International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 1232– 1237

A Fuzzy Logic Based Novel Signature Verification System on Bank Cheque with Fractal Dimensions and Connected Components

Ashok Kumar. D[1] and Dhandapani.S[2*]
Department of Computer Science and Applications
Government Arts College,
Tiruchirapalli - 620 022, TamilNadu, INDIA.
drashoktrichy22@gmail.com[1] sdpudt@rediffmail.com[2*]

***Abstract*—** Signature plays its authorization role in almost every document. Proper care should be taken for the verification of the genuineness of the signature in legal documents. Signature verification scheme can be online or offline based on the acquisition type. A novel method for offline signature verification in bank cheques is proposed. It is found out that using fractal dimensions for verification purpose improves the accuracy rate. Also the fundamentals of offline signature verification process are discussed. The proposed system uses connected Components Labeling, Fractal Dimensions and Fuzzy Logic for signature verification. The signature is scanned and preprocessed. Using connected components labeling, the signature is split into regions and each region is labeled uniquely. Feature values for each labeled regions are extracted and normalised. Fractal dimensions of signature images are calculated. Extracted feature values and fractal dimensions are compared with the feature values of the sample signatures for its genuineness. Fuzzy classifies the genuine and forged signatures correctly to its fullest extent. Some signatures may have more noise or it may be complex for the system to identify or classify. Those signatures may need some manual intervention. The proposed verification system shows very good results with good sensitivity and specificity. It has an accuracy of maximum 50%.

Keywords- *Signature verification; connected components; Fractal Dimension; Fuzzy Logic.*

*****

I. INTRODUCTION

Signature is one of the oldest and also the cheapest method of authorization. One may forget his password or he may have missed his smart card used for the verification purposes. Signature takes the advantage of them all [13]. It is also widely accepted by people for many legal transactions. Signature verification has gained momentum [10] and it is considered with renewed awareness in the recent years due to the bank cheque fraud case reports [18]. The signature verification can be broadly classified into online or offline on the basis of image acquisition type. Online signing requires special electronic equipments like the stylus and the tablet. The signer has to be present at the place where the gadgets are installed [14]. Offline signatures requires only a pen. The signer can sign from anywhere and the verification is done at offices, in our case, the bank. Signature verification is easy in case of online signatures. All the necessary signature features like the signing speed, number of lifts of the electronic pen, pressure applied at various positions and also the angle of inclination can be extracted. But in offline signature verification, the researcher will have only the scanned digital copy of the signature and not the behavioural information like pressure, velocity and sequence of the strokes [22]. One has to preprocess the available signature for higher verification accuracy.

Man is the most powerful machine. They get trained and their neuron's learning process is a continuous one. One can identify a signature and in a fraction of a second, can judge its genuineness. The problem is that he may get fatigue after long time of verification process. The verification may get sluggish in the evening hours. Even professional forensic department document examiners do a correct classification rate of only about 70% [2]. A genuine signature may be questioned and a forged signature may be accepted due to human error. Either of the case, it may irritate bank's valuable customers. To assist him in the classification, this new system is proposed. As a result of verification, signature is categorized into genuine, forged or complex. Complex signature is the one which the verification system finds that human intervention is also needed. This may be due to noise created due to cheque mutilation or signature not legible. No one can put his signature so exactly the very next time. Since signature is a behavioural biometric [9], so intra-class variations are higher. The signature depends on the psychophysical state of the user. This makes the system complex by carefully managing intra-class differences and also identifying the inter-class variations. As age increases, the style of the signature gets changed but the length remains the same. Figure 1 shows a sample cheque.

Figure 1. A Sample Cheque

simple and random forgeries. Skilled forgery is one the forger keeps a copy of the genuine signature handy and after a couple of practices, he quickly puts the signature on the required document. In simple forgery the forger remembers the signature from any other document and tries to imitate the same from his memory. Random forgery is the one where the forger signs knowing only the name of the signer. Since the proposed model deals with bank cheque signature verification, only skilled forgery is focused.

The number of individual regions may be different for different signatures due to noises. An isolated individual pixel may also be recognized as a separate region and the number of

regions may vary due to the presence of noise. So preprocessing along with normalization is done and the signature is cleaned. Number of regions may vary in random and simple forgeries. But in skilled forgery, we assume that the number of regions may be equal to the genuine signature.

II. LITERATURE REVIEW AND PROPOSED SYSTEM

Any Signature verification system developed should be accepted universally and it should help the administrative and financial offices. The system developed should be of low cost, high speed and with maximum accuracy. Handwritten Signature verification is a technique which is reliable, economical and unintrusive to the signer [8]. The proposed signature verification system uses CEDAR signature dataset. The system uses connected components labeling concept. Connected component labeling is a fundamental step in automatic image analysis. Different labels are assigned to various disjoint connected components of the image. Properties like shape, area and boundary of the labeled regions can be calculated easily. Values of these properties form the feature set. Signatures can be seen as an image and recognized using image processing. In [16], authors used structural parameters and local variations to train artificial neural network for signature verification and used angle features in fuzzy logic based system for forgery detection. Connected components labeling was used in [4] and the similarity between the features was calculated by the Manhattan distance method.

It has been analyzed in [21] that the handwriting of male writers is more consistent than that of female writers. Shekar and Bharathi [20] uses eigen signature construction to extract features from the signature shape and compares it with the texture based feature extraction. Authors in [16] use the preprocessed signature to extract features and detect forged signatures using artificial neural network. In [11], the authors proposed a method to extract signatures from a complex background by capturing the structural saliency.

A. Image Acquisition

The process of digitizing the image is done in image acquisition phase. To extract handwritten information, authors in [6] used a topological criterion called filiformity. The signature can be photographed using a camera or scanned using the scanner. Since scanner gives high resolution in DPI format, signature is scanned from the bank cheque using a scanner of high resolution. Cheque may contain logo and designs with different background colour. Separating the signature, from the background and design of a cheque, is a tedious process[19]. Since the signature is scanned using a scanner, sampling and quantization noise may creep in [18]. Also fixing the rubber stamp on the cheque of the signer over the signature or part of it, may need some preprocessing to extract the signature.

B. Image Preprocessing

Preprocessing is done to reduce the noise in the scanned signatures. In connected components labeling, the regions are identified using the pixel connectivity. If a noise appears in the scanned image it has to be cleaned. The individual pixel or noise which is not a part of the signature may also be considered as a region. If the irrelevant pixels are labeled and used for training they may lead to error. Preparing the signature image for verification process should not consume more time. Cheque transaction time in banks is limited nowadays to offer a quick service to the account holder.

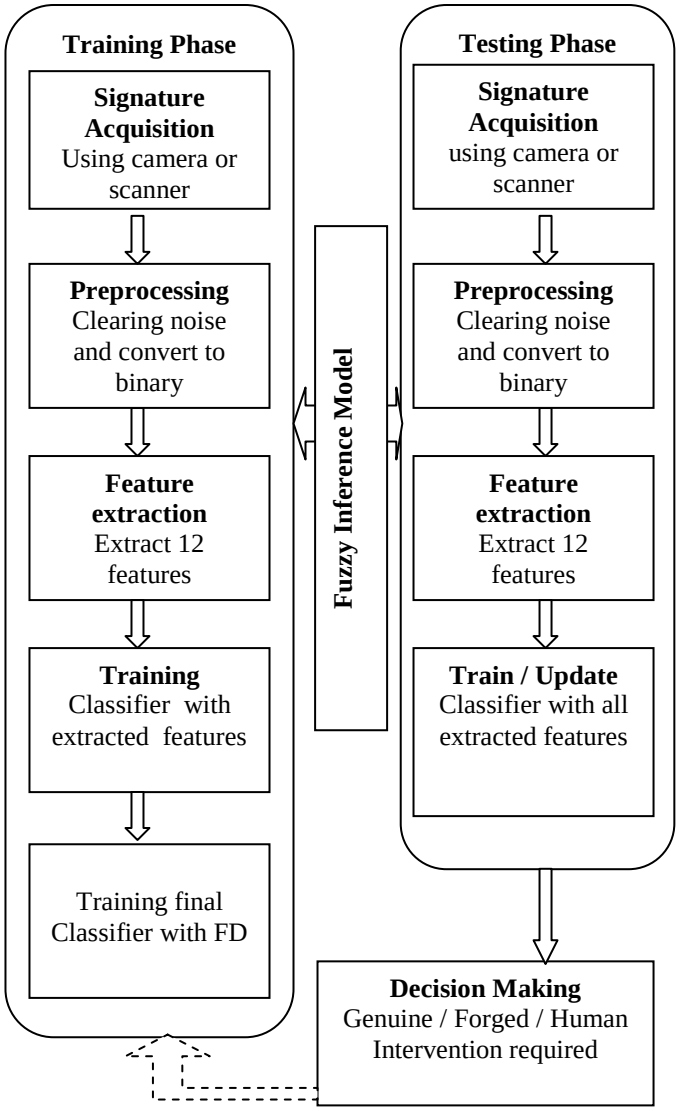

Figure 2. Signature Verification Model

C. Feature Extraction

Feature extraction is the most important task in a signature verification system. The goal of feature extraction is to improve the efficiency and effectiveness of classification [7]. The effectiveness can be increased by minimizing the number of features and maximizing pattern discrimination. Since signature is a behavioural biometric system, the feature plays the major role in recognition and identification.

Any feature set for a signature verification system should provide lesser intra-class variation and large inter-class variation [5]. Also more features does not necessarily improve performance [8]. To extract the features, the signature image is scanned pixel by pixel. The pixels are scanned and labeled from left to right and then downwards. Labeling is needed to recognize connected components in a binary image [5]. If a pixel to be scanned is four connected to previously labeled pixel, it is given the same label. Some pixel will be connected to two different label names. Such equivalent pairs are found

and relabeled. Now all the individual components are labeled uniquely in groups or regions. The features of the entire individual labeled regions are extracted. Proper care and security measures should be taken to the sample signatures and features stored in the bank.

Table I shows the sample list of features extracted from each region. The possibilities are by its shape, intensity, area and boundary. Any of the features can be taken into account. The process is repeated for sample and testing signature images.

Area calculates the actual number of pixels in the region. MajorAxisLength and MinorAxis Length are the length of the major axis and minor axis of the ellipse that has the same normalized second central moments as the region. The eccentricity is the ratio of the distance between the foci of the ellipse and its major axis length. The value will be between 0 and 1.

Orientation is the angle between the x-axis and the major axis of the ellipse that has the same second-moments as the region. ConvexArea specifies the number of pixels in ConvexImage. FilledArea specifies the number of on pixels in FilledImage. EulerNumber specifies the number of objects in the region minus the number of holes in those objects. EquivDiameter specifies the diameter of a circle with the same area as the region. It is calculated using the formula sqrt(4*Area/pi). Solidity specifies the proportion of the pixels in the convex hull that are also in the region. Extent specifies the proportion of the pixels in the bounding box that are also in the region. It is computed by dividing the Area by the area of the bounding box. Perimeter is the p-element vector containing the distance around the boundary of each contiguous region in the image, where p is the number of regions. Regionprops computes the perimeter by calculating the distance between each adjoining pair of pixels around the border of the region.

A fractal is a geometrical figure or a curve. Each part of a fractal will have the same statistical character as the whole. They are useful in modeling structures in which similar patterns recur at progressively smaller scales. Fractals are most complex in their geometry. Any fractal object will have three properties. They are self-similarity, iterative formation and fractal dimension. Wavelets and fractals are texture feature types. In this paper we take fractal dimension into account and show how textural information can be utilized for classification of signature images. Signature is verified online or offline depending upon the application it is used. Transforming the fractals, Kai Huang and Hong Yan [12], has proposed a work for online signature verification. They have worked for random forgery by comparing the fractal codes and the varying distances. They have attempted to explore the self similarity information. A fractal dimension is a ratio providing a statistical index of complexity comparing how detail in a pattern changes with the scale at which it is measured. It has also been characterized as a measure of the space-filling capacity of a pattern that tells how a fractal scales differently from the space it is embedded in. A fractal dimension of an irregular set does not have to be an integer. Fractal dimension can be calculated by many methods like radial mass method, correlation method, Box counting method and Hausdorff's dimension. In this paper we used Hausdorff's dimension to calculate the fractal dimension of the signature by the algorithm I proposed by [1].

ALGORITHM I: FRACTIONAL DIMENSION CALCULATING ALGORITHM

Step 1: Pad the image for a dimension of 2
Step 2: Adjust the box size so that atleast a single pixel of the signature is inside the box.
Step 3: Compute the points with log(N(e)) x log(1/e)
Step 4: Draw line by the last square method using the points.
Step 4: The slope of the line is the dimension of the signature

Using the above algorithm we can find the dimension of irregular shapes like signatures. They do not have uniform characteristics sizes. A conventional cheque contains at least eleven special marks of identification but the vital mark of identification is the authorized person's signature. Forgers forge the signature carefully in terms of size and shape. They may even trace the signature or draw with the genuine signature nearby. When a signature is forged to the extent that, it is hectic to identify, the time taken is more so the signature will be wrinklier. A skilled forgery takes more time. [5]

TABLE I. SAMPLE FEATURE VALUES OF THE REGIONAL PROPERTIES OF THE SIGNATURE

Feature	Region1	Region2	Region3
Area	2435	151	63
MajorAxisLength	217.3152	33.58855	15.47299
MinorAxisLength	100.2363	11.9054	6.22238
Eccentricity	0.88727	0.935076	0.902862
Orientation	10.91051	12.34612	-32.6674
ConvexArea	17962	290	76
FilledArea	3404	154	63
EulerNumber	-9	-1	1
EquivDiameter	55.68068	13.86576	8.956232
Solidity	0.135564	0.52069	0.828947
Extent	0.086357	0.347926	0.484615
Perimeter	1193.183	90.76955	37.79899

Fuzzy Logic is used to classify the signatures into genuine and forged with the target values 1 and 0. Genuine signatures will have a value close to 1 and forged signature to 0. Using a threshold value, we can classify the signature to genuine or forged one. In Table II, we have presented some of the output values from the classifier and the genuine signatures result will be close to 1 and forged signatures results will be close to 0. Value in the 8^{th} row, 0.6547, is a false prediction and also value in the 9^{th} row, which is, 0.4515 is a false prediction. They are complex type and needs human intervention.

TABLE II. SAMPLE CLASSIFIER OUTPUT VALUES AND SAMPLE FRACTAL DIMENSIONAL VALUES

S.NO	GENUINE	FORGED	FRACTAL DIMENSION
1	0.8723	0.2103	1.335
2	0.8610	0.21031	1.339
3	0.8229	0.0167	1.338
4	1.0271	0.24905	1.337
5	0.6258	0.1972	1.342
6	0.9418	0.1841	1.344
7	0.6670	0.2412	1.333
8	1.1157	0.6547	1.331
9	0.4515	0.0254	1.305
10	0.6317	0.4417	1.336

Signature of a person changes over time. After certain years, the false positive values may shoot up due to the changes in the signature of the signer. It may be of his age, inconvenience in signing the existing signature, unable to remember his signature, personal preference and change of one's name. The system should be able to update the samples as the signature gets changed with proper approval.

ALGORITHM II: REGION LABELING ALGORITHM

Step 1: Scan the binary signature from left to right and downwards and initialize label (li) to 0.
Step 2: if (top & left pixel) = 0, assign label li +1
Step 3: if (top or left pixel) = 1, label = label (top or left pixel)
Step 4: if(top and left pixel) =1, label = label(top or left pixel) note that top and left are equivalence classes
Step 5: repeat till the last pixel.
Step 6: equivalent classes are analyzed and labeled commonly.

III. TRAINING AND SIGNATURE VERIFICATION

Signature verification is a binary type of classification since it predicts whether the signature is genuine or forged. The sample signatures are collected for training. The feature values are computed using the connected components labeling and regionprops. The input to the classifier is the preprocessed and normalized feature values.

Fuzzy Logic is used as a classifier. The modelled system shows a good performance and the results are better than the network designed using the GLCM features [3]. In [3], gray level co-occurrence matrix was used along with feed forward back propagation neural network. The accuracy claimed was 92.08%. The result of the classifier with regional features along with the fractal dimension of the signature is fed to another neural network of same design and the results are more convincing than without the fractal dimension.

IV. PERFORMANCE AND QUALITY MEASURES

The quality of a signature verification system is usually measured by terms like FAR, FRR, TP, TN, FP, FN. FAR is the false acceptance ratio and FRR the false rejection ratio. TP is the number of correct positives, TN is the number of correct negatives, FP is the number of incorrect positives, FN is the number of incorrect negatives. False Rejection is also called Type I errors and False Acceptance is also called Type 2 errors. Also statistical measures like sensitivity, which measures the proportion of actual positives and specificity, which measures the proportion of actual negatives are measured. In signatures there are inter-class and intra-class variations. Inter-class variations are variations that arise in signatures by the same person the very next time [17]. No one can put the exact signature next time and so exact pixel matching for verification is not feasible. Table III shows the measures.

TABLE III. PERFORMANCE MEASURES

FAR	**FN / (TN + FN)**
FRR	**FP / (TP + FP)**
Sensitivity	**TP / (TP + FN)**
Specificity	**TN / (TN + FP)**
Accuracy	**(TP + TN) / (TP +TN + FP +FN)**

Figure 3 shows the fuzzy logic controller. The input is a crisp set and it is fuzzified. The fuzzy inference engine uses the fuzzy rules to map the input to the output and finally defuzzification takes place and the out is in the crisp form.

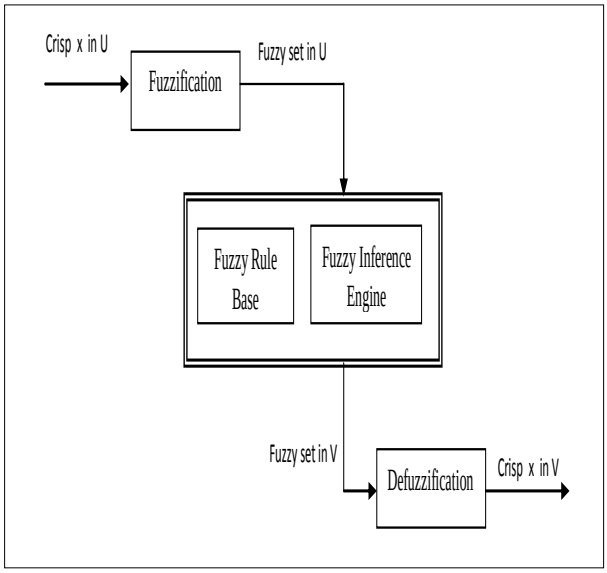

Figure 3. Fuzzy Logic Controller

Intra-class is the variations found in forged signatures. Pixel to pixel matching is not always possible. So an amount of

threshold is used for verification. The value of threshold depends on the application the system is used. If we lower the FAR too much then FRR will increase [15]. We are concerned about bank cheque signatures and the threshold will be minimum.

TABLE IV. EXPERIMENT AND RESULT ANALYSIS OF THE PROPOSED SYSTEM WITHOUT FRACTAL DIMENSION - 1

	TP	TN	FP	FN	FAR	FRR
Sign-1	5	5	7	7	0.58	0.58
Sign-2	1	5	11	7	0.58	0.92
Sign-3	7	4	5	8	0.67	0.42
Sign-4	5	4	7	8	0.67	0.58
Sign-5	5	2	7	10	0.83	0.58

TABLE V. EXPERIMENT AND RESULT ANALYSIS OF THE PROPOSED SYSTEM WITHOUT FRACTAL DIMENSION - 2

Run	Sensitivity	Specificity	Accuracy
Sign-1	0.42	0.42	42
Sign-2	0.13	0.31	25
Sign-3	0.47	0.44	46
Sign-4	0.38	0.36	38
Sign-5	0.33	0.22	29
Average	**0.35**	**0.35**	**36**

Table V and VI show the experimental results of the system using the regional properties of the signature alone. The result lies in proper execution of the entire process like scanning, preprocessing and training the classifier. Any signature system should have some facility to update the specimen signature. As the years pass on, the signer may change his sign due to many reasons.

TABLE VI. EXPERIMENT AND RESULT ANALYSIS OF THE PROPOSED SYSTEM WITH FRACTAL DIMENSION – 3

	TP	TN	FP	FN	FAR	FRR
Sign-1	4	5	8	7	0.58	0.67
Sign-2	1	5	11	7	0.58	0.92
Sign-3	8	4	4	8	0.67	0.33
Sign-4	5	4	7	8	0.67	0.58
Sign-5	5	3	7	9	0.75	0.58

TABLE VII. EXPERIMENT AND RESULT ANALYSIS OF THE PROPOSED SYSTEM WITH FRACTAL DIMENSION – 4

Run	Sensitivity	Specificity	Accuracy
Sign-1	0.36	0.38	38
Sign-2	0.13	0.31	25
Sign-3	0.50	0.50	50
Sign-4	0.38	0.36	38
Sign-5	0.36	0.30	33
Average	**0.35**	**0.37**	**37**

Table VII and VIII shows the result analysis when the fractional dimension of the signature image is included to the neural network. We can clearly see that the accuracy of the system increases by 1% when the fractal dimensional feature is included. Performance of proposed signature verification model is found to be encouraging.

Figure 4 shows the chart analysis of the classifier with connected components features. It shows sensitivity and specificity measures. Figure 5 shows the chart analysis of the proposed system, with fractal dimension included for the classification. It shows that the results have improved when the fractal dimension of the signature image is included as a feature for classification. The signature is a complex structure

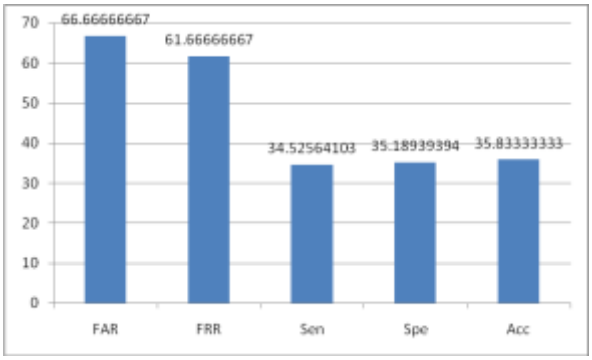

Figure 4 .Experimental Analysis of the system without Fractal Dimension

and it inherits some property of the fractals and so the fractal dimension can be used as the feature for signature verification.

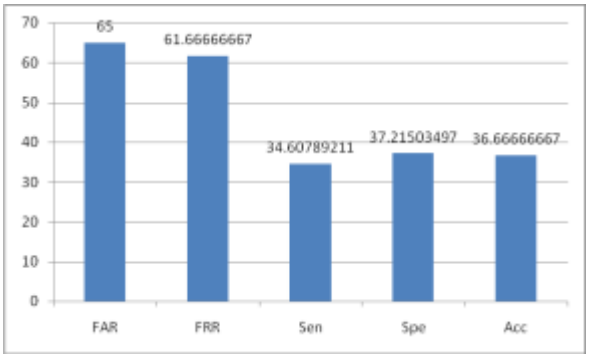

Figure 5 .Experimental Analysis chart of the system with Fractal Dimension

V. CONCLUSION AND FUTURE WORK

In this research, the authors have modeled a signature verification system for verifying signatures on bank cheques. The modeled system uses Connected Components Labeling, Fractal Dimensions and Fuzzy Logic for verification. Signature is scanned and divided into components based on pixel connectivity. The features of individual components of the sample signatures are extracted and used to train fuzzy classifier. The system modeled works very fine with signatures tested from CEDAR database. The system shows results with the accuracy of 37%. When the fractal dimension of the signature is added for classification with the neural network, the accuracy increases by 1 %.

ACKNOWLEDGEMENT

The authors are very thankful to the researchers who have given their valuable inputs to bring out this model. The authors thank everyone who has extended their help and support.

REFERENCES

[1] Alceu Ferraz Costa, Joe Tekli, Agma Juci Machado Traina, "Fast fractal stack: fractal analysis of computed tomography scans of the lung". International ACM Workshop on Medical Multimedia Analysis and Retrieval (MMAR), pages 13-18, 2011

[2] Alonso-Fernandez, M.C. Fairhurst, J. Fierrez and J. Ortega-Garcia, "Impact of Signature Legibility and Signature Type in Off-Line Signature Verification", Biometrics Symposium, pages .1,6, 11-13 Sept. 2007.

[3] Ashok Kumar. D and Dhandapani. S, "A Bank Cheque Signature Verification System using FFBP Neural Network Architecture and Feature Extraction based on GLCM", IJETTCS, Volume 3, Issue 3, May – June 2015.

[4] Chalechale, A, Naghdy, G, Pramaratne, P & Mertins, "Document image analysis and verification using cursive signature", IEEE International Conference on Multimedia and Expo(ICME '04), 27-30 June 2004.

[5] Dinesh Kumar and Premith Unikrishnan, "Class Specific Feature Selection for Identity Validation using Dynamic Signatures", Journal of Biometrics and Biostatistics, 2013.

[6] Djeziri, S., Nouboud, F., Plamondon, R., "Extraction of signatures from check background based on a filiformity criterion", IEEE Transactions on Image Processing, doi: 10.1109/83.718483vol.7, no.10, pp.1525, 1538, Oct 1998.

[7] Donato Impedovo and Giuseppe Pirlo, "Automatic Signature Verification:The State of the Art", IEEE transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 38, no. 5, September 2008.

[8] Dullink. H, Van Daalen.B, Nijhuis.J, Spaanenburg.L, Zuidhof.H, "Implementing a DSP Kernel for Online Dynamic Handwritten Signature Verification Using the TMS320 DSP Family", EFRIE, France, December 1995.

[9] Fairhurst M.C, "Signature verification revisited: promoting practical exploitation of biometric technology", Electronics & Communication Engineering Journal, December 1997.

[10] George Nagy, "Twenty Years of Document Image Analysis", IEEE Transactions on Pattern Recognition and Machine Intelligence, Vol 22, No. 1., Jan. 2000.

[11] Guangyu Zhu, Yefeng Zheng, David Doermann, and Stefan Jaeger, "Multi-scale Structural Saliency for Signature Detection", 1-4244-1180-7/07/2007.

[12] Kai Huang; Hong Yan, "Signature verification using fractal transformation," Pattern Recognition, 2000. Proceedings. 15th International Conference on , vol.2, no., pp.851,854 vol.2, 2000.

[13] Meenu Bhatia, "Off-Line Hand Written Signature Verification using Neural Network", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 5, May 2013.

[14] Mohamad Hoseyn Sigari, Mohamad Reza Pourshahabi, Hamid Reza Pourreza, "Offline Handwritten Signature Identification using Grid Gabor Features and Support Vector Machine", ICEE, pages: 281-286. 2008.

[15] Mukta Rao, Nipur, Vijaypal Singh Dhaka, "Enhancing the Authentication of Bank Cheque Signatures by Implementing Automated System Using Recurrent Neural Network", Journal Of Advanced Networking and Applications, Vol. 01 No. 01 pages: 15 -24, 2009.
Gautham S Prakash and Shanu Sharma, Computer Vision and Fuzzy Logic Based Offline Signature Verification and Forgery Detection, IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-6, Dec, 2014.

[16] Perez-Hernandez, A. Sanchez and J.F. Velez, "Simplified Stroke-based Approach for Off-line Signature Recognition", Second COST 275 Workshop, 2004.

[17] Pushpalatha K.N, Aravind Kumar Gautham, D. R.Shashikumar, K. B. ShivaKumar and Rupam Das, "Offline Signature Verification with Random and Skilled Forgery Detection Using Polar Domain Features and Multi Stage Classification-Regression Model", International Journal of Advanced Science and Technology, Vol.59, pages 27-40, 2013.

[18] Ranju Mandal, Partha Pratim Roy, Umapada Pal, "Signature Segmentation from Machine Printed Documents using Conditional Random Field", ICDAR, 2011.

[19] Shekar, B. H.; Bharathi, R. K., "Eigen-signature: A robust and an efficient offline signature verification algorithm", Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, vol., no., pp.134,138, 3-5 June 2011.

[20] Swati Srivastava, "Analysis of Male and Female Handwriting", International Journal of Computer and Communication System Engineering (IJCCSE), ISSN: 2312-7694, Vol. 1 No.02 August 2015.

[21] Vu Nguyen, Michael Blumenstein, Graham Leedham, "Global Features for the Off-Line Signature Verification Problem", 10th International Conference on Document Analysis and Recognition, 2009.