International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 12 6784 - 6787

Neural Network Based Approach For Signature Verification And Recognition

Ms. Shital S. Wagh
Department of Computer Science And Engineering,
PRMIT, Badnera,
Amravati, India
shitalwagh12@gmail.com

Dr. S. R. Gupta
Department of Computer Science And Engineering,
PRMIT, Badnera,
Amravati, India
sunilguptacse@gmail.com

***Abstract*—** Signature can be seen as an individual characteristic of a person which can be used for his/her validation. An automated signature verification and recognition technique saves valuable time and money. Neural network based approach for signature verification and recognition discussed in this paper which enables the user to recognize whether a signature is original or a fraud. The user introduces into the computer the scanned images, modifies their quality by image enhancement and noise reduction techniques, to be followed by feature extraction and neural network training, and finally verifies the authenticity of the signature. The paper is primarily focused on five features of extraction like eccentricity, kurtosis, skewness, orientation and centroid. The extracted features of investigation signature are compared with the previously trained features of the reference signature. This technique is suitable for various applications such as bank transactions, passports with good authentication results etc

Keywords-*image processing; neural network; feature extraction; signature verification and recognition*

*****

I. INTRODUCTION

Signature verification is an important research area in the field of person's identity authentication. Signature Verification is the process of recognizing an individual's handwritten signatures. Signatures have been by far the most popular means for establishing the authenticity of individuals. Signature authentication offers a quick, simple and cost effective means for validating the authenticity of a document by determining the difference between an original signature and a counterfeit one. In this area signature is a special case that provides secure means for authentication, attestation authorization in many high security environment. The signature verification has an advantage over other forms of biometric security verification techniques; including fingerprint, voice, iris recognition, palm prints, and heart sound recognition. It is mostly used to identify a person carrying out daily routine procedures, i.e. bank operations, document analysis, electronic funds transfer, and access control, by using his handwritten signature [1,2].

A signature verification and recognition system and the techniques used to solve this problem can be divided into two classes Online and Off-line. On-line approach uses an electronic tablet and a stylus connected to a computer to extract information about a signature and takes dynamic information like pressure, velocity, speed of writing etc. for verification purpose. Off-line signature verification involves less electronic control and uses signature images captured by scanner or camera. An off-line signature verification system uses features extracted from scanned signature image. The features used for offline signature verification are much simpler [4]. This paper deals with an automated method of verification an off line signature recognition by extracting features that characterizes the signature. The approach starts by scanning images into the computer, then modifying their quality through image enhancement and noise reduction, followed by feature extraction and neural network training, and finally verifies whether a signature is original or fake. [5,7,8]

The objective of the signature verification system is to discriminate between two classes: the original and the forgery, which are related to intra and interpersonal variability. The variation among signatures of same person is called Intra Personal Variation. The variation between originals and forgeries is called Inter Personal Variation [5].

II. TYPES OF FORGERIES

Forgeries are then further classified into three different categories namely Random, Simple and Skilled.

A. Random forgery

The signer uses his/her own style to forge the victim sign to create a forgery is known as random forgery. It is very easy to recognize by the naked eye. These signatures are not based on any knowledge of the original signature. Please embed symbol fonts, as well, for math, etc.

B. Simple forgery

The signer does not have any prior experience to forge the victim sign for forgery is known as simple forgery. It is also very easy to detect by the human eye. These are based on an assumption of how the signature looks like by knowing the name of the signer.

C. Skilled forgery

It is the most difficult than rest of all forgeries. The signer is an expert and has prior experience to copy the victim sign to make forgery or in other words it is an imitation of the original signature. It is very hard to recognize by eye even by the verification system.

III. PROCESS METHODOLOGY

There are three major steps used for signature verification and recognition and each of these steps consists of many methods that contribute to improved results. Following steps are:

A. Data Acquisition

Paper based signature is first converted into a digital image by scanning and then it is used for verification purpose.

B. Image Pre-processing

It is the most important step in signature verification and recognition that exists for the manipulation and modification of images. Its successful implementation produces improved results and higher accuracy rates.

Different levels of processing are

1) Elimination of background: Threshold method is used to extract the signature from the background of a signature. All pixels of signature are converted to "1" and rest of pixels those are belongs to background of signature convert to "0".

2) Noise reduction and width normalization: Noise reduction filter is employed to the binary signature to do this job. It removes the single black pixels on the white background. Defects removal, image enhancement and quality achieved. Width normalization means given signature is then resized for proper dimensions because the signature may vary between interpersonal and intrapersonal.

3) Thinning: Thinning removes the thickness differences that can occur because of different pens. Thinning operations uses morphology concept. Morphological operations rely only on the relative ordering of pixel values, not on their numerical values, and therefore are especially suited to the processing of binary images. Morphological operations can also be applied to greyscale images such that their light transfer functions are unknown and therefore their absolute pixel values are of no or minor interest.

Morphological Operations are of two types,

- Dilation- Dilation, in general, causes objects to dilate or grow in size
- Erosion- Erosion causes objects to shrink.

Figure 1 Original Scanned Signature

Figure 2 Segmented and binarized signature

Figure 3 Thinned Signature

C. Feature Extraction

The main function of this step is to generate features which can be used as comparison measurements. Since the issue of signature verification is a highly sensitive process, more than one feature/measurement has to be generated in order to enhance the accuracy of the results. The term feature here refers to a certain characteristic that can be measured using designed algorithms; which can then be retrieved by "extraction"[1]. For this signature recognition and verification research, five main features will be extracted. These features are: eccentricity, skewness, kurtosis, orientation and centroid.

1) Eccentricity: Eccentricity is defined as the central point in an object. In case of signature image, eccentricity is the central point of the signature. The importance of this feature is that we need to know the central point of 2 images in order to compare them. After identifying the central point, we can then compare the features around them. If there is a deviation in the central point of an image, this will indicate a possible imitation of the signature, but this is not enough evidence by itself. The central point is acquired by applying the ratio of the major to the minor axes of an image.

2) Skewness: "Skewness is a measure of symmetry, or more precisely, the lack of symmetry. A distribution, or data set, is symmetric if it looks the same to the left and right of the center point" [11]. The measurement of skewness allows us to determine how bowed are the lines in each segment of the signature. The percentage of this torsion is then calculated and extracted. Furthermore, this percentage is compared to that extracted from the other image. The importance of this feature is that it measures the symmetry or the lack of it, which is an important aspect of a signature. Most signatures are complicated, with no edges but twists, and the width and height of these twists is a very important aspect for measurement and comparison.

3) Kurtosis: Kurtosis is a measure of whether the data are peaked or flattened, relative to a normal distribution. That is, data sets with high kurtosis tend to have a distinct peak near the mean, decline rather rapidly, and have heavy tails. Data sets with low kurtosis tend to have a flat top near the mean rather than a sharp peak. A uniform distribution would be the extreme case [11]. The kurtosis measurement highlights the peaks in each segment of a signature. It also measures the existence, or the absence of tails, that are unconnected lines with no peaks. As you can see, kurtosis and skewness are highly interlinked.

4) Orientation: Orientation defines the direction of the signature lines. This feature is important because it allows us to know how the signer wrote down the signature, which letters came first emphasizing the direction of angles and peaks. The orientation feature is used to compute the optimal dominant ridge direction in each block of a signature. Orientation is acquired by applying the ratio of angle of major axis. The orientation of the signature can be found using the Matlab "regionprops" function, in which the angle between the x-axis and the major axis of the ellipse that has the same second-moments as the region.

5) Centroid: Centroid is the point where all the weight of an image concentrated. Signature image is combination of black and white portion. Centroid determine the point where weight of white portion located. This value of each and every signature varied so this feature is important in feature extraction.

IV. SIGNATURE PROCESSING AND NEURAL NETWORK APPROACH

Processing of signature consists of two main parts that is Trainning phase and Testing phase. In experiment of proposed method, standard database that is GPDS960 used to train the network, and also some skilled forgeries are introduced in the training dataset. Neural networks are known for being a very accurate and efficient technique for pattern recognition in general. In this section, we will explain more about the idea and structure of neural networks, their types, and how they contribute to pattern recognition. A neural network is one application of artificial intelligence, where a computer application is trained to think like a human being or even better. A neural network is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. The key element of this paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems [12]. As back-propagation is having the highest classification accuracy as compared with other implemented algorithms. Feed-forward networks have the following characteristics: Perceptrons are arranged in layers, with the first layer taking in inputs and the last layer producing outputs. The middle layers have no connection with the external world, and hence are called hidden layers. Each perceptron in one layer is connected to every perceptron on the next layer. Hence information is constantly "fed- forward" from one layer to the next., and this explains why these networks are called feed-forward networks. There is no connection among perceptrons in the same layer. Back-propagation is used for its simplicity, efficiency and performance measure. Different types of Back propagation are studied .From which Feed-forward back-propagation network, Cascade-forward back-propagation network are giving the finest results .Diagrams of those neural networks are shown below.

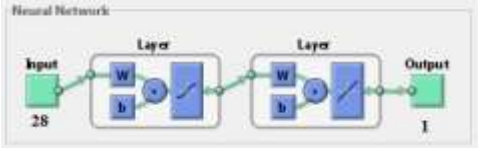

Figure 4 Feed forward neural network

A. Training and testing: The proposed network was trained with input database GPDS960. When the training process is completed for the training data, the last weights of the network were saved to be ready for the testing procedure. The time needed to train the training datasets was approximately 10 minutes. The testing process is done for various signatures that are fed to the proposed network and their output is recorded.

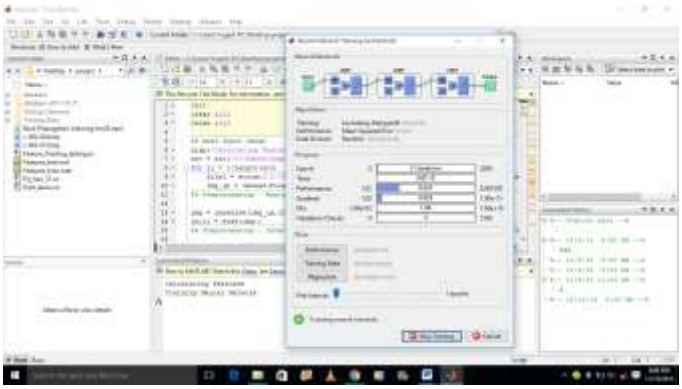

Figure 5 Training window

This is the training window while traning neural network. Training State Plot: Training state plot show the deferent training state in training process and validation check graph. These plots also show the momentum and gradient graph and state in training process. The results show in the following figure 6.

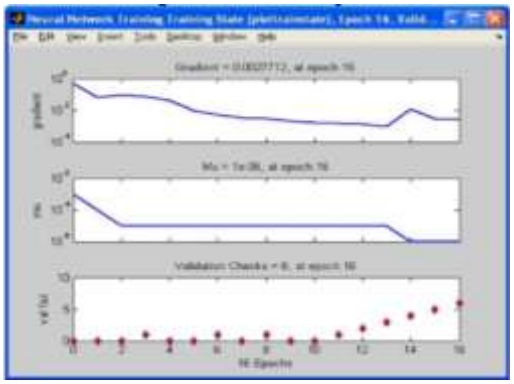

Figure 6 Training state plot

Like wise of training state plot there are Performance plot: Performance plot show the training errors, validation errors, and test errors appears, as shown in the training process. Training errors, validation errors, and test errors appears. After training neural network, neural network training window shows that the performance goal mate. Also specify the accuracy of trainlm. Then it is ready for testing. When we enter coice 1 for evaluation then it shows the values of all features like eccentricity, kurtosis, skewness, orientation angle along with values of False Acceptance Rate (FAR) and False Rejection Rate (FRR). When we want to verify any signature , we have to provide that image as an input. Then it evaluated whether the image is genuine or forgery.

V. RESULT AND ACCURACY

As mentioned earlier in this paper, security is one the most critical issues when it comes to signature recognition, especially if used by banks. One fraud signature, can mess up transactions, causes the bank and customers financial losses, and affect the security reputation of the bank, which is a damage that cannot be easily fixed[9]. For those reasons, 5 features were used in the feature extraction section of this dissertation, and were applied to all the samples tested. In addition to that, the following are the accuracy rates and error rates calculated as an average of the calculations made for over more than 200 samples. For that standard database have been used that is GPDS960.

Error rates are useful to determine result and accuracy of signature verification and recognition system. Types of error rates are as follows False rejection rate (FRR) is one of the most important specifications in any biometric system. The FRR is defined as the percentage of identification instances in which false rejection occurs. It is also known as Type- I error

$$FRR = \frac{number\ of\ originals\ rejected}{number\ of\ originals\ tested} \times 100$$

False acceptance rate (FAR) is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts. It is also known as Type- II error [10].

$$FAR = \frac{number\ of\ forgeries\ accepted}{number\ of\ forgeries\ tested} \times 100$$

A following error rate is hereby reported by this approach, a great improvement over other published studies.
FAR (False Acceptance Rate) = 0.41
FRR(False Rejection Rate) = 0.45
Also training and testing accuracies are as follows

	Proposed System
Training Accuracy	80 %
Testing Accuracy	66 %

This indicates that approach of proposed system and the five features are working well with a good optimization of verification and recognition of the offline signature.

VI. CONCLUSION

This paper presents a method for offline signature verification and recognition by using neural network that used five features; eccentricity, skewness, kurtosis, centroid and orientation, which can be extracted by image processing. The neural network was trained using backpropagation concept. Error rate is hereby reported by this approach, a great improvement over other published studies that reported error rates, FAR is 0.41 and FRR is 0.45. Also accuracy of training is 0.80 while testing accuracy is 0.66. This indicates that proposed approach based on five features are working well with a good optimization of verification and recognition of the offline signature.

REFERENCES

[1] S.Odeh, M.Khalil, "Offline Signature Verification and Recognition: Neural Network Approach," IEEE, 2011, 978-1-61284-922-5/11.

[2] C. Allgrove and M.C. Fairhurst, "Majority Voting for Improved Signature Verification," IEE Colloquium on Visual Biometrics 2000, (Ref No. 2000/018), pp. 9/1 –9/4.I.

[3] J. F. Vargas, M. A. Ferrer, C. M. Travieso, J. B. Alonso , "Offline Signature Verification Based on Pseudo-Cepstral Coefficients ", 10th International Conference on Document Analysis and Recognition, IEEE, DOI 10.1109/ICDAR.2009.68, 2009, pp. 126–130.

[4] Ashwini Pansare, Shalini Bhatia, "Handwritten Signature Verification using Neural Network", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 1– No.2, January 2012

[5] Mahendra S. Chauhan, "Offline Signature Verification Scheme Using Feature Extraction Method" thesis, NIT, Rourkela, May 2007

[6] M. Ferrer, J. Alonso, and C. Travieso, "Offline geometric parameters for automatic signature verification using fixedpoint arithmetic". IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(6):993– 997, 2005.

[7] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, and J. Ortega-Garcia, "An off-line signature verification system based on fusion of local and global information", In Workshop on Biometric Authentication, Springer LNCS-3087, pages 298–306, May 2004.

[8] N. S. Kamel, S. Sayeed, and G. A. Ellis, "Glove-Based Approach to Online Signature Verification", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 30, No. 6, 2008, pp. 1109-1113.

[9] 'Apply Multi-Layer Perceptrons Neural Network for Off-line Signature verification and recognition' by S. Odeh, M. Khalil, IJCSI, Vol. 8, Issue 6, No 2, November 2011

[10] S. Khan and A. Dhole, " A Review on Off line signature verification and recognition Techniques", IJARCCE, Vol.3, Issue 6,June 2014.

[11] A. Kholmatov and B. Yanikoglu, " Biometri authentication using online signatures". In Lecture Notes in Computer Science- ISCIS. OCT.2004.

[12] C. Stergiou, and D. Siganos, "Neural Networks. Computing". Surprise96 journal, vol. 4, 1996.