Signature Recognition &Verification Using ANN

Vaishali M. Deshmukh, Sachin A. Murab

Abstract:- ***The signature of a person is an important biometric attribute of a human being which can be used to authenticate human identity. There are various approaches to signature recognition with a lot of scope of research. 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. This paper presents a proposed method for verifying offline-signatures. A Neural Network will be used for verifying signatures***

Keywords-component; image preprocessing, feature extraction; Neural network training and testing; signature verification and recognition.

I. INTRODUCTION

A signature may be termed a behavioral biometric, as it can modify depending on many essentials such as: frame of mind, exhaustion, etc. The exigent aspects of automated signature recognition and verification have been, for a long time, a true impetus for researchers. Research into signature verification has been energetically pursued for a number of years [1] and is still being explored (especially in the off-line mode) [2]. Signature recognition and verification involves two separate but strongly related tasks: one of them is identification of the signature owner, and the other is the decision about whether the signature is genuine or forged. Also, depending on the need, signature recognition and verification problem is put into two major classes: (i) online signature recognition and verification systems (SRVS) and (ii) offline SRVS[15].Prior approaches describes the novel system for off-line signature verification, in the novel system both static and pseudo dynamic features are extracted as original signal, which is processed by Discrete Wavelet Transform (DWT) for the purpose of enhancing the difference in time domain between a genuine signature and its forgery [4]. Also writer-independent model which reduces the pattern recognition problem to a 2-class problem, hence, makes it possible to build robust signature verification systems even when few signatures per writer are available. Receiver Operating Characteristic (ROC) curves are used to improve the performance of the proposed system [5]. Experiments are carried out using both off-line systems, involving the discrimination of signatures written on a piece of paper, and on-line systems, in which dynamic information of the signing process (such as velocity and acceleration) is also available [6].

Manuscript Received on November, 2012

Vaishali M. Deshmukh, Computer Science & Engineering Dept., Sant Gadge Baba Amaravati University, P.R.M.I.T. & R.Badnera, Amravati, India.

Sachin A. Murab, Information Technology Dept., Sant Gadge Baba Amaravati University, P.R.M.I.T. & R. Badnera, Amravati, India.

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 [7]. Various classifiers, such as Support Vector Machines (SVMs) and Hidden Markov Models (HMMs), have also been successful in off-line signature verification; SVMs providing an overall enhanced outcome than the HMM-based approach [9].

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 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 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 [10].

B. Types of Forgeries

- Random: these signatures are not based on any Knowledge of the original signature
- Simple: these signatures are based on an assumption of how the signature looks like by knowing the name of The signer
- Skilled: an imitation of the original signature, which means that the person knows exactly how the original Signature looks like [3].

II. RELATED WORK

Traditional bank checks, bank credits, credit cards and various legal documents are an integral part of the modern economy. They are one of the primary mediums by which individuals and organizations transfer money and pay bills. Even today all these transactions especially financial require our signatures to be authenticated. The inevitable side-effect of signatures is that they can be exploited for the purpose of feigning a document's authenticity. Hence the need for research in efficient automated solutions for signature recognition and verification has increased in recent years to avoid being vulnerable to fraud [8]. signature verification and recognition using a new approach that depends on a neural network 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 [11]. An off-line signature verification and recognition system based on a combination of features extracted such as global features, mask features and grid features. The system is trained using a database of signatures. For each person, a centroid feature vector is obtained from a set of his/her genuine samples using the features that were extracted. The centroid signature is then used as a template which is used to verify a claimed signature. To obtain a satisfactory measure of similarity between our template signature and the claimed signature, we use the Euclidean distance in the feature space. The results were very promising and a success rate of 84.1% was achieved using a localized threshold [13].

The next approach described Feature extraction is an important process in offline signature verification. In this work, the performance of two feature extraction techniques, the Modified Direction Feature (MDF) and the gradient feature are compared on the basis of similar experimental settings. In addition, the performance of Support Vector Machines (SVMs) and the squared Mahalanobis distance classifier employing the Gradient Feature are also compared and reported. Without using forgeries for training, experimental results indicated that an average error rate as low as 15.03% could be obtained using the gradient feature and SVMs [12].

This approach is based on the boundary of a signature and its projections are described for enhancing the process of automated signature verification. The first global feature is derived from the total 'energy' a writer uses to create their signature. The second feature employs information from the vertical and horizontal projections of a signature, focusing on the proportion of the distance between key strokes in the image, and the height/width of the signature. The combination of these features with the Modified Direction Feature (MDF) and the ratio feature showed promising results for the off-line signature verification problem. When being trained using 12 genuine specimens and 400 random forgeries taken from publicly available database, the Support Vector Machine (SVM) classifier obtained an average error rate (AER) of 17.25%. The false acceptance rate (FAR) for random forgeries was also kept as low as 0.08%[14]. Alan McCabe et al, presents a method for verifying handwritten signatures by using a NN architecture. Various static (e.g., height, slant, etc.) and dynamic (e.g., velocity, pen tip pressure, etc.) Signature features are extracted and used to train the NN. Several Network topologies are tested and their accuracy is compared. The resulting system performs reasonably well with an overall error rate of 3.3% being reported for the best case [16].

III. OBJECTIVES

Objectives are as follows.

1. To develop signature recognition & verification System by using artificial neural network
2. To verify an entered signature with the help of an Average signature, which is obtained from the set of, previously collected signatures
3. To accurately characterize each user's signature, thus offering good verification and recognition performance
4. To reduce the time required for Signature verification and recognition
5. To maintain the Security in various financial domain such as banking, Insurance etc.

IV. PROPOSED METHODOLOGY

To perform verification or identification of a signature, several steps must be performed.

These steps are

A. Image pre-processing
B. Feature extraction
C. Neural network training

A. Image Pre-Processing

Image pre-processing represents a wide range of techniques that exist for the manipulation and modification of images. It is the first step in signature verification and recognition. A successful implementation of this step produces improved results and higher accuracy rates.

B. Feature Extraction

Feature extraction is the second major step in signature recognition and verification. If we are to compare 2 sketches; there should be at least one measurement on which to base this comparison. 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 result.

C. Neural Network Training

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 very helpful 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 to detect the differences is needed to achieve a decision on its authenticity. Neural networks do not follow a set of instructions, provided for them by the author, but they learn as they go case by case.

Signature Recognition &Verification Using ANN

Neural networks are highly reliable when trained using a large amount of data. They are used in applications where security is highly valued.

For signature recognition and verification several steps must be performed. In our proposed work basically we collect the scanned images of signature of different persons, basically we collect the 10 scanned images of individuals' actual signatures and there forged signatures. These images are stored in a database which we are going to use in training & testing of ANN, In our proposed work we have to use an interface with scanner for getting an image and These images are stored in a database. After preprocessing all signatures images from the database, features extraction will be used to extract various features of signature such as stroke, moment invariants, GLCM, color dominant, histogram that can distinguish signatures of different persons. These are used for training and testing of neural network.

The proposed methodology or procedure for signature recognition and verification are as follows:

1. Acquire the Signature images.
2. Image preprocessing.
3. Extract the various features.
4. Use these features to train the system using Backpropagation algorithm
5. Test the Signature image.
6. Take decision as originals or forgeries.

Proposed System Design

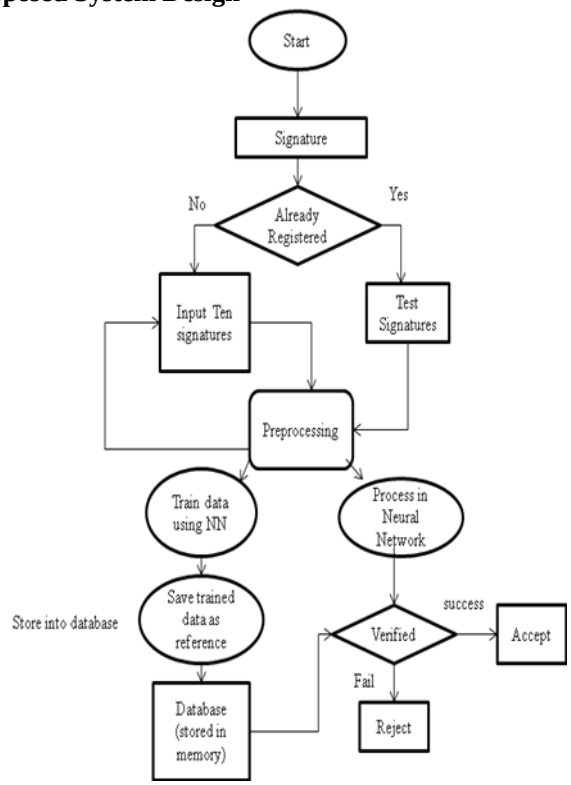

Figure 1. Signature Recognition & Verification

V.CONCLUSION

This paper is focused on Offline signature recognition and verification. Signatures are verified based on parameters extracted from the signature using various image processing techniques. This paper will be completed when the utility of signature verification is shown i.e. it helps in detecting the exact person and it provides more accuracy of verifying signatures for implementation of above, this paper uses Neural Networks for recognition and verification of signatures of individuals.

REFERENCES

1. K. Han, and I.K. Sethi, "Handwritten Signature Retrieval and Identification", Pattern Recognition 17, 1996, pp. 83-90.
2. S. Chen, and S. Srihari, "Use of Exterior Contour and Shape Features in Off-line Signature Verification", 8th International Conference on Document Analysis and Recognition (ICDAR'05), 2005, pp. 1280-1284.
3. Özgündüz,T. Uentürk and M. E. Karslıgil, "Off line signature Verification and recognition by support vector machine", Eusipco 2005, Antalya, Turkey 4 -8 September, 2005, , pp.113-116.
4. Wei Tian, Yizheng Qiao and Zhiqiang Ma, A New Scheme for Off-line Signature Verification Using DWT and Fuzzy Net, IEEE 8th ACISInternational Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007, pp.30-35
5. Luiz S. Oliveira, Edson Justino, and Robert Sabourin, Off-line Signature Verification Using Writer-Independent Approach, Proceedings of International Joint Conference on Neural Networks, Orlando, Florida, USA, August 12-17, *IEEE* 2007.
6. Fernando Alonso-Fernandez, Julian Fierrez, Almudena Gilperez, Javier Galbally, Javier Ortega-Garcia, Robustness of Signature Verification Systems to Imitators With Increasing skills, IEEE 2009,pp. 728-732.
7. Plamondon, "The Handwritten Signature as a Biometric Identifier: Psychophysical Model & System Design" IEE Conference Publications, R.1995, Issue CP408, 23-27.
8. Ali Karouni Bassam Daya, Samia Bahlak, Offline signature Recognition using neural networks approach, Procedia Computer Science 3, 2010, pp.155-161.
9. E.J.R. Justino, F. Bortolozzi, and R. Sabourin. "A comparison of SVM and HMM classifiers in the off-line signature verification",Pattern Recognition Letters 26, 2005, pp. 1377- 1385.
10. Ms. Vibha Pandey Ms. Sanjivani Shantaiya. "Signature Verification Using Morphological Features Based on Artificial Neural Network", 2012 pp. 288-292
11. Suhail M. Odeh, Manal Khalil ,Off-line signature verification and recognition: Neural Network Approach,IEEE 2011,pp.34- 38
12. Vu Nguyen, Yumiko Kawazoey, Tetsushi Wakabayashiy, Umapada Palz, and Michael Blumenstein, Performance Analysis of the Gradient Feature and the Modified Direction Feature for Off-line Signature Verification , the IEEE 12th International Conference on Frontiers in Handwriting Recognition, 2010,pp.303-307.
13. Bradley Schafer, Serestina Viriri, An Off-Line Signature Verification System, IEEE International Conference on Signal and Image Processing Applications, 2009, pp. 95-100
14. Michael Blumenstein, Graham Leedham, Vu Nguyen, Global Features for the Off-Line Signature Verification Problem, IEEE 10th International Conference on Document Analysis and Recognition, 2009,pp.1300-1304.
15. Cemil OZ, Fikret Ercal, Zafer Demir Signature Recognition and Verification with ANN Sakarya University Computer Eng. Department Sakarya,Turkey,UMR Computer Science Department Rolla,MO65401
16. Alan McCabe, Jarrod Trevathan and Wayne Read, school of mathematics, physics and Information Technology, James cook University, Australia. Neural Network-based handwritten signature verification, Journal of computers, vol.3, No. 8 August 2008, pp. 9-22.