www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 9 September 2017, Page No. 22442-22449
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i9.09

Offline Signature Verification System for Bank Cheques Using Zernike Moments, Circularity Property and Fuzzy Logic

Ashok Kumar. D[1] and Dhandapani. S[2] *

Department of Computer Science and Applications
Government Arts College,
Tiruchirapalli - 620 022, TamilNadu, INDIA.

Abstract

Handwritten signature plays its authorization role in most legal and financial documents. It is the most accepted and economical means of personnel authentication. It can be verified using online or offline verification schemes. This paper proposes a model to verify signatures by combining features like Zernike moments, circularity and aspect ratio. Unlike characters, signatures vary each time because of its behavioural biometric property. Signatures can be identified based on their shape. Moments are the good translational and scale invariant shape descriptors. The amplitude and phase of Zernike moments, circularity property and aspect ratio of the signature are the features that are extracted and fed to fuzzy classifier. Fuzzy logic classifies the signature into genuine or forged. Experimental results reveal that this methodology of combining zernike moments along with the two mentioned geometrical properties give higher accuracy and the accuracy rate increases with the increase in number of samples given to the fuzzy classifier.

Keywords: Offline Signature Verification, Zernike Moments, Fuzzy Logic.

1. Introduction

Signature is the widely used and accepted form of authentication and it is used even before the usage of computers [1]. It is easier because it does not require any physical hardware to capture as that of fingerprints and iris scanner. Signature takes the advantage of traditional biometric methods like passwords, PIN and ID cards which can be stolen, lost or one may forget. Handwritten signatures are used in almost all documents where authentication is required. It has a low conflict percentage. There is huge number of modern techniques followed by the fraudulent to counterfeit the signature. As a result, the numbers of bank cheque fraud cases are rising. The cheque is washed with special fluid to erase the amount figures and writing a huge amount, changing the name of the bearer, removing the signature and placing duplicated signatures are the different ways cheque fraud is reported. To avoid such offense activities, a model to verify signature is badly needed. Reserve Bank of India introduced cheque truncation system which will minimize the above problems [2]. Signatures are not easy to verify like that of characters. Verifying signatures in bank cheques is a challenging opportunity in image processing. Characters have definite shape and can easily be identified. Since signature is a behavioral biometric, it varies according to the mood, environmental condition and presence of mind of the signer. No one can put the signature alike all the times. There may be small variations which are called intra-class variations. These variations are to be neglected during the verification process. Only inter-class variations verify and classify the signatures into genuine or forged. Handwritten signatures can be verified using online or offline schemes. Online signature can be captured using electronic devices like writing pad or stylus attached to a computer. It can capture dynamic features, like writing speed, angle, number of pen ups and time taken to put the signature, which will make the verification process easier and more accurate. Offline signature will have only the digitised signature from which required features can be extracted. Since this paper deals with signatures on bank cheques, offline signature verification scheme is chosen. A signature which is suspicious is called a forged signature. Forgery can be of four types. Simple forgery is the forger writing the name of the signer casually. Random forgery is the forger trying to imitate the genuine signature. Skilled forgery is the forger trying to put the near exact signature by many practices. Disguised forgery is the forgery that the genuine user himself puts his signature incorrectly to later deny that he has not signed. The proposed model uses CEDAR (Center of Excellence of Document Analysis and Recognition) database which is publicly available. Fuzzy logic is used for the classification purpose as neural network has some limitations [3]. Signature verification is a two-class pattern recognition problem. The output of the classifier may be '0' or '1' representing forged and genuine signatures respectively.

The breakdown of this paper is as follows. Section 2 discusses the Literature Review. Section 3 discusses image acquisition and preprocessing works done for the signature. Section 4 discusses the feature extraction process. Section 5 discusses about Fuzzy Logic and Classification. Section 6 discusses the experimental results and Section 7 finally concludes the research paper.

2. Literature Review

In [4], Rajesh kumar etal proposed a signature verification system using the surroundedness feature and thay have used CEDAR database. Hai-Lin and Hai-zhou [5] proposed a verification method using Zernike moments since it is rotation and scale invariant. Pushpalatha etal [6] proposed a verification method with polar feature descriptor for signature that contains radon transformation and zernike moments. The system detects skilled forgery. Khotanzad and Hong [7] studied the superiority of Zernike moment feature over regular moments and moments invariants. Sohail and Rashid [8] combined circularity with other structural features and have gained good results. Jovisa [9], defined the circularity measure which is robust to noise and it is invariant to translation, rotation and scaling. Huazhong etal [10] presented a brief description of types of moments and reveal that Zernike moments are invariant to rotational transformation. Divjyot and Dutta [11] used Zernike moments and minutae features for signature verification. Neo Han etal [12] combined a new feature set using Zernike moments and wavelet transforms for face recognition. Pham etal [13] extracted features using an adaptation of the shape context descriptor which were robust to noise, rotation and scaling. This lead them not to depend upon the preprocessing activities. Cemil Oz [14] proposed a signature verification method with two separate sequential neural networks, one for recognition and other for verification. He used moment invariant methods for feature extraction and found that the performance was good enough to verify the signature. Pradeep and etal [15] proposed a signature verification system using the shape descriptor and Euclidian distance. They used correspondences between signatures, aligned transforms and got encouraging results.

3. Image Acquisition and Preprocessing

The process of converting the hardcopy of the bank cheque into soft copy for further processing of the image is called image acquisition. It can be done in two ways. The signature can photographed or scanned using a high resolution scanner. Signature verification systems normally face the problem of number of signature samples available for training the classifier. In reality, banks mostly get three specimen signature samples. Those samples are taken immediately and so the customer signs casually one after another three times. Intra personnel variations can be recorded if the signature samples are collected at different times. Any classifier requires its adequate amount of samples for training which will not be practically possible. But Fuzzy Logic requires less samples when compared to Neural networks. Diaz and etal [16] have proposed an idea to create duplicate signatures using a cognitive inspired algorithm. It is based on transformations which simulate the human spatial cognitive map and motor system intra-personal variability during the signing process.

Preprocessing is done to remove the noise from the image. The noise may have crept during scanning or folding of cheque leaves. Bank cheque usually contains logo and some background images or patterns. The signature may be on the background part and that has to be removed. Only the signature part alone is to be isolated. A threshold is used to make other pixels white and the signature pixels black. Preprocessing improves accuracy and classification rate. The normal steps in preprocessing are converting to grayscale, binarisation, segmentation. Median filters can be used to remove external noise [17]. Processing images in gray scale is easier than RGB. Binarisation will have only 0 or 1 pixels instead of 256 gray levels which may make the task little complex. Area of interest, signature portion, is located by segmentation process. Normalization is done for making the verification process easy and to extract feature values accurately [17].

4. Feature Extraction

Feature extraction is the vital portion of a signature verification process. It is the process of defining image characteristics to represent the image information more meaningfully and efficiently. The effectiveness of feature extraction can be increased by reducing number of features used and maximizing pattern discrimination [18]. It is used for further analysis and classification purposes. Aspect Ratio is the ratio of the number of columns to the number of rows [24]. The circularity of the signature is calculated with its Perimeter (p) and Area (Ar) by

$$\text{Circularity} = \frac{4\pi Ar}{P^2} \qquad - \quad (1)$$

Moments are the count of number of objects at a distance from a point. They are simple. Translational and scale invariant shape descriptors [19]. Moment descriptors has the high quality in representing shapes [20]. Zernike moments are chosen because of its robustness towards image noise, geometrical invariance property and orthogonal property. Using Zernike moments reduces the false negative rate [21]. Algorithm I is used to extract the moment features.

Zernike Polynomials are an orthogonal set of complex-valued polynomials represented as

$$Vnm(x,y) = R_{nm}\ (x,y).exp\left(\left(jm.\tan^{-1}\frac{y}{x}\right)\right) \qquad - \quad (2)$$

where,

$$x^2 + y^2 \leq 1, j = \sqrt{-1}, n \geq 0, |m| \leq n$$

and $n - |m|$ is even and Radial polynomials $\{R_{nm}\}$ are defined as

$$R_{n,m}(x,y) = \sum_{s=0}^{\frac{n-|m|}{2}} b_{n|m|s}(x^2 + y^2)^{\frac{n}{2}-s} \qquad - \ (3)$$

where,

$$B_n|m|s = \frac{(-1)^s(s-1)!}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n+|m|}{2}-s\right)!}$$

The complex Zernike moments of order n and repetition m are given by

$$A_{nm} = \frac{n+1}{\pi}\sum_k \sum_y f(x,y)V_{nm}^*(x,y) \qquad - \qquad (4)$$

where,

$x^2 + y^2 \leq 1$ and symbol * denotes the complex conjugate operator.

The Zernike moments can be computed using the scale invariant central moments by

$$\frac{n+1}{n}\sum^{n}_{\underline{\;k-|m|\;}\atop n-k=even} \sum_{a=0}^{b} \sum_{d=0}^{|m|}(-j^d).\left(\left|\frac{m}{d}\right|\right)\left(\frac{b}{a}\right) B_{n|m|s}G_{k-2a-d,2a+d} \qquad - \quad (5)$$

where $\qquad b = \frac{n-|m|}{2} - S \quad and\; j = \sqrt{-1}$

The meshgrid function in Algorithm I replicates the grid vectors x and y to produce full grid by X and Y. The signature's orientation angle can be found using the phase angle of the Zernike moments. The order of the Zernike moments is set to 4 and the repetition number of the Zernike moments is set to 2.

Algorithm I: Extraction of Amplitude and Phase Angle from Moments

Input :
P, input image matrix, n, order of the Zernike moments, m,
repetition number of Zernike moments.

Output :
A, Amplitutde of the moment and Phi, the phase (angle) of the moment.

Method:

```
Procedure  calculatezm ( p,n,m)
begin
        N ← size(p);
        begin x  ← 1 to N, y ← x;
                X,Y ← meshgrid(x,y)
        end
                calculate the radial polynomial using the equation (3)
                calculate moments by using the equation (4)
                calculate amplitude(A) and phase angle(Phi) from the  moments.
end
```

The radial polynomial is first obtained using equation (3) and the moments are calculated using equation (5). Equation (2) gives the zernike polynomials from which amplitude and phase angle are calculated.

5. Classification with Fuzzy Logic

Fuzzy logic allows problem to be described in a natural linguistic way instead of mathematical derivations [22]. Fuzzy logic can be used for pattern recognition and classification [23]. The elements of a fuzzy set have degrees of membership. The membership can be from 0 to 100 %. The membership function decides the degree of the element's membership. Fuzzy sets and fuzzy operators are the subjects and verbs of fuzzy logics. Fuzzy inference, as shown in Fig. 3., maps the input to the output using fuzzy logic. The proposed approach is based on a Mamdani type of fuzzy model. Fuzzy logic control system consists of four major parts.

They are fuzzification, rule base, fuzzy inference engine and defuzzification as shown in Fig.3.

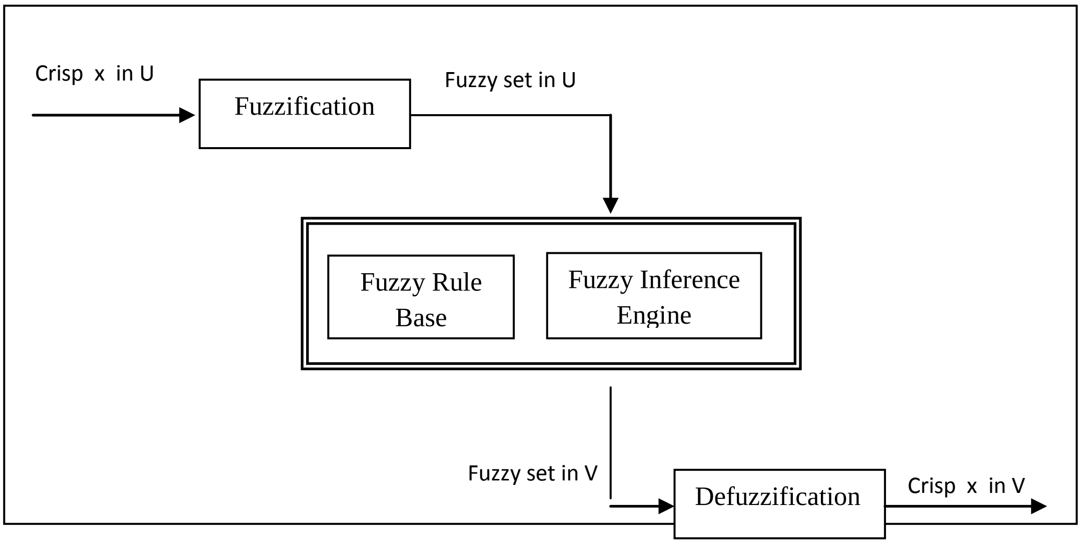

Fig. 3. Fuzzy Logic Controller

A fuzzy set A in the universe of discourse U (into the interval [0, 1]) can be defined as a set of ordered pairs and is given by:

$$\tilde{A} = \{ (x, \mu_{\tilde{A}}(x_i)) \mid x \in U\}$$

where μ Ã (x) represents degree of membership of x in Ã and called membership function of Ã. The membership function defines the degree (0 to 100 %) of a elements membership. The Fuzzy set is represented by the membership function,

$$\mu(x) = \exp\left\{-\frac{(x-\mu)^2}{\sigma^2}\right\}$$

where, μ and σ are the parameters of the membership function.

The fuzzification part accepts the input and measures the values. It performes scaling according to the range mentioned in the parameters and fuzzifies the input. It converts crisp data to fuzzy sets. The main decision making is done in the fuzzy inference engine according to the rules given to the classifier. Defuzzification gives non fuzzy output, which is the inverse of the transformation done in the fuzzification.

Algorithm I : Fuzzy Inference Engine Algorithm

```
Input: Crisp x in U
Output : Crisp y in V

Step 1: start the process
Step 2: fuzzify the input crisp data using $fuzzifier(x_0) = \bar{x}_0$ , $\mu\bar{x}_0\,(x) = \int_{0\; for\; x \neq x_0}^{1\; for\; x=x_0}$
Step 3: find the firing level of each rule
Step 5: find the output of each rule and aggregate the individual rule's output to obtain overall
        output
Step 6: Apply defuzzification operator toobtain crisp data. $z_0 = defuzzifier(C)$, where C is the
        fuzzy set and $defuzzifier$ is a defuzzification operator.
```

6. Experimental Results and Discussion

Signature verification on bank cheques is a difficult task because of the limited number of samples available for training the classifier. In this modeling, the signature is scanned, preprocessed and the features are extracted and fed to the fuzzy classifier. Table 1 shows the performance calculation formula which is applied on the fuzzy logic output values.

. Table 1: Performance measure calculation method

FAR	$\frac{FN}{FN+TN}$
FRR	$\frac{FP}{FP+TP}$
Sensitivity	$\frac{TP}{TP+FN} * 100$
Specificity	$\frac{TN}{FP+TN} * 100$
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN} * 100$

In Table 1, True Positive (TP) indicates number of correct positive predictions, False Positives

(FP) indicates number of incorrect positives, True Negtives (TN) indicates number of correct negatives, and False Negatives (FN) indicates number of incorrect negatives.

Table 2: TP, TN, FP and FN outcomes

	Sign. Set 1	Sign. Set 2	Sign. Set 3
TP	7	12	11
TN	5	0	1
FP	2	0	1
FN	10	12	11

Table 2 shows the true positive, true negative, false positive and false negative values for three signature sets. Each set contains 12 genuine signature and 12 forged signature. The signature set 1 has 24 signatures out of which, 7 signatures are true positive, 5 signatures are incorrectly rejected, 2 signatures are false positives and 10 signatures are wrongly accepted.

Table 3: Sensitivity, Specificity and Accuracy values

	Sign. Set 1	Sign. Set 2	Sign. Set 3	Average
Sensitivity	0.41	0.50	0.50	**0.47**
Specificity	0.29	0.00	0.50	**0.26**
Accuracy	0.38	0.50	0.50	**0.46**

Table 3 shows the sensitivity, specificity and accuracy values for the 72 signatures. Sensitivity is the measure of actual positives and specificity measures the actual negatives. In reality, a person can even digest when his signature is forged by somebody but he cannot digest when his own signature is rejected for a transaction. So a signature verification model is considered best when the false rejection rate is low.

7. Conclusion

Handwritten signature verification is the most easiest and non-invasive biometric method. Signatures can be identified by their geometrical shape. The verification system modeled is generous to intra-personnel signature variations and rude to inter-personnel signature variation ones, the forgery. Zernike moments itself enhances signature verification because of their scale and rotation invariancy property. This shape descriptor feature is combined with geometric features like circularity and aspect ratio and yielded a better accuracy.

References

1. Indrajit Bhattacharya, Prabir Ghosh and Swarp Biswas, Offline Signature Verification Using Pixel Matching Technique, Elsevier Procedia Technology, vol. 10, pp. 970-977, 2013.
2. Ashok Kumar.D and Dhandapani.S, A Bank Cheque Signature Verification System using FFBP Neural Network Architecture and Feature Extraction based on GLCM, IJETTCS, vol. 3, issue 3, pp. 46-52, June 2014.
3. Saki. F, A. Tahmasbi.A, Soltanian-Zadeh.H, Shokouhi.S.B, Fast opposite weight learning rules with application in breast cancer diagnosis, Comput. Biol. Med., vol. 43, no. 1, pp. 32-41, 2013.
4. Rajesh Kumar, J D Sharma, Bhabatosh Chanda, Writer-Independent Off-line Signature Verification using Surroundedness Feature, Pattern Recognition Letters October 10, 2011.

5. Hai Lin and Hai-Zhou Li, Chinese signature verification with moment invariants, IEEE International Conference on Systems, Man, and Cybernetics, Beijing, vol.4., pp. 2963-2968, 1996.
6. Pushpalatha K. N., Kumar Gautham. A, Shashikumar. R, 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, pp. 27-40, 2013.
7. Khotanzad.A and Hong.Y.H., Invariant Image Recognition by Zernike Moments, IEEE Transactions on Pattern Analysis and Machine Intelligence archive vol. 12, issue 5, pp. 489-497, May 1990.
8. Sohail Jafar and Rashid Jalal Qureshi, Off-line signature verification using structural features, 7th International Conference on Frontiers of Information Technology, Abbottabad, Pakistan, December 16-18, 2009.
9. Jovisa Zunic and Kaoru hirota, Measuring Shape Circularity, Proceedings of the 13th Iberoamerican congress on Pattern Recognition: Progress in Pattern Recognition, Image Analysis and Applications, pp. 94 – 101, CIARP, 2008.
10. Huazhong Shu, Limin Luo and Jean-Louis, Moment based Approaches in Imaging, IEEE Eng Med Biol Magazine, vol.26(5), pp. 70-74, Sep-Oct, 2007.
11. Divjyot Singh Puri and Maitreyee Dutta. Article: A Comparative Analysis of Offline Signature Verification using Zernike Moment and Minutiae using Artificial Neural Network Approach. International Journal of Computer Applications 101(14):13-19, September 2014.
12. Neo Han Foon, Ying-Han Pang and D.N.C.Ling, An efficient method for human face recognition using wavelet transform and Zernike moments, International Conference on Computer Graphics, Imaging and Visualization, pp. 65-69, July 2004.
13. Pham, Hong-Ha Le, Nang-Toan Do, Offline Handwritten Signature Verification using Local and Global Features, Springer Annals of Mathematics and Artificial Intelligence , vol 75 , issue 1, pp. 231-247, October 2015.
14. Cemil Oz, Signature Recognition and Verification with Artificial Neural Network Using Moment Invariant Method, Springer, Advances in Neural networks, vol. 3497 of the series Lecture Notes in Computer Science, pp. 195-202, 2005.
15. Pradeep Narayanan Narwade, S.V.Bonde and D.D. Doye, Offline Signature Verification using Shape Dissimilarities, IEEE International Conference on Communication, Information and Computing Technology, pp. 1-6, Jan 2015.
16. Moises Diaz, Miguel A Ferrer, George S Eskander and Robert Sabourin, Generation of Duplicated Off-line Signature Images for Verification Systems, IEEE Transactions on Pattern Analysis and Machine Intelligence, issue: 99, 2016.
17. Jasmine etal, Bank Cheque Authentication using Signature, IJARCSSE, vol 3, issue 5, May 2013.
18. Ashok Kumar.D and Dhandapani.S, A Novel Signature Verification System on Bank Cheque with Fractal Dimensions and Connected Components, IJAER, vol 10, No.(14), pp. 34383-34389, 2015.
19. Alireza Khotanzad and Yaw Hua Hong ,Invariant Image Recognition by Zernike Moments, IEEE Transactions on Pattern Analysis and Machine Intelligence. vol. 12, No. 5, May 1990.
20. Amanatiadis. A and et al, Evaluation of shape descriptors for shape-based image Retrieval, IET Image Process, vol. 5, issue. 5, pp. 493–499, 2011.
21. A. Tahmasbi, F. Saki, S. B. Shokouhi, Classification of Benign and Malignant Masses a. Based on Zernike Moments, Comput. Biol. Med., vol. 41, no. 8, pp. 726-735, 2011.
22. Nedeljkovic.I, Image Classification Based on Fuzzy Logic, The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Vol. 34, Part XXX.
23. Yannis S. Avrithis and Stefanos D. Kollias, Fuzzy Image Classification Using Multiresolution Neural Networks with Applications to Remote Sensing, 2010.
24. Ashok Kumar. D and Dhandapani. S, Offline Signature verification System for Bank Cheques using Zernike Moments, Circularity Property and Neural Network, International Journal of Artificial Intelligence And Applications, Vol. 7, No. 5, pp. 61-77, September 2016.