An Enhanced Artificial Neural Network Based Offline Signature Verification and Recognition System

Shilpa Adke (M.E-II Computer)
Prof. Anagha. P. Khekar (Guide)
Department of Computer Engineering,
Matoshri College of Engineering and Research Centre,Nashik
University of Pune

Abstract

*Today's society has placed biometrics at the vital position to cater the needs of security requirements. Handwritten signature is one such biometric behavioural characteristic which is widely accepted attribute for signature identification. Forging of signature is the major hurdle in applications of signature verification. Since last two decades, researchers have contributed a significant work to mitigate such forgery by enhancing the designs of classifiers used for signature recognition. Research was initiated by developing special Artificial Neural Network (ANN) called Siamese. Further combination of ANN with segmentation and spectral analysis was introduced. In addition to this, method based on moment invariant, Support vector machine and Hidden Markov Model were developed to cater the same. With such an amendment, desirable classifiers were introduced but the features on which the results obtained were simple in all the previous contributions and 44% error rate was reported. Later the signature verification system comprised of ANN as classifier and features viz. Kurtosis, skewness, orientation and eccentricity reported 21% error rate. It indicated further scope for improvement in terms of accuracy and error rate. In view of this, proposed work is presented to focus on observed vital feature aspect and introduces new features viz. 60 points feature and weight * depth value. It is an extension of earlier work which includes ANN with back propagation algorithm as a classifier. This proposed work is tested on standard benchmark GPDS 300 signature database. The results clearly indicate enhancement in the performance of the system in terms of 88% accuracy and reduced error rate by 9%*

1. Introduction

In biometric systems, various forms of biometric security exists which includes finger printing, iris recognition, speech recognition and keystroke recognition [1]. However despite the novelty and achieved security of the above mentioned techniques, the most natural method for verifying ones identity is through the use of a handwritten signature. Signature verification is an automated method of verifying and recognizing a signature by extracting features about a signature shape and the characteristics of how the person signs name in real-time. Proposed work deals with an automated method of verifying an offline signature recognition by extracting features that characterizes signature. The approach begins by acquiring and scanning images into the computer. Further, the images undergoes pre-processing like gray scaling, thresholding, scaling, inverting and thinning. Image enhancement is followed by feature extraction process, neural network training and finally verifies whether a signature is genuine or a forgery.

The purpose of proposed work is to determine how precisely the novel features eradicate or minimize the errors prevailed in existing signature system. From the analysis of previous research contributions, it was retrieved that the performance of signature system crucially depends upon the classifiers utilized, features on which classifiers compare their values and data sets applicable for respective fields.

1.1 Artificial Neural Network

Neural networks - like human beings depend on the idea of learning in order to achieve any task. They learn through training on a large number of data, which enables them to create a pattern with time, that they will use later. They are found very much useful in detecting patterns that are complicated and hard to derive by humans or by simple techniques. Just like the case of signature recognition, it is very hard to tell whether a signature is original or forged, especially if it is carried out by a skilled forger. Thus a more advanced technique is required to detect the signature recognition. Neural networks learn by themselves through various cases. It learns the recognition of patterns once trained precisely.

2

Results of Neural networks are improved if they are trained by considering large amount of data. So they are found to be very applicable in the systems where security is highly valued.

3

In proposed work we will use Multi Layer Perceptrons MLPs neural network. The structure of this neural network depends on the multi layer feed forward, where all the nodes in any layer have connections to all the nodes in the next layer and so on, but these nodes do not have any connections with the previous layers. Then, it was modified to function as a back propagation neural net-work, using the BP algorithm.

2. Related Work

The review of relevant literature in the field of signature verifications systems has been taken since last two decades and presented below in brief.

The research in signature verification filed using artificial neural network was initialized by J.Bromley et.al in 1993 by introducing the Siamese based time delay network concept to verify signature [2]. This method considered features like speed and acceleration which penalized the forgers who do not write at correct speed. But the the speed of particular signature cannot be the vital feature to detect forgery.

In the next year, G. Dimauro introduced a method for signature verification based on component oriented algorithms. It was found that to be more complex concern with practical implementations [3]. In this light, T.Kiet et.al in 2001 presented work which considered the pen pressure measurement as a feature to be extracted. The attempt failed as an error rate of 2.13 was encountered for rejecting genuine signatures and 3.40% for accepting false signatures.

After two years, Z.demir et.al combined the techniques of image processing, global invariants and some global variables with ANN [5]. They considered global features like signature area, height to width ratio, maximum horizontal histogram and maximum vertical histogram. The system failed due to lack of trained ANN. Their study concluded that errors can be eradicated, if more features are considered during the overall forgery analysis.

In next year, J.Fierrez-Aguilar proposed an online signature verification based on local and global analysis[6]. Their work concluded that the performance can be improved by exploiting user interactions. After an year, M.E Karshgil et.al proposed the utilization of SVM for offline signature verification [7]. They considered features like signature area, signature height to width ratio, maximum horizontal histogram, horizontal and vertical centre of the signature and edge points of the signatures. Their work highlighted the major difference between the classifiers ANN and SVM still the results can be improved if more features concentrated approach is implemented.

In the same year, M.Ferrer et.al proposed offline geometric Parameters for automatic signature verification using Fixed-Point Arithmetic [8]. They utilized two classifiers Hidden Markov Model and Support Vector Machine. Results revealed that their method was only useful in detecting simple and randomly forged signatures but failed for skilled forgery.

In 2011, Manal khalil et.al proposed an extension of the earlier work and developed an offline signature verification system using artificial neural network approach along with back propagation algorithm. They considered 4 features viz. Eccentricity, kurtosis, orientation and skewness. The classifier was implemented successfully but an error rate of 22.1 % encountered in rejecting genuine signatures. The proposed work is an extension of this work with consideration of strong features viz. 60 points feature and weight*depth feature value of the signature.

3. Image Pre-processing

Image pre processing is the firstly implemented to enhance the signature image quality. Thresholding, thinning, gray scaling and inverting were performed.

4. Features Extraction

4.1 60 Points Feature

A geometric image is based on 2-dimensional plane. 60 points of an image are obtained by considering the vertical and horizontal plane. At first centre point of signature is determined. with reference to the centre , signature image is braked along the horizontal and vertical plane. 4 squares are obtained with this splitting. A centre of each square is determined. Again each square is braked along corresponding horizontal are vertical plane. After complete splitting 30 points were obtained horizontally and 30 points were obtained vertically. At the end 60 points are extracted of a given signature im-age. The figures 1,2 and 3 provide the exact working of horizontal and vertical splitting. This 60 points are totally unique for corresponding signature. Hence it can be considered as a vital feature to verify signatures in the proposed system

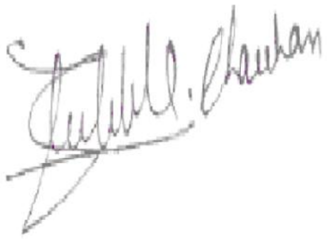

Figure 1 Given signature

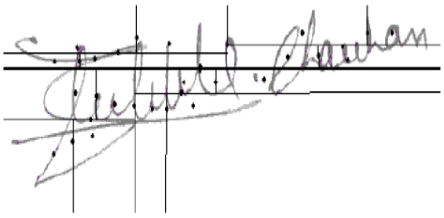

Figure 2.Thirty Points obtained by horizontal splitting

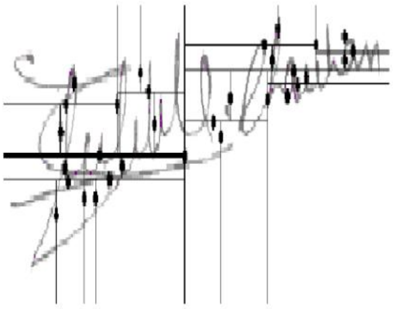

Figure 3.Thirty Points obtained by vertical splitting

4.2 Wight *Depth Value

The basic purpose of 60 points is to determine the similarity between the user features and the features saved in databases. The similarity factor value is computed using weight*depth value of corresponding feature point.

5. Signature Recognition and Verification

Artificial Neural Network learns through training, similar to human brain. The neural networks are trained to extract the 60 points and weight * depth value feature of the input signatures. With the help of these values it will recognize the user. With the reference of the similarity between the feature points of users against those saved in database the respective user is verified. The process is follows

The trained neural network that has learned how to work on signatures and their features through training compares features of the given signatures with those saved in databases.

a. The differences between the extracted features from the new signature and those in databases are calculated.

b. The tag of the signature with least differences is then returned with a number showing difference.

c. If the difference ranges between 1500-2000 it is a genuine signature. If the difference ranges up to 3000 it is still accepted. But above 3000 is suspicious.

6. Results and Discussion

The results of the developed system are obtained by testing on various users in datasets. The obtained results of feature extraction, 60 points are shown in below figures. Skewness of the signature signifies the lack of symmetry. A distribution is symmetric if it looks the same to the left and right of the centre point. Kurtosis is a measure of whether the data are peaked or flat relative to a normal distribution. Standard deviation shows how much variation which exists from the average or expected value. A low standard deviation indicates that the data points tend to be very close to the mean. High standard deviation indicates that the data points are spread out over a large range of values. 60 points feature is used to determine the similarity between stored user signature and the current user by comparing weight*depth value the user is recognized either genuine or fraud user. Zonal features indicate the boundaries of different regions. Precision is the fraction of retrieved instances that are relevant, while recall is the fraction of relevant instances that are retrieved. The precision and recall depicted enhance performance of the developed work as compared to the previous contribution.

7. Conclusion

The offline signature verification and recognition system comprised of MLP ANN as classifier and60 points considered as features has been developed and thoroughly tested on the benchmark and other databases. The results of this system clearly indicates increased accuracy and decreased error rate in comparison with earlier system which considered 4 features: eccentricity, kurtosis, orientation and skewness. Error rate is about 12 % which is decreased by 9% as compared to previous work. Accuracy rate obtained is 88% which is enhanced as compared to previous work by 10%

The developed work can be extended further by changing existing classifier by considering same 60 points feature. It may be predicted that the best classifier tested with 60 points feature will provide further improvement in the performance of offline signature verification and recognition system.

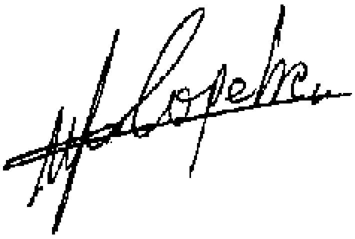

Figure 4. Original signature

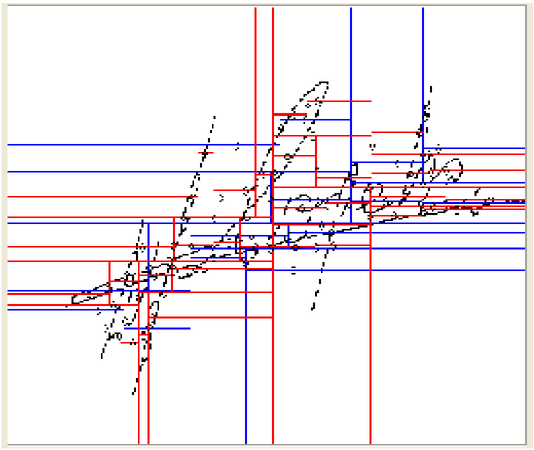

Figure 5. Sixty points feature obtained

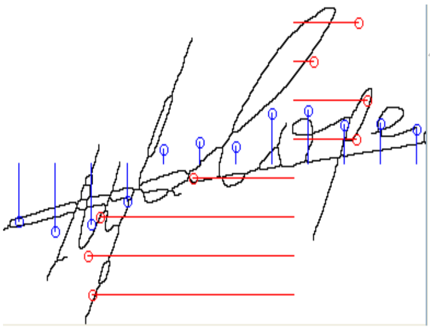

Figure 6. Zonal features obtained

Table 1. Results of previous system

Stage	Accuracy rate	Error Rate
Training	64%	36%
Test	78.8%	21%

Table 2. Results of proposed system

Stage	Accuracy Rate	Error Rate
Training	86%	14%
Test	88%	12%

References

1. J.F.Vargas et.al., ”*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. 126âĂ 130.
2. R.D Sudhakar et.al., ”*Offline signature verification and recognition: An approach Based on Four Speed Stroke Angle*” International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009.
3. Bromley et.al., ” *Signature Verification Using a ”siamese” Time Delay Neural Network*”. Copy-right,1994, American Telephony and Telegraph Company.
4. S.KUMAR et.al., ”*offline Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks*”, International Journal of Engineering Science and Technology Vol. 2(12), 2010, 7035-7044.
5. M.E.Karshgil et.al.,” *Offline Signature Verification and Recognition by Support Vector Machine*”
6. M.A.Ferrer et.al., ”*offline Geometric Parameters for Automatic Signature Verification Using Fixed-Point Arithmetic*”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.27,No.6,June 2005.
7. L.Nanni et.al., ”*An Offline Signature Verification System Based on Fusion of Local and Global Information*”, AVBPA 2005, LNCS 3546, pp. 523âĂ 532, 2005. Springer-Verlag Berlin Heidel-berg 2005.
8. M.Khalil et.al.,”*Offline signature verification and recognition: A Neural Network Approach*”, 2011 IEEE
9. N.S. Kamel et.al., ”*Glove-Based Approach to Online Signature Verification*”, IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol.30, No.6,June 2008.
10. ASHRAF A. ZAHER et.al., ” *A Hybrid ANN-Based Technique for Signature Verification*” ,Proceedings of the 4th WSEAS International Conference on COMPUTATIONAL INTELLIGENCE.
11. B.Erkmen et.al,. ”*Conic Section Function Neural Network Circuitry for Offline Signature Recognition*”,IEEE TRANSACTIONS ON NEURAL NETWORKS, VOL. 21, NO. 4, APRIL 2010.
12. D.Zhang et.al., ”*Guest Editorial Special Issue on Biometric Systems* ”,IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICSâĂŤ-PART C: APPLICATIONS AND REVIEWS, VOL. 35, NO. 3, AUGUST 2005.
13. A.McCabe et.al., ”*Neural Network-based Hand-written Signature Verification*” ,JOURNAL OF COMPUTERS, VOL. 3, NO. 8, AUGUST 2008.