



Artificial Intelligence Based Bank Cheque Signature Verification System

Shemaz Parven¹, Rizeen Shaikh², Shreya Karkada³, Sneha S Poojary⁴, Vinaya Kumar⁵
BE Student^{1, 2, 3, 4}, Assistant Professor⁵
Department Electronics and communication
SMVITM, India

Abstract:

An integral part of security is authentication as based on a person's identity he is authorized to certain privileges. There are many means for authentication, and signature is one among them. Signature verification technique used by the banks intelligence agencies and high profile institutions to validate the identity of individual. An important advantage of the signature verification compared with others is its long tradition in many commercial fields such as e-business, which includes online banking transaction, electronic payments, access control and so on. To date signatures verification is done manually in banks where a person manually verifies the signature on the cheque with specimen signature. But this method is not accurate as naked eye cannot detect forgeries. Our proposed system deals with computerized signature verification in banking application. Verification of signatures can be done on-line or off-line depending upon the application. 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 techniques. The signature features, to be tested, are fed to the trained neural network to find whether the signature is genuine or a forged one.

Index Terms: Image preprocessing, Feature extraction, Neural network training and testing, Signature verification and recognition

I. INTRODUCTION

A signature is a handwritten depiction of someone's name, nick name or other mark that a person writes on a document as a proof of identity and intent. Signature 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 and is still being explored (especially in the off-line mode). 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. 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. 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 is used to improve the performance of the proposed system. 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. The types of forgeries encountered are: 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. Based on the definitions of signature, it can lead to two different approaches of signature verification: A) 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. B) 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.

II. LITERATURE SURVEY

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[6]. 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 [2]. 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 70 to 80% was achieved using a localized threshold [4]. 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 [8].

III. EXISTING SYSTEM

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. 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.

IV. PROPOSED SYSTEM

Signature verification is primarily a pattern recognition problem that accepts query signature as input. Then the query signature is compared against signature set of pre-existing trained dataset of a particular individual for verification of genuine of an individual. The proposed architecture for signature verification constitute four major phases, i.e. acquiring signature, pre-processing of acquired signature, extracting features from pre-processed signature and matching of extracted features to prove genuine. For matching purpose CNN algorithm is used in proposed experimentation.

V. METHODOLOGY

A. Image pre-processing

The techniques used for the modification of images represent image pre-processing. The aim of pre-processing is an improvement of the image data that removes unwanted distortions or enhances some features important for further processing. In this paper we crop the image of the signature

Implementation of this step obtains enhanced output and higher accuracy rates.

B. Feature Extraction

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. Broadly speaking, the feature extraction techniques can be classified as Static or Pseudodynamic, where pseudo- dynamic features attempt to recover dynamic information from the signature execution process (such as speed, pressure, etc.). Another broad categorization of the feature extraction methods is between Global and Local features. Global features describe the signature images as a whole -features such as height, width of the signature, or in general feature extractors that are applied to the entire signature image. In contrast, local features describe parts of the images, either by segmenting the image or most commonly by the dividing the image in a grid (of Cartesian or polar coordinates), and applying feature extractors in each part of the image. 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.

D. 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 their 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 pre-processing 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.

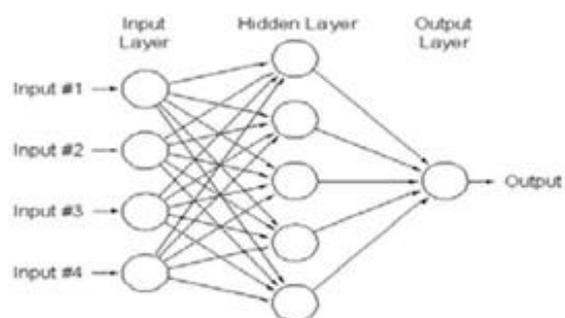


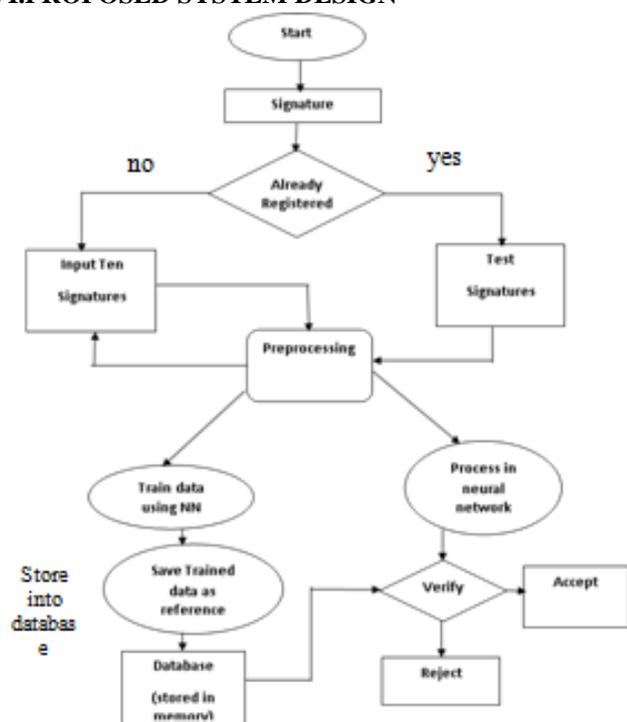
Figure.1. Neural Network diagram

Here these are ANN mathematical models which mimicking biological neural networks where they consist of a group of connected which representing the neurons of the brain. It represented by a diagram of nodes in various layers with weighted connections between nodes in different layers. Where RBF network is an ANN that uses radial basis functions as activation functions where RBF networks typically have three layers that are input layer, hidden layer with a non-linear RBF activation function and an output layer with linear activation functions and the most popular form is given below:

$$\hat{y}(x) = \sum_{i=1}^m \omega_i h_i(x)$$

In our proposed paper we have implemented Convolutional Neural Networks (CNNs) algorithm. It has been proved successful in recent years at a large number of image processing-based machine learning tasks. Many other methods of performing such tasks revolve around a process of feature extraction, in which hand-chosen features extracted from an image are fed into a classifier to arrive at a classification decision. Such processes are only as strong as the chosen features, which often take large amounts of care and effort to construct. By contrast, in a CNN, the features fed into the final linear classifier are all learned from the dataset. A CNN consists of a number of layers, starting at the raw image pixels, which each perform a simple computation and feed the result to the next layer, with the final result being fed to a linear classifier. The layers' computations are based on a number of parameters which are learned through the process of backpropagation, in which for each parameter, the gradient of the classification loss with respect to that parameter is computed and the parameter is updated with the goal of minimizing the loss function.

VI. PROPOSED SYSTEM DESIGN



EXPERIMENTAL RESULT

The signature is acquired, pre-processed and features are extracted and are fed to the Neural Network for classification of signatures into genuine or forged. Thus we have accomplished the task of verifying the signature as shown below in fig2. If the signature is genuine, Valid status is obtained else rejected.

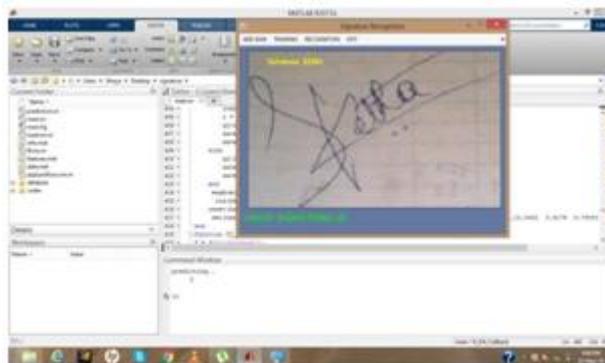


Figure.2. Valid signature

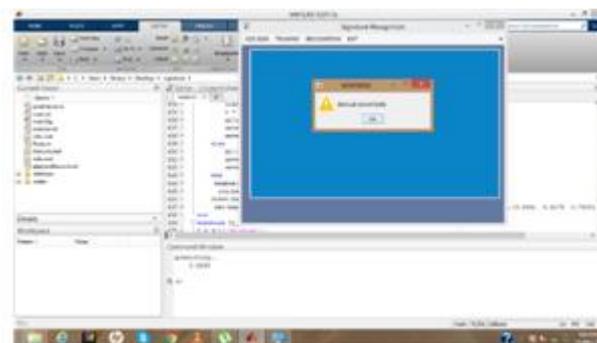


Figure.3. Invalid signature

V. CONCLUSION

This proposed system is focused on Bank Cheque Signature Verification System using artificial neural network. Signatures are verified based on parameters extracted from the signature using various image processing techniques. This proposed system will gives utility of signature verification is shown. 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.

VI. REFERENCES

- [1]. Minal Tomar and Pratibha Singh, "A Directional Feature with Energy based Offline Signature Verification Network", International Journal on Soft Computing (IJSC), Vol.2, No.1, February 2011.
- [2]. Ashwini Pansare, "Handwritten Signature Verification using Neural Network" International Journal of Applied Information Systems (IJ AIS) Volume 1- No.2, January 2012
- [3]. Poornima G Patil, Ravindra S Hegadi, "Offline Handwritten Signatures Classification Using Wavelets and Support Vector Machines", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 4, July 2013.
- [4]. M. V. Kanawade & S. S. Katariya "Offline signature verification and recognition", International Journal of Electronics, Communication and Instrumentation Engg Research and Development Aug 2013.
- [5]. Rishabh Jain, Akanksha Verma, Abhishek Kumar Singh, Adhbuti Hajela "A Review Paper on Offline Signature Verification Using Back Propagation " International Journal of

[6]. R. M. Samant¹, Mahendra Shilwant², Bhojraj Sarsambi³, Mahesh Shelke “Signature Verification System“, International Journal of Advanced Research in Computer and Communication Engg April 2017.

[7]. S. Dhandapani,” Neural Network based Signature Verification model for Bank Cheques with Three Specimen Signatures “, International Journal of Computer Science Engg and Information Technology Research Aug 2017.

[8]. K. Harika & T. Chandra Sekhara Reddy,” A Tool for Robust Offline Signature verification “, International Journal of Advanced Research in Computer and Communication Engg Sept 2017.

[9]. Gabe Alvarez, Blue sheffer, Morgan Bryant, “offline signature verification with Convolutional Neural networks”, April 2017