Offline signature verification based on geometric feature extraction using artificial neural network

Subhash Chandra
Indian School of Mines, Dhanbad, India
Email: subhash08mit@gmail.com

Sushila Maheskar
Indian School of Mines, Dhanbad, India
Email:sushila_maheshkar@yahoo.com

Abstract— **Signature verification is widely used for personal verification. But, it has an inevitable problem of getting exploited for forgery therefore an automatic signature recognition and verification system is required. Verification can be accomplished either Online or Offline based application. Offline systems work on the scanned image of a signature. Online systems use dynamic information like pressure, speed etc. of a signature during the time when the signature is made. In this paper, we present an offline signature verification technique based on geometric features. We have used six geometric features namely Area, Centroid, Standard deviation, Even pixels, Kurtosis and Skewness. In our technique first the preprocessing of a scanned signature image is done to isolate the signature and to remove noise. The system is trained using a database of signatures obtained from authenticated users. Then artificial neural network (ANN) is used in recognition and verification of signatures: genuine or forged, and efficiency is about 89.24% having threshold of 80%. Simulation results shows that the technique is robust and clearly differentiates between genuine and forgery signatures.**

Keywords— Offline signature; Neural network; Geometric feature; False Acceptance Rate; False Rejection Rate.

I. INTRODUCTION

Handwritten signature is widely used for the identification of the particular person. Signature of an individual is recognised as the primary mechanism for both authentication and authorization in legal transactions and help in personal identification. It provides authentication and security to various assets of the signer. In the era of advanced technology security is the vital issue to avoid fakes and forgeries [5]. Thus, an automated signature verification system is demand of the time to improve the authentication process and provide secure means for authorization of legal documents. The signature verification systems help to discriminate between the original and fake signatures. The signature verification is classified into online system and offline verification systems[4]. A signer signs on electronic devices such as Tablet PC, touch screen with an electronic pen, and characteristics like pressure exerted, stroke length, writing speed are used for the verification in online signature verification. In offline signature verification, the signature is done on the paper and is scanned to convert it into digital form. Since the data is in the form of 2-D image, the extraction of dynamic data is a challenging issue where signature verification is done by comparing the signed signature with the template signature already stored in the database at the time of training data[2]. There are two types of variation in the signature, intra variation and inter variation[7]. In intra variation a signature of the same person varies due to abnormal conditions whereas the variation in the original and forged signature is termed as inter variation. In case of forgery, a person attempts to copy the signature of another person. The forgery signature can be classified into three following way [1].

Random forgery: In this type of forgery the signer knows only the name of the person whose signature is to be signed and uses his own style to sign the document and can be detected by naked eye.

Simple forgery: In this case the signer has seen the signature pattern but does not have any prior experience of signing the signature of the victim.

Skilled forgery: Here the signer knows the signature as well as the pattern very well and has experience in forgery. The signer signs exactly the same as the victim and it is very difficult to distinguish between original and forged signature.

In this paper, we focus on the geometric features based on gray scale information from image containing handwritten signatures.

The rest of the paper is organised as follows. Section 2 describes preliminaries of the artificial neural network, section 3 explains proposed algorithm (preprocessing,feature extraction and training). In section 4, experimental results are given. In section 5, conclusion of the paper is stated.

II. PROPOSED ALGORITHM

In this paper, the recognition and verification of offline signature samples using artificial neural network is relevant as it follows a paradiagm which models human learning patterns.

A. Data Acquisition/Signature Database

In offline signature verification signatures from individual person are taken on paper and then scanned with scanner. In

978-1-4799-8579-1/16/$31.00 ©2016 IEEE

this paper we have used standard MCYT-75 offline signature corpus database[3]. The database contains data from individuals, including genuine signatures and forgeries signatures. The signatures are collected by acquisition device using WACOM Intuos (Inking pen). Each signature image having dimension of 850×360 pixels.

B. Preprocessing

Preprocessing help us to improve the property of signature. The scanned signature image may carry spurious noise and has to be removed to avoid errors and make the signatures ready for feature extraction in both training and testing phase. The prepossessing stage includes following steps.
Step 1 (RGB to gray scale conversion): In this step RGB image is converted into gray scale intensity signature image to eliminate the hue and saturation information while retaining the luminance Fig. 2.

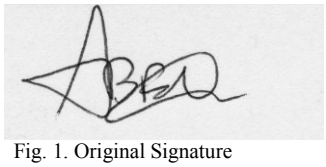

Fig. 1. Original Signature

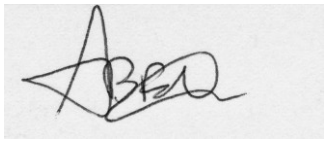

Fig. 2. Gray scale image

Step 2 (Binarization): A gray scale signature image is converted into binary to count the number of black pixels which make feature extraction simpler Fig. 3.

Fig. 3. Binary Image

Step 3 (Cropping): We cropped the image by the value returned by bounding box calculation method. This reduces the area of signature to be used for further processing Fig. 4.

Fig. 4. Cropped Image

C. Feature Extraction

We use features extraction technique to extract the feature of signature image using six global features. The extracted features of a signature image are based on geometrical features like size and shape. The different features we use in this paper are: Standard Deviation, Skewness, Centroid , Kurtosis, Even pixels and Area [8].

1) Area: Total number of black pixels present in the binary image. As for example the area of the selected signature is shown in Fig. 5.

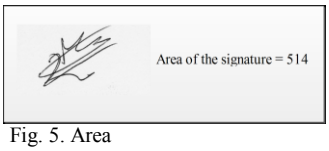

Fig. 5. Area

2) Centroid: It denotes to the center point of vertical and horizontal of the signature. For example the centroid of the selected signature is shown in Fig. 6.

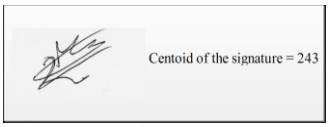

Fig. 6. Centroid

3) Standard Deviation (σ): It measures the amount of variation or dispersion on a set of mean data values. If deviation is closed to the mean data value then the variation is less otherwise spread over a wider range of values.

Standard deviation is mathematically represented as

$$\sigma = \sqrt{\sum_{i=0}^{L-1} (r_i - \mu)^2 \, p(r_i)} \tag{1}$$

where, [0,L-1] is range of intensity value, r_i is i^{th} intensity value, $p(r_i)$ is probability of intensity r_i .

$$p(r_i) = n_i / M * N \tag{2}$$

where, n_i is number of pixels in the signature with intensity r_i , $M * N$ is size of signature, μ is average intensity value.

$$\mu = \sum_{i=0}^{L-1} (r_i) p(r_i) \tag{3}$$

In image processing, standard deviation is used as sharpening of edge, as the pixel value varies most at the edge of image. Standard deviation of signature is shown in Fig.7.

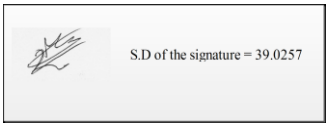

Fig. 7. Standard Deviation

4) Skewness: It measure the asymmetricity of the probability distribution of a real valued random variable having positive, negative or may have undefined value, where positive denote that the tail on the left side is smaller

978-1-4799-8579-1/16/$31.00 ©2016 IEEE

than the right side while negative represent that the tail on the right side of the probability density function is smaller than the left side and zero denote that the values are comparatively distributed on either sides of the mean.

Skewness is mathematically represented as

$$S = \sigma^{-3} \sum_{i=0}^{L-1} (r_i - \mu)^3 \, p(r_i) \tag{4}$$

where, σ is standard deviation, L is intensity level, r_i is the i^{th} intensity level, μ is the average intensity value, $p(r_i)$ is the probability of intensity r_i .

In terms of image processing, hazy and smooth surfaces bend towards positively skewed than lighter and matte side. So skewness is used in making discretion of image level. As for example the skewness of the signature is shown in Fig. 8.

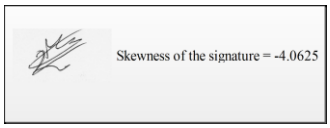

Fig. 8. Skewness

5) Kurtosis: It measures the structure of probability distribution function of a real valued random variable and is related to the fourth moment of a mean. Higher value of kurtosis distribution indicates thicker tails, longer and a sharper peak whereas lower value denotes shorter, thinner tails.

Kurtosis is mathematically represented as

$$K = \sigma^{-4} \sum_{i=0}^{L-1} (r_i - \mu)^4 \, p(r_i) \tag{5}$$

where, σ is standard deviation, L is intensity level, r_i is the i^{th} intensity level, μ is the average intensity value, $p(r_i)$ is the probability of intensity r_i .

In image processing kurtosis values are illustrated in combination with resolution and noise measurement. In which high kurtosis values gives low noise and low resolution. Kurtosis of signature is shown in Fig. 9.

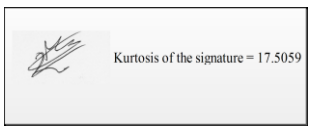

Fig. 9. Kurtosis

6) Even pixels: The positions in the image matrix. Even position refers those matrix positions for which both the coordinates are even. For example the even pixel count of the signature is shown in Fig. 10. Overall extracted feature of a signature is shown in Fig. 11.

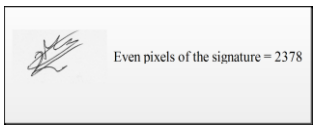

Fig. 10. Even pixels count

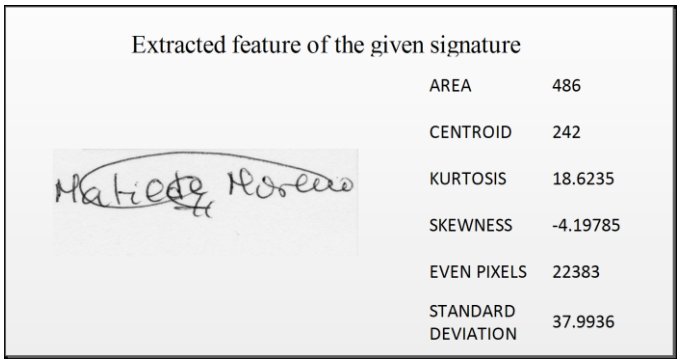

Fig. 11. Extracted Feature

D. Training and Verification

The geometric feature are extracted and organised as an input array to the back propagation network. The selected feature vectors are directed as input to the neural network. The trained neural network is used to verify the signature as either genuine or forged. If the signature is match then it shows genuine otherwise forgery Fig. 11.

III. Experimental Results

A. MCYT database

The signature database is collected from MCYT-75 offline signature corpus database[4]. Each signature is done using a WAMCOM Intuous inking pen. In which 15 genuine and 15 forgery signature samples are given for each of 75 users in database. The forgery signature in the MCYT database is the mixture of random, simple and skilled forgeries.

B. Performance measures

The performance measure of the signature verification is measured in terms of false rejection rate (FRR) and false acceptance rate (FAR). False acceptance occurs when forgeries signatures are accepted as genuine while in case of false rejection genuine signature are accepted as forgery.

$$FAR = \frac{\text{Number of genuine accepted}}{\text{Number of forgery tested}} \times 100 \tag{6}$$

$$FRR = \frac{\text{Number of genuine rejected}}{\text{Number of genuine tested}} \times 100 \tag{7}$$

978-1-4799-8579-1/16/$31.00 ©2016 IEEE

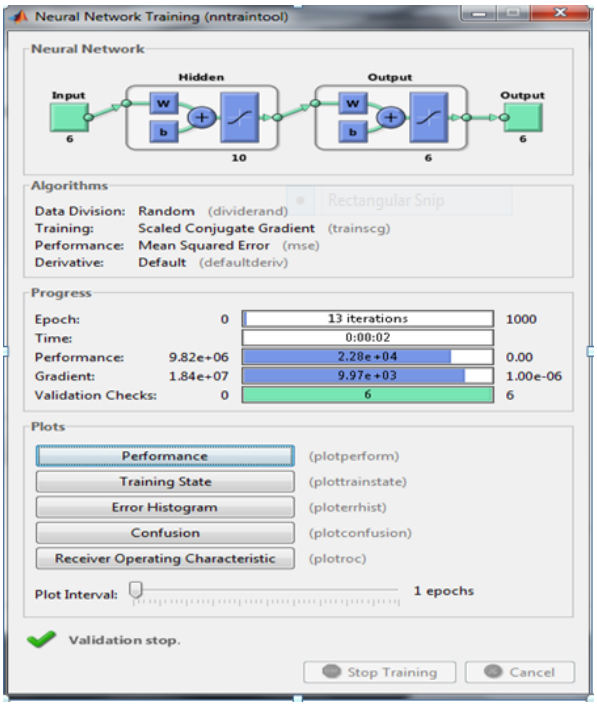

Fig. 12. Trained data

The overall accuracy of the system is the mean between percentage of genuine signatures verified as genuine and percentage of forgery signature is verified as forgery.

$$Accuracy = \frac{(100 - FAR) + (100 - FRR)}{2} \qquad (8)$$

C. Results

Simulation was performed on Matlab R2013a to assess the performance of proposed method. Experiments were conducted on 18 different users. Each having 15 genuine and 15 forgery signatures. Total number of 540 signature is taken each having dimension of 850×360 pixels. As shown in Figure 13 and Figure 14 we have GUI interface. First we train the data through neural network. Then select signature from the test database. The neural network is trained with signature database having 180 signatures. The result is demonstrated on a database of 18 users each having 15 signatures. Out of these 8 signature are genuine while 7 of them is forgery. Furthermore, the simulation has been done and features are extracted. Then the neural network is tested with 360 signatures of 18 users each having 15 signatures. Out of these 7 signature are genuine while 8 of them is forgery. In which, we have obtained FAR of 10.62 and FRR of around 10.91. The tested results is shown in Fig. 5. and Fig. 6. Table 1 shows the comparison results with the existing technique. Thus, the total accuracy obtained using the proposd method comes out to be above 89.24% .

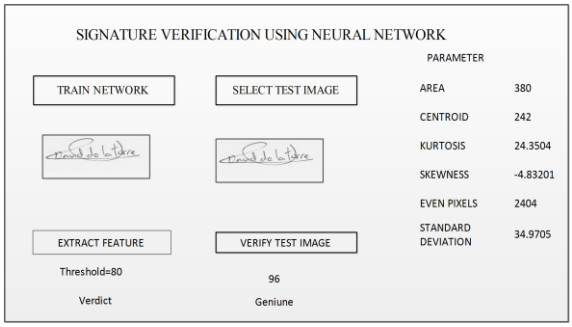

Fig. 13. GUI of the genuine signature recognised

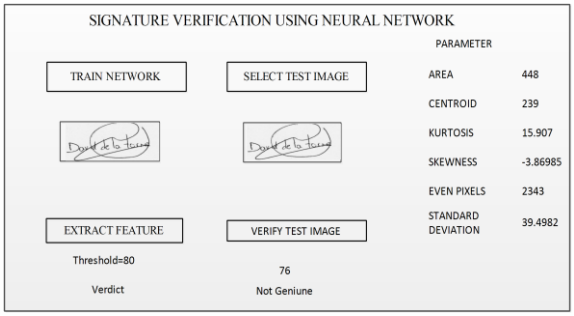

Fig. 14. GUI of the forgery signature recognised

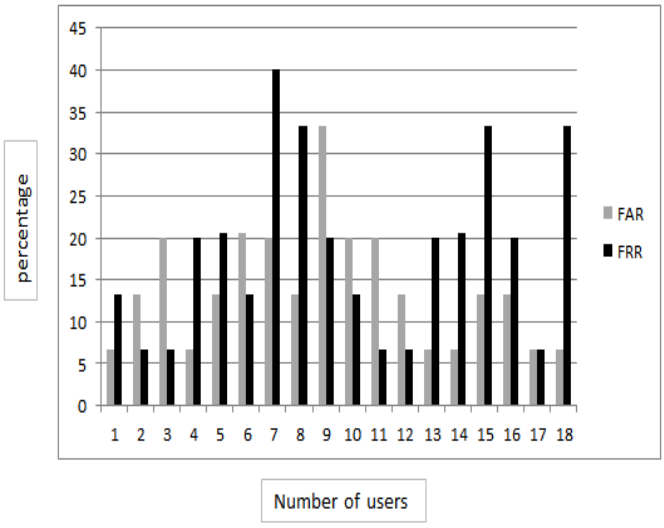

Fig. 15. FAR and FRR of each user

TABLE I: COMPARISON WITH THE EXISTING TECHNIOUES

TECHNIQUE	No.of Signature	TRR	TAR	FAR	FRR	EFFICIENCY
Sisodia et al [6].	240	95.83	92.72	4.16	7.29	94.22
Proposed method	540	89.09	89.38	10.62	10.91	89.24

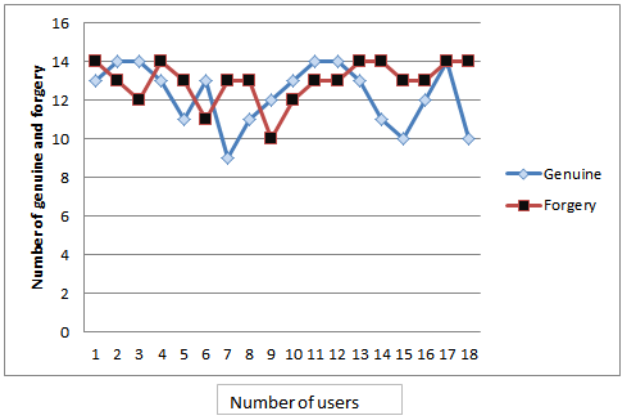

Fig. 16. Number of Genuine and Forgery signature recognised

IV. CONCLUSION

In this paper, we explored the application of geometric based feature extraction on offline signature verification. The performance of the proposed method is examined using Back propagation learning technique, with 18 sets of different users having varying number of training and testing samples. Experiments were conducted on CEDAR dataset. In terms of future work, better preprocessing method will be designed to improve the accuracy of the geometric based feature extraction.

REFERENCES

[1] Mujahed Jarad, Nijad Al-Najdawi, and Sara Tedmori. Offline handwritten signature verification system using a supervised neural network approach. In Computer Science and Information Technology (CSIT), 2014 6th International Conference on, pages 189–195. IEEE, 2014.

[2] Ali Karouni, Bassam Daya, and Samia Bahlak. Offline signature recognition using neural networks approach. Procedia Computer Science, 3:155–161, 2011.

[3] Javier Ortega-Garcia, J Fierrez-Aguilar, D Simon, J Gonzalez, M Faundez-Zanuy, V Espinosa, A Satue, I Hernaez, J-J Igarza, C Vivaracho, et al. Mcyt baseline corpus: a bimodal biometric database. IEE Proceedings-Vision, Image and Signal Processing, 150(6):395–401, 2003.

[4] Meenakshi Sharma and Kavita Khanna. Offline signature verification using supervised neural networks. International Journal of Management, IT and Engineering, 4(8):82, 2014.

[5] Jyoti Singh and Manisha Sharma. Offline signature verification using neural networks. i-Manager's Journal on Information Technology, 1(4):35, 2012.

[6] Kshitij Sisodia and S Mahesh Anand. Off-line handwritten signature verification using artificial neural network classifier. International Journal of Recent Trends in Engineering, 2(2):205–207, 2009.

[7] Shiwani Sthapak, Minal Khopade, and Chetana Kashid. Artificial neural network based signature recognition & verification. International Journal of Emerging Technology and Advanced Engineering, ISSN-2250-2459, ISO, 2008, 2001.

[8] Htight Htight Wai and Soe Lin Aung. Feature extraction for offline signature verification system. IJCCER, 1(3):84–87, 2013.

978-1-4799-8579-1/16/$31.00 ©2016 IEEE