forgery by extracting features and comparing it with features of genuine one.
- Compare various configurations model for the purpose of identifying a good one to use for the signature verification system.
- Make use of performance metrics of Accuracy and False Acceptance Rate(FAR), False Rejection Rate (FRR) of the system after comparing performance of both models set viz. 1. Neural network and 2. Support Vector Machines (SVMs).

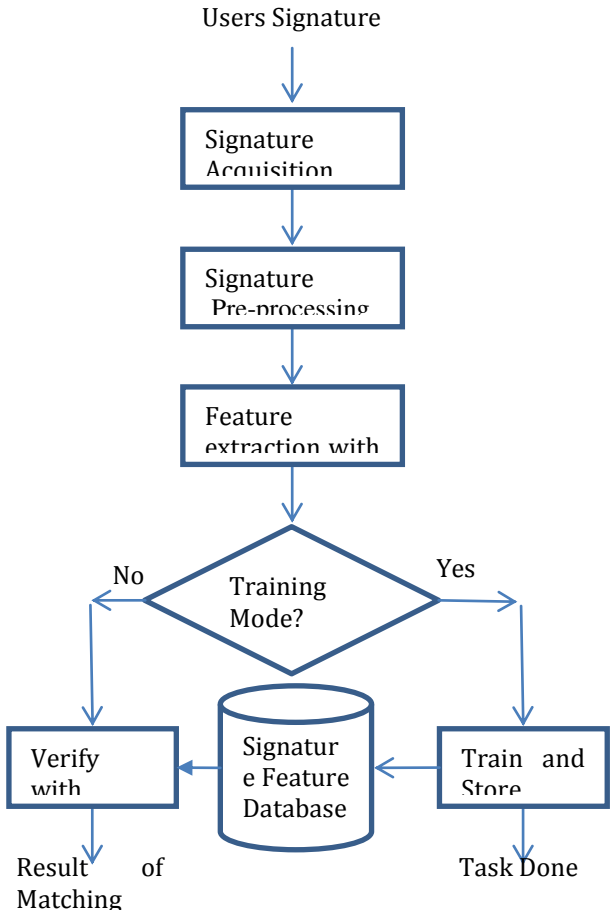

Fig-1: Flow of the Signature Verification system

3. Methodology

3.1 Overview

This section details the method employed in the system development. It details the pre-processing followed by signature database structure, and the NN features. The steps involved are : Signature Acquisition, Pre-processing, Feature Extraction with grouping, NN Training and Matching. Fig.1 depicts the process flow.

3.2 Signature Preprocessing

The signatures available after scanning are having different sizes which complicates the task for comparing them. Even feature extraction for a single signature considered with scaling will give different feature values as per its scale. For this purpose we perform pre-processing on the signature image.

The pre-processing steps carried out are as below:

1. Binary conversion and Scaling to a fixed size of 100 x 200 pixels.
2. Feature extraction with grouping based on feature groups:

- Global features
- Segmentation based Features
- Transform based features
- GLCM + Blob based features.

The Global Features supported are: Col Sum, Row Sum, Mean, Kurtosis_Min, Kurtosis_Max, Standard Deviation, Skewness_Min, Skewness_Max, Entropy, Moment_Min and Moment_Max. The global features are used as a basic set of features for all signatures. The remaining three feature sets can be selected by the user to form a configuration which is numbered from 0 to 7. The table 1 presents the features considered for various configurations.

The Segmentation based Features supported are by means of dividing the image into blocks of 50 X 50 pixels for 100 x 200 image, thus getting 2 rows and 4 columns of 50 X 50 blocks. Each of the block is used to find the following features in this group: Col Sum, Row Sum, Mean, Standard Deviation and Entropy

Table -1: Eight Different configurations Possible due to potential features

Config Number	**Groups of Features used**		
	Segmentation features	***Transf rm Features***	***GLCM+ Blob Features***
0	No	No	No
1	No	No	Yes
2	No	Yes	No
3	No	Yes	Yes
4	Yes	No	No
5	Yes	No	Yes
6	Yes	Yes	No
7	Yes	Yes	Yes

The Transform based Features supported are by means of three transforms which are applied on the image: Distance transform, Radon transform and Hough transform. The use of first M maximum values is done in this group, For the Distance transforms M=4, For Radon M=5, for Hough Transform M = 10.

The GLCM (Gray Level Co-occurrence matrix) and Blob based Features supported are: Orientation, BoundingBox, Centroid,Area, ConvexArea, Eccentricity, EquivDiameter, EulerNumber, Extent, FilledArea,, MajorAxisLength, MinorAxisLength and Solidity

For configuration 0 we use only Global features and for Configuration 7 the use of all feature groups is made to train the neural as well as the SVM model.

3.3 Training

The 8 configurations mentioned are applied to NN to get "NN Config 0" to "NN Config 7" and also for SVM to get "SVM Config 0" to "SVM Config 7" configurations. Each of these 16 configurations hold their input for training as well as the training information in a data folder. Once training is done for all the configurations the user can select the configuration with the best accuracy and save the setup.The trained model of saved configuration is used for verification process after that point in time.

3.4 Verification

The user submits a signature image for verification and the system. The Configuration selected at the end of the training process is used to verify this signature. The result of verification can be either a valid signature being found or an forged signature being found in the submitted image file. The results are informed to the user.

3.5 Signature Database

The Signature Database module is implemented in order to organize the multiple user accounts each having 15 signatures (Fig.1). The signature database is organised into multiple folders one per account. Each of the user folders hold 15 signatures out of which 10 are valid user signatures and 5 are forged ones.

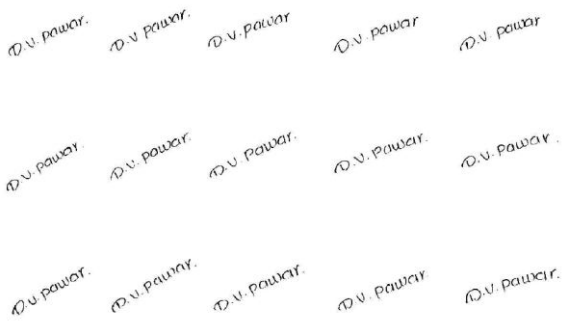

Fig-2: Typical user Signature set

With a total of 50 users are already registered in the signature verification system we have a total of 15 x 50 = 750 signatures.

3.6 Graphical User Interface (GUI)

The GUI is developed in Matlab, it has screen with a 6 button easy to use interface allowing for processing of user signatures for validation. Multiple bank accounts are supported.

The various panels available are:

- Setup Panel : allows the user to select the configuration based on feature groups (Fig.2,4)
- Database Panel : provides access to view the signature and their feature values for any signature stored in the Signature database(Fig.3,5).

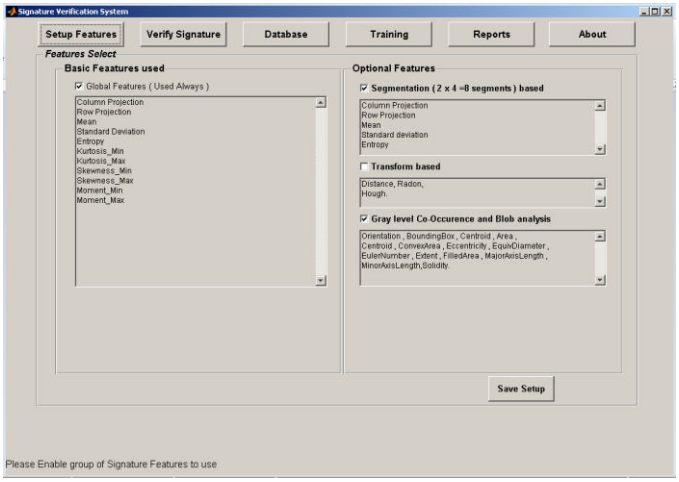

Fig-3: Setup Panel with feature selection

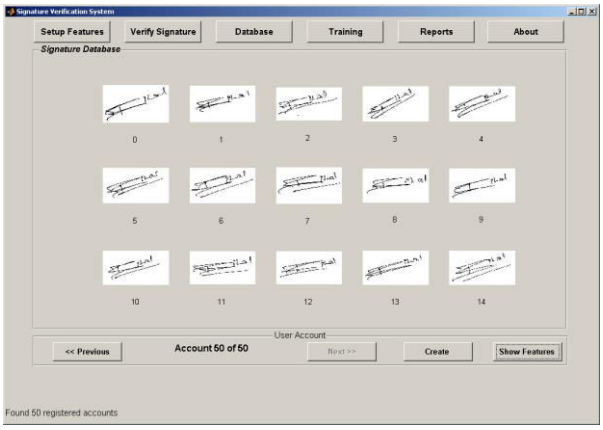

Fig-4: Database Panel with feature selection

- Report Panel : provides statistical output for the process(Fig.8,9)
- Verify Signature Dialog : allows user to submit a signature and view the result (Fig.7).

4. 4. Performance Comparision Of NN and SVM models

The total of 16 configurations of NN and SVM were explored in this work after training them for signature verification and analysed on basis of FAR, FRR and finally on the Accuracy they deliver for the task

- Training Panel : allows user to train the system either for a single configuration or for all configurations(Fig.6).

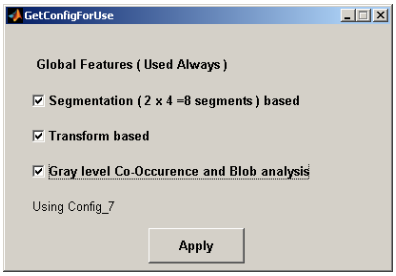

Fig-5: Configuration selection by user

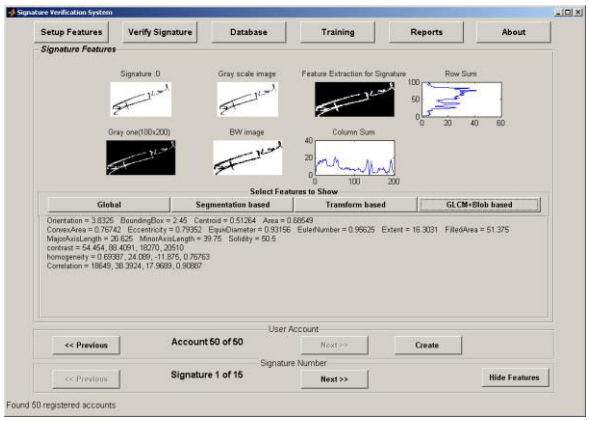

Fig-6: Database Panel with GLCM+Blob Feature displayed

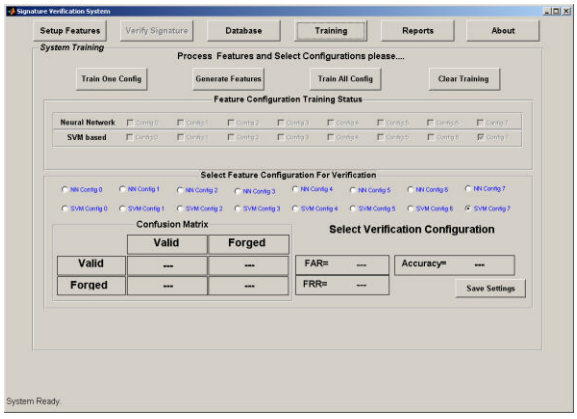

Fig-6: Training Panel

$$FAR = \frac{\text{false negatives}}{\text{true positives} + \text{false negatives}}$$

$$FRR = \frac{\text{false positives}}{\text{false positives} + \text{true negatives}}$$

$$Accuracy = \frac{\text{true positives} + \text{true negatives}}{\text{total signature count}}$$

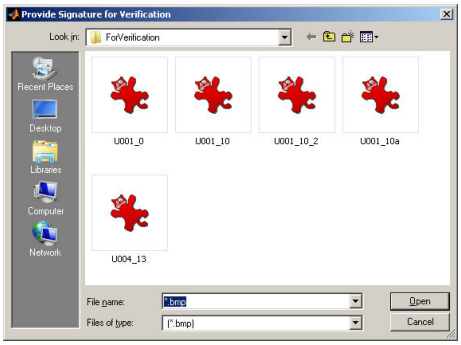

Fig-7: Signature verification dialog

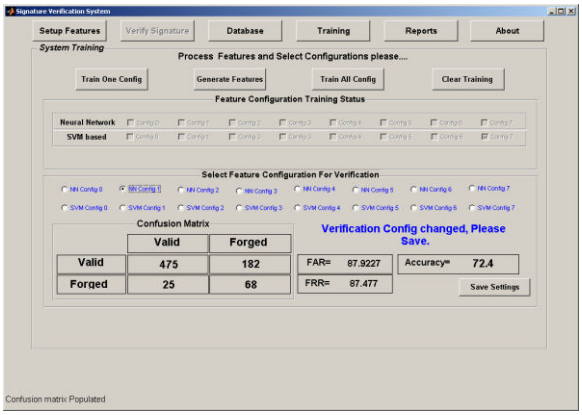

Fig-8: NN Configuration 0 Report

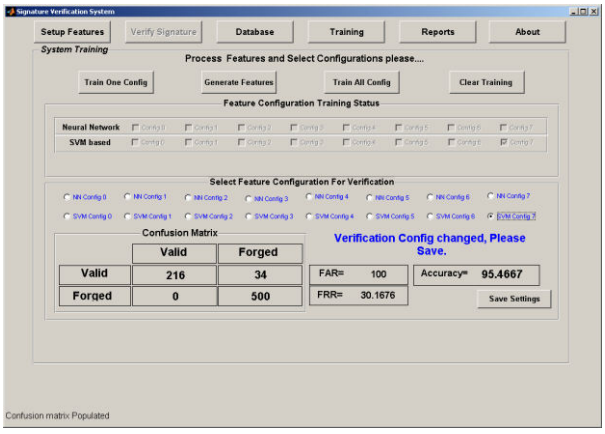

Fig-9: Configuration 7 Report

In order to evaluate the performance we check out the same for the NN and SVM models and compare them on configuration by configuration basis.

Higher accuracy with lower FAR and FRR are desired. These metrics can be interpreted in many ways, but mostly it is important to achieve low FAR scores, as a good signature verification system should not let forgeries pass through, whereas accidentally classifying a genuine signature as a forgery is less of a problem because one can simply ask the person to sign their signature again and verify.

Table -2: Performance measures Obtained for Different 16 Configurations

Configuration Number	Performance Measures		
	FRR	***FAR***	***Accuracy***
NN-0	73.305	85.0194	68.53333
NN-1	87.922	87.4769	72.40000
NN-2	86.637	90.5405	69.06666
NN-3	55.000	78.1632	65.33333
NN-4	63.855	81.8363	66.80000
NN-5	100.00	99.2063	67.20000
NN-6	98.734	96.8810	68.40000
NN-7	i.0000	99.6015	66.93333
SVM-0	94.090	8.11320	70.66666
SVM-1	88.541	25.2293	87.20000
SVM-2	94.444	26.8436	90.40000
SVM-3	96.923	27.2992	91.33333
SVM-4	100.00	30.0699	95.33333
SVM-5	100.00	29.9719	95.20000
SVM-6	100.00	29.6765	94.80000
SVM-7	100.00	30.1675	95.46666

In order to evaluate the performance for the NN and SVM models and compare them on configuration by configuration basis using the FRR Values, FRR followed by the Accuracy of the models.

Table -3: **FRR Comparison For NN and SVM**

Configuration Number	FRR	
	NN	***SVM***
0	73.30508	94.090909
1	87.92270	88.541667
2	86.63793	94.444444
3	55.00000	97.300000
4	63.85542	100.00000
5	100.0000	100.00000
6	98.73417	100.00000
7	100.0000	100.00000

The graph of fig.10 indicates that NN configuration 0, 3 and 4 show a FRR of less than 80% while for SVM model the minimum FRR obtained is around 88.5%. In the sense of the False Rejection Ration the SVM performs good. But only FRR alone cannot be used as a performance criterion.

Table -4: FAR Comparision for NN and SVM

Configuration Number	FAR	
	NN	***SVM***
0	85.0194	8.11320
1	87.4769	25.2293
2	90.5405	26.8436
3	78.1632	27.2992
4	81.8363	30.0699
5	99.2063	29.9719
6	96.8810	29.6765
7	99.6015	30.1675

Table -5: Accuracy comparision for NN and SVM Configuration

Configuration Number	Accuracy	
	NN	***SVM***
0	68.5333	70.6666
1	72.4000	87.2000
2	69.0666	90.4000
3	65.3333	91.3333
4	66.8000	95.3333
5	67.2000	95.2000
6	68.4000	94.8000
7	66.9333	95.4666

The graph of fig. 11 indicates that all NN configuration have a FAR of 80% or higher whereas the SVM configuration limit it to 30.16%, This low false acceptance ratio allows SVM to perform better than the NN configuration. Again FAR alone cannot be used as a performance criterion so now we look at the accuracy.

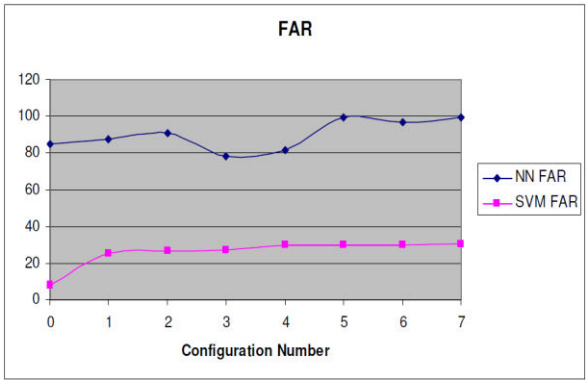

Fig.10: Performance metric FRR

The graph of fig.12 indicates that all NN configuration have an accuracy which is less than that of corresponding SVM model except for the case of configuration 0 where they are comparable. Also the margin is around 12 % or higher for all configurations except for configuration 0 where it is merely 2%.

5. Conclusion

A collection of 16 models was analysed in this work with 8 based on NN and rest on SVM. Each model made use of signature features categorized in 4 groups Global, Segmentation based, Transform based and GLCM + Blob analysis based. The configuration 0 was only using global features which was considered as basic features and rest all were treated as optional feature groups. Each of this group was used in all possible binary combinations from configuration 0 to configuration 7 for both NN as well as SVM.

It is observed that all SVM models have a minimum FRR around 88.5% which is far better than those offered by NN models. The NN models of have a FAR of 80% or higher whereas the SVM configuration limit it to 30.16%.

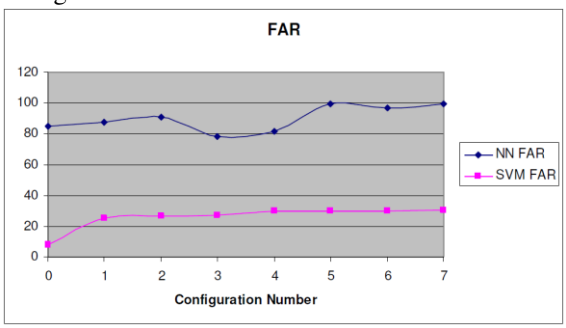

Fig.11: Performance metric FAR

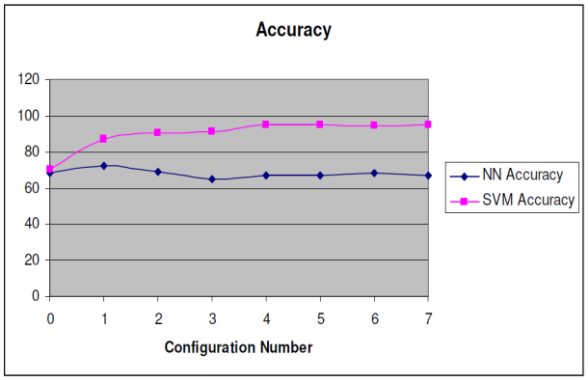

Fig.12: Performance metric Accuracy

Only for configuration 0 the accuracy of the two models is comparable as the difference is 2%.

The improvement in average accuracy for SVM models over NN models is observed to be 21.966 % and the average FAR of SVM is less by 63.91 % than that of NN models. The SVM offers a higher average FRR by 13.61521 % than the NN model.

This allows one to conclude that in an offline signature verification system:

- Feature grouping allows for performance variation, In general more features gives the better results
- SVM models outperforms the NN models in all the three performance metrics of FR, FAR and accuracy.

References

[1] A. Jain, F. Griess and S. Connell, “On-line signature Verification: Pattern Recognition”, WSEAS Transactions on Mathematics, Issue 9, Volume 8, 2010

[2] M. R. Teaque, "Image Analysis via the General Theory of Moments," Journal of the Optical Society of America, vol. 70, pp. 920-930, 1980.

[3] S. N. Srihari, A. Xu, and M. K. Kalera, "Learning Strategies and Classification Methods for Off-line Signature Verification," Proceedings of the 9th Int’l Workshop on Frontiers in Handwriting Recognition (IWFHR-9 2004), 2004.

[4] G. F. Russell and A. B. Jianying Hu, "Dynamic Signature Verification Using Discriminative Training," in Proceedings of the 2005 Eight International Conference on Document Analysis and Recognition (ICDAR’05), 2005.

[5] V.A. Baradi, H.B. Kakere, “Offline Signature Recognition System”, International Journal of Computer Applications (0975 - 8887) Vol.1, p.p. 48-56, 2010.

[6] C. Quek, R.W. Zhou. Antiforgery: a novel pseudo-outer product based fuzzy neutral network driven. Signature verification system, Pattern Recognition Lett.23(2002) 1795-1816.

[7] S. Djeziri, F. Nouboud, R. Plamondon, Extraction of signatures from check

background based on a filiformity criterion, IEEE Trans. Images Process.7(10)(1998) 1425-1438.

[8] M. Hanmandlu, K.R. Murali Mohan. Vivek Gupta, Fuzzy Logic based character recognition.Proceeding of the International Conference on Image Processing, Santa Barbara, USA, pp.714-717.

[9] Madasu Hanmandlu, Mohd. Hafizuddin, Mohd. Yusof, Vamsi Krishna Madasu, Offline signature verification and forgery detection using Fuzzy Modeling, Pattern Recognition38(2005)341-356