ISSN:0975-9646

Offline Signature Verification Using Surf Feature Extraction and Neural Networks Approach

Priyanka Sharma

CSE Department, Baddi University
Makhumajra Distt : Solan HP

***Abstract*— In this paper we will evaluate the use of SURF features in handwritten signature verification. For each known writer we will take a sample of three genuine signatures and extract their SURF descriptors. In this paper, off-line signature recognition & verification using neural network is proposed, where the signature is captured and presented to the user in an image format. Signatures are verified based on parameters extracted from the signature using various image processing techniques. The Off-line Signature Recognition and Verification is implemented using Matlab.**

***Keywords*— Network, Signature, SURF Extraction, Signature Recognition and Verification.**

I. Introduction

Image registration plays the important role in the image processing application such as remote sensing and computer vision. It's purpose is to overlay two or more images of the same scene which are taken at different times from different viewpoints and by different sensors[1,2].

Image registration method can be divided into two categories: One is based on gray pixel, which is few researches as present. The other is based on characteristics, which match the different images by analyzing interest points. There are some important steps in feature-based image matching method. First, features of image are extracted, second, matching between the features, third, completing the features matching in the different images.

The biometrics have a significant advantage over traditional authentication techniques (namely passwords, PIN numbers, smart cards etc) due to the fact that biometric characteristics of the individual are not easily transferable are unique of every person and cannot be lost, stolen or broken. The choice of one of the biometric solutions depends on several factors which include

1.User acceptance
2.Level of security required
3.Accuracy
4.Cost and implementation time

The method of signature [3,4] verification reviewed in this paper benefits the advantage of being highly accepted by potential customers. The use of the signature has a long history which goes back to the appearance of writing itself. Utilization of the signature as an authentication method has already become a tradition in the western civilization and is respected among the others. The signature is an accepted proof of identity of the person in a transaction taken on his or her behalf. Thus the users are more likely to approve this kind of computerized authentication method.

The objective of signature verification systems is to differentiate between original and forged signature, related to intra personal and inter personal variability. Intra personal variations is distinction among the signatures of the same person and inter personal is the variation between the originals and the forgeries. There will always be slight variations in a human's handwritten signature, the consistency generated by natural motion and practice over time generates a recognizable pattern that makes the handwritten signature suitable for biometric identification. A signature forgery means an attempt to copy someone else's signature and use them against him to steal his identity there can be basically three types of forgeries [5]: Both offline and online systems are used to detect various types of forgeries.

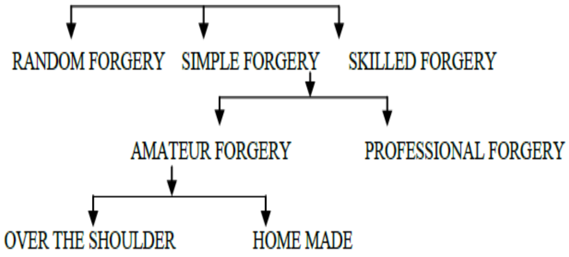

Figure1. Classification of forgeries

The following is the flowchart of the offline signature recognition.

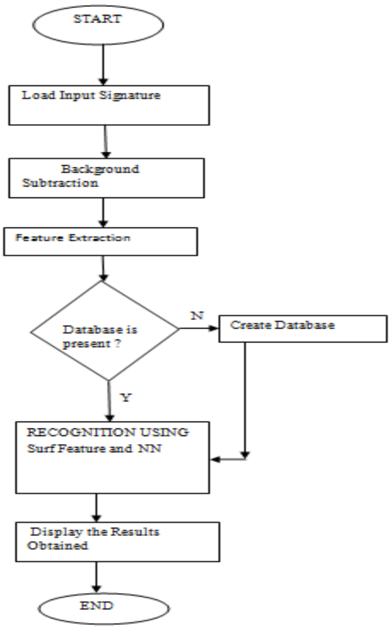

Figure 2. The flowchart of the signature recognition system.

II. Image Preprocessing and Features Extraction

We approach the problem in two steps. Initially, the scanned signature image is preprocessed to be suitable for extracting features. Then, the preprocessed image is used to extract relevant geometric parameters that can distinguish forged signatures from exact ones using the NN[6] approach.

Preprocessing:

The signature is first captured and transformed into a format that can be processed by a computer. Now it's ready for preprocessing. In preprocessing stage, the RGB image of the signature is converted into grayscale and then to binary image. The purpose of this phase is to make signatures ready for feature extraction. The preprocessing stage includes two steps: Color inversion, Filtering and Binarization.

Color Inversion[7,8]: The true color image RGB is converted to the grayscale intensity image by eliminating the hue and saturation information while retaining the luminance.

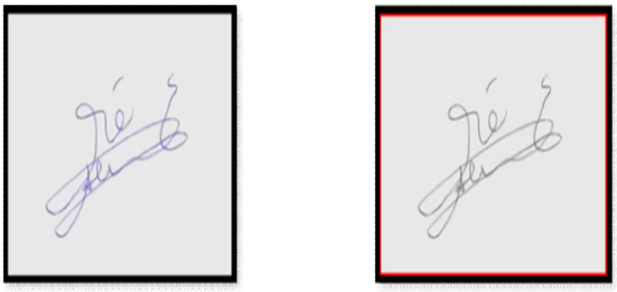

Figure 3. A sample signature to be processed; (b) A Grayscale Intensity Image

A. Types of Signature Verification

Based on the definitions of signature, it can lead to two different approaches of signature verification.

1. *Off-Line or Static Signature Verification Technique*

This[9] approach is based on static characteristics of the signature which are invariant. In this sense signature verification, becomes a typical pattern recognition task knowing that variations in signature pattern are inevitable; the task of signature authentication can be narrowed to drawing the threshold of the range of genuine variation. In the offline signature verification techniques, images of the signatures written on a paper are obtained using a scanner or a camera.

2. *On-line or Dynamic Signature Verification Technique*

This is the second type of signature verification technique. This approach is based on dynamic characteristics of the process of signing. This verification uses signatures that are captured by pressure sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features[10] include the number of order of the strokes, the overall speed of the signature and the pen pressure at each point that make the signature more unique and more difficult to forge. Application areas of Online Signature Verification include protection of small personal devices (e.g. PDA, laptop), authorization of computer users for accessing sensitive data or programs and authentication of individuals for access to physical devices or buildings.

III. Recognition

Neural networks give effective results for solving multiple class classification problems. Chau [11] notes that neural network facilitate gate recognition because of their highly flexible and non linear modeling ability. Neural network has three types of layers: input layer, output layers and hidden layers. Hidden layer does intermediate computation before directing the input to output layer. Back propagation can also be considered as a generalization of delta rule. When back propagation network is cycled, an input pattern is propagated forward to the output units through the intervening input to hidden and hidden to output weights. Neural network have been widely used in image and signal processing.

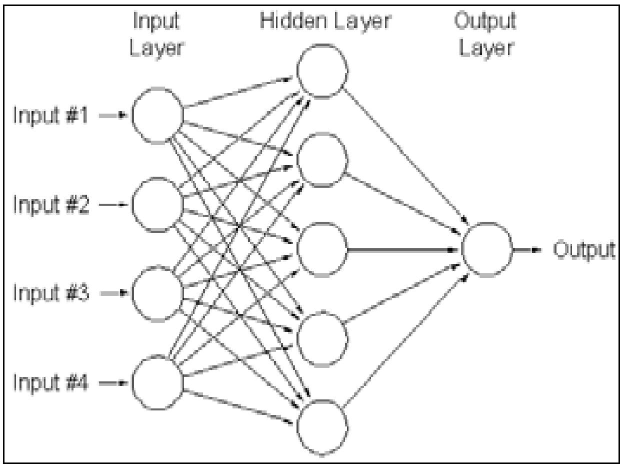

Figure 4. Neural Network

The proposed system [12] using structure features from modified direction feature and other features as surface area, length skew and centroid feature where signature is divided into two halves and for each half a position of the centre of gravity is calculating with reference to the horizontal axis. For classification two approaches are compared the Resilient Backpropagation (RBP) neural network and Radial Basic Function(RBF) using a database of 2106 signatures containing 936 genuine and 1170 forgeries. These two classifiers register 91.21% and 88 % true verification respectively.

The works of Alan McCabe [12] Several Network topologies are tested and their accuracy is compared. The most successful version of the NN based HSV system uses a single MLP with one hidden layer to model each user's signature. It is trained using five genuine signatures and one hundred zero-effort forgeries. Using this approach, a 3:3% OER is reported for the best case.

In [13] signature is captured and presented to the user in an image format. Then Signatures are verified cbn using parameters extracted from the signature based on various image processing techniques. It helps in detecting the exact person and it provides more accuracy of verifying signatures as compared to prior works. For verification of signatures some novel features needs to be extracted. For implementation of above this paper uses Neural Network (NN) for recognition and verification of signatures of individuals.

IV. CONCLUSIONS

In this research work we have proposed offline signature recognition using surf feature extraction and neural network approach which shows far better result than previous work done.

ACKNOWLEDGMENT

Thanks to all my teachers and friends. Special thanks to my parents to support me always.

REFERENCES

[1] G.A. Khuwaja. An adaptive combined classifier system for invariant face recognition. Digital Signal Processing 12, 21–46, DOI:10.1006/dspr.2001.0413, 2002.

[2] D. Zhang, J. Campbell, D. Maltoni, and R. Bolle. Special issue on biometric systems. IEEE Trans. Systems, Man and Cybernetics - C, 35(3):273–275, 2005.

[3] K. Bowyer, V. Govindaraju, and N. Ratha. Introduction to the special issue on recent advances in biometric systems. IEEE Trans. Systems, Man and Cybernetics - B, 37(5): 1091–1095, 2007.

[4] G. A. Khuwaja. Fingerprint identification with LVQ. Proc of the 9th IEEE Int Conf on Neural Information Processing (ICONIP'OZ), Vol. 2, Singapore, Nov. 2002.

[5] J.F. Vargas, M.A. Ferrer, C.M. Travieso, and J. B. Alonso. Offline signature verification based on pseudo-cepstral coefficients. 10th IEEE Int Conf on Document Anal. & Recognition, 2009.

[6] A.I. Al-Shoshan. Handwritten signature verification using image invariants and dynamic features. Proc of the IEEE Int Conf on Computer Graphics, Imaging and Visualization (CGIV'06), 2006.

[7] M. Piekarczyk. Hierarchical random graph model for off-line handwritten signatures recognition. IEEE Int Conf on Complex, Intelligent, Software Intensive Systems, 2010.

[8] S.M.S. Ahmad, A. Shakil, M.A. Faudzi, R.M. Anwar. Analysis of 'goat' within user population of an offline signature biometrics. 10th IEEE Int Conf on Information Science, Signal Processing and their Applications (ISSPA 2010).

[9] J.P. Drouhard, R. Sabourin, and M. Godbout. A neural network approach to off-line signature verification using directional PDF. Pattern Recognition, 29(3), (1996), 415--424.

[10] E.J.R. Justino, F. Bertolozzi, and R. Sabourin. A comparison of SVM and HMM classifiers in the offline signature verification. Pattern Recognition Letters, vol. 26, 1377-1385, 2005.

[11] K. Delac and M. Grgic. A survey of biometric recognition methods. Proc of 46th IEEE Int Symposium Electronics, Croatia, 184-193, June 2004.

[12] B. Kovari, Z. Kertesz, and A. Major. Off-line signature verification based on feature matching. 11th IEEE Int Conf on Intelligent Engineering Systems, Budapest, Hungary, 29 June - 1 July 2007.

[13] A. Kholmatov and B. Yanikoglu. Identity authentication using improved on-line signature verification method. Pattern Recognition Letters, Volume 26, Issue 15, November 2005, pp. 2400-2408.

[14] T.S. Ong, W.H. Khoh, A. Teoh. Dynamic handwritten signature verification based on statistical quantization Mechanism. IEEE Int Conf on Computer Engineering and Technology, 2009.