ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Handwritten Signature Recognition, Verification and Dynamic Updation using Neural Network

Meetu Sangwan[1], Mr. Daulat Sihag[2]

Student, CSE, JCDM College of Engineering, Sirsa, India [1]

Asst Professor, CSE, JCDM College of Engineering, Sirsa, India [2]

Abstract: The hand written signature is regarded as the primary means of identifying the signer of a written document based on the implicit assumption that a person's normal signature changes slowly and is very difficult to erase, alter or forge without detection. The handwritten signature is one of the ways to authorize transactions and authenticate the human identity compared with other electronic identification methods such as fingerprints scanning, face recognition and retinal vascular pattern screening. It is easier for people to migrate from using the popular pen-and-paper signature to one where the handwritten signature is captured and verified electronically. The signature of a person is an important biometric attribute of a human being and is used for authorization purpose. Various approaches are possible for signature recognition with a lot of scope of research. Here, we deal with an off-line signature recognition technique. Signatures are composed of special characters and flourishes and therefore most of the time they can be unreadable. Also intrapersonal variations and interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together. Signature recognition is the process of verifying the writer's identity by checking the signature against samples kept in the database. The result of this process is usually implementing the resizing, cropping, etc for matching and dynamic updating based on the features parameters. Signature recognition is used most often to describe the ability of a computer to translate human writing into text.

Keywords: OCR (Optical Character Recognition), FRR (False Rejection Rate).

I. INTRODUCTION

Nowadays, person identification (recognition) and verification is very important in security and resource access control. Signature is a special case of handwriting which includes special characters and flourishes. Many signatures can be unreadable. They are a kind of artistic handwriting objects. However, a signature can be handled as an image, and hence, it can be recognized using computer vision and artificial neural network techniques. Signatures are most legal and common means for individual's identity verification. People are familiar with the use of signatures in their daily life. Automatic signature recognition has many applications including credit card validation, security systems, cheques, contracts, etc.

There are two types of systems in this field, signature verification systems and signature identification systems.

- A signature verification system just decides whether a given signature belongs to a claimed writer or not.
- A signature identification system, on the other hand, has to decide a given signature belongs to which one of a certain number of writers

In signature verification systems, two common classes of forgeries are considered: casual and skilled. A casual forgery is produced by only knowing the name of the writer, and without access to a sample of the genuine signature. When forger uses his own signature or genuine signature of another writer as a casual forgery, it is called a substitution forgery. So, stylistic differences are common in casual forgeries. In skilled forgeries, the forger has access to a sample of genuine signature and knows the signature very well. Since skilled forgeries are very similar to genuine signatures, some appropriate features for detection of casual forgeries are ineffective in detection of skilled forgeries. The precision of signature verification systems can be expressed by two types of error: the percentage of genuine signatures rejected as forgery which is called False Rejection Rate (FRR) and the percentage of forgery signatures accepted as genuine which is called False Acceptance Rate (FAR).

The signature verification is performed in two steps, feature extraction and classification.

- During the feature extraction phase, personal features of each training signature are extracted and trained to the classifier.
- In the classification phase, personal features extracted from a given signature are fed into classifier in order to judge its validity.

Local features describe only a small part of signature and extract more detailed information from image. These features include unballistic motion and tremor information in stroke segments, stroke elements, local shape descriptors, and pressure and slant features. The use of handwritten signatures for authenticating documents or personal identification dates back to to ancient times and has since been increasingly used for numerous financial and business transactions. The use of handwritten signature for authentication plays an important role in the everyday life of society and is applied in almost every sphere of human activity due to its relative ease of use, especially offline handwritten signatures . According to,

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

most financial institutions give preference to the use of the offline handwritten signature despite the fact that the online signatures have proved to be more reliable but however require more complex processing and high-tech gadgets which the offline signatures do not require. Offline signatures can be signed on a piece of paper, which as at today plays a very vital role in documentation despite the ongoing revolution. Online signatures on the other hand, require special hardware such as digitizers and pressure tablets necessary to acquire the dynamic information such as pressure and speed of the signer, besides the static image of the signature. The problem however is that the offline signature can be easily imitated or forged which could lead to false representation or fraud.

Recognition and verification

A clear distinction should be made between systems developed for signature recognition and those intended for signature verification. A recognition system receives as input a signature of unknown origin. The system then has to determine to which one of its finite number of enrolled writer classes the input signature is a closest match. A -class recognition system therefore needs to compare its input to samples representative of each of its writer classes before delivering a probabilistic output as to the origin of the input signature. A verification system, on the other hand, receives as input a signature of unknown origin, but also a claim of ownership. The system then has to either confirm or reject the validity of this claim. In order to achieve this, the system compares the signature to samples of the claimed owner, before delivering an output as to its certainty concerning the validity of the claim of ownership. Verification systems may therefore be viewed as a specific subclass of recognition systems, namely bi-class recognition systems that classify input as belonging to either the positive (genuine) or negative (forgery) class. As a result, there exists certain terminology that is used to describe either system indiscriminately. During the course of this study, for example, there are references to classifiers and classes, whilst it is implied that reference is being made to verifiers and genuine/forged signatures, respectively.

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.

Handwritten signatures

Handwritten signatures, henceforth referred to only as signatures, have been considered valid proof of identity and consent for centuries. The signing of the US Declaration of Independence, presented as Figure 1.6, is epitomic of this social credence. Even in our present day and age, dominated by advanced technological systems and protocols, signatures remain the preferred method for identity verification, as they are both nonintrusive and easily collectable. An individual's signature is usually composed of stroke sequences much unlike those used in ordinary handwriting and, in addition, tends to evolve towards a single, unique design. This is not only as a result of repetition3, but also the innate desire of each person to create a unique signature. Signatures are therefore able to reflect a writer's subtle idiosyncrasies to a much greater extent than ordinary handwriting.

1.1 Handwritten Signature Recognition

Handwritten signature verification has been extensively studied & implemented. Its many applications include banking, credit card validation, security systems etc. In general, handwritten signature verification can be categorized into two kinds – on–line verification and off–line verification. On–line verification requires a stylus and an electronic tablet connected to a computer to grab dynamic signature information. Off–line verification, on the other hand, deals with signature information which is in a static format. [2]

In On–line approach we can acquire more information about the signature which includes the dynamic properties of signature. We can extract information about the writing speed, pressure points, strokes, acceleration as well as the static characteristics of signatures.

This leads to better accuracy because the dynamic characteristics are very difficult to imitate, but the system requires user co-operation and complex hardware. Digitizer tablets or pressure sensitive pads are used to scan signature dynamically, In off–line signature recognition we are having the signature template coming from an imaging device, hence we have only static characteristic of the signatures. The person need not be present at the time of verification. Hence off-line signature verification is convenient in various situations like document verification, banking transactions etc. As we have a limited set of features for verification purpose, off-line signature recognition systems need to be designed very carefully to achieve the desired accuracy.

Figure 1 Pre-processing of a signature (Image)

Feature Extraction

We are using various feature extraction algorithms. The feature set includes the conventional global features of signature as well as new features. The new features that are proposed include Walsh coefficient of pixel distribution, codeword Histogram based on clustering technique (Vector Quantization), spatial moments of codeword, Grid & Texture features, and Successive Geometric centres of depth 2.

Enrollment & Training

The extracted features are stored in to database. The human signature is dependent on varying factors, the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

signature characteristics change with the psychological or mental condition of a person, physical and practical condition like tip of the pen used for signature, signatures taken at different times, aging etc. We have to consider a high degree of intra-class variation because two signatures from a same person are never same. Our system should consider this variation and at the same time the system should possess high degree of accuracy to detect forged signatures.

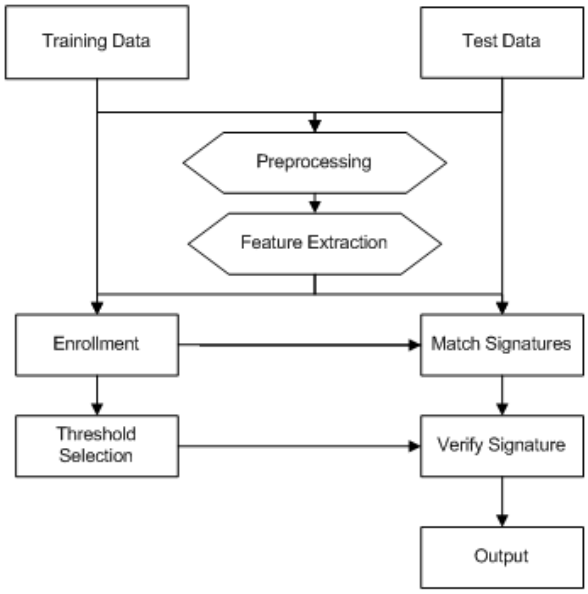

Figure 2 Simplified workflow for a typical Signature recognition

II. LITERATURE REVIEW

Cemil OZ present an off-line signature recognition and verification system which is based on moment invariant method and ANN. Two separate neural networks are designed; one for signature recognition, and another for verification (i.e. for detecting forgery). Both networks use a four-step process. First step is to separate the signature from its background. Second step performs normalization and digitization of the original signature. Moment invariant vectors are obtained in the third step. And the last step implements signature recognition and verification. [1]

ANWAR YAHY EBRAHIM, Handwriting is a skill that is highly personal to individuals and consists of graphical marks on the surface in relation to a particular language. Signatures of the same person can vary with time and state of mind. Several studies have come up with several methods on how to detect forgeries in signatures given to the security implication of signatures to daily business and personal transactions. This paper illustrates the proposed methodology for an offline handwritten signature identification and verification system which extracts certain dynamic features derived from velocity and acceleration of the pen together with other global parameters like total time taken and number of pen-ups in order to distinguish between forged signatures and genuine signatures signed under duress. Adaptive Window Positioning technique was employed for feature extraction, which focuses on not just the meaning of the handwritten signature but also on the individuality of the writer by dividing the handwritten signatures into 13 small windows of size nxn (13x13) such that it is large enough to contain ample information about the style of the author and small enough to ensure a good identification performance. Then, a signer specific codebook approach was used to generate a separate codebook of patterns for each individual signer such that the number of classes in each codebook varies as a function of the writing sample (signer), and a 3-layered Backward Propagation Artificial Neural Network (BPANN) method was used to produce a maximal matching and preserve the efficiency of the network. The proposed method was validated using a trained GPDS data set of 2400 original signatures of 100 different signers and comparing the results with those of two different known techniques of offline handwritten signature verification systems. The findings indicate that the proposed technique had the lowest ERR value of 7.23, indicating a more improved performance when compared against the two known techniques respectively thus proving to be a more efficient and superior method for offline handwritten signature identification and verification. [2]

Vahid Kiani propose a new method for signature verification using local Radon Transform. The proposed method uses Radon Transform locally as feature extractor and Support Vector Machine (SVM) as classifier. The main idea of their method is using Radon Transform locally for line segments detection and feature extraction, against using it globally. The advantages of the proposed method are robustness to noise, size invariance and shift invariance. Having used a dataset of 600 signatures from 20 Persian writers, and another dataset of 924 signatures from 22 English writers, our system achieves good results. The experimental results of our method are compared with two other methods. This comparison shows that our method has good performance for signature identification and verification in different cultures.

III. OBJECTIVES

The objective is to design, the handwritten signature recognition problem has been approached in various ways. In general, handwritten recognition is a difficult task because of the variation of writing styles even with the same writer; therefore, great attentions must be taken in designing a recognition system. The current research presents satisfactory results in the recognition of handwritten signatures using Back propagation Neural Network.

IV. PROPOSED METHODOLOGY

Signature verification system which verifies the authenticity of given signature of a person.
The design of a system is divided into two stages:
1. Training stage
2. Testing stage

DOI 10.17148/IJARCCE.2015.4846

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

A training stage consist of four major steps 1) Retrieval of a signature image from a database 2) Image pre-processing 3) Feature extraction 4) Neural network training.

A testing stage consists of five major steps 1) Retrieval of a signature to be tested from a database 2) Image pre-processing 3) Feature extraction 4) Application of extracted features to a trained neural network 5) Checking output generated from a neural network.

Fig. 1 shows one of the original signature image taken from a database and all the subsequent figures show the resultant signature image obtained after performing the steps mentioned in an algorithm. performing the steps mentioned in an algorithm.

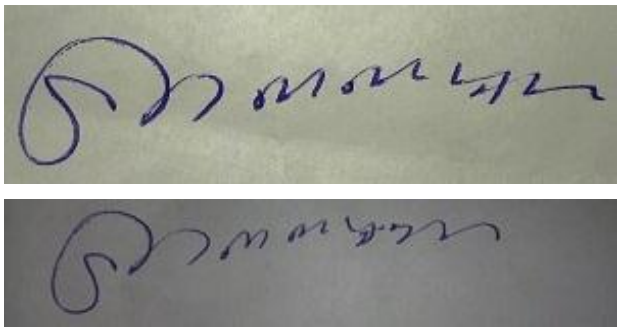

Figure 3 Signature Image (Images)

V. CONCLUSION AND FUTURE WORK

In this work there is a challenge of creating a system with the ability to recognize hand written signature and verify its authenticity. This poses a problem because we are trying to get the computer to solve a problem with a method of solution that goes outside the convention of writing an algorithmic process.
The challenge involves making the computer solve the problem using a series of new steps. After a lengthy research, the only feasible solution required is using the concept of the Neurons in human brain, which is familiar with medical practitioners. Back Propagation Artificial Neural Network: There are several algorithms that can be used to create an artificial neural network, but the Back propagation was chosen because it is probably the easiest to implement, while preserving efficiency of the network. Backward Propagation Artificial Neural Network (ANN) use more than one input layers (usually 3).

REFERENCES

[1] Cemil OZ, Fikret Ercal, Zafer Demir" Signature Recognition and Verification with ANN".
[2] V A Bharadi, H B Kekre" Off-Line Signature Recognition Systems", International Journal of Computer Applications, 2010
[3] ANWAR YAHY EBRAHIM, GHAZALI SULONG" OFFLINE HANDWRITTEN SIGNATURE VERIFICATION USING BACK PROPAGATION ARTIFICIAL NEURAL NETWORK MATCHING TECHNIQUE ",Journal of Theoretical and Applied Information Technology, 2014
[4] Vahid Kiani, Reza Pourreza & Hamid Reza Pourreza" Offline Signature Verification Using Local Radon Transform and Support Vector Machines", International Journal of Image Processing (IJIP)
[5] Dr. S.A Daramola" Efficient on-line Signature Verification System ", International Journal of Engineering & Technology (I J E N S) , 2010
[6] Muhammad Reza Pourshahabi, Mohamad Hoseyn Sigari, Hamid Reza Pourreza" Offline Handwritten Signature Identification and Verification Using Contourlet Transform", International Conference of Soft Computing and Pattern Recognition, 2009
[7] Stephen Krawczyk" USER AUTHENTICATION USING ON-LINE SIGNATURE AND SPEECH", 2005
[8] Vitthal K. Bhosale, Dr. Anil R. Karwankar" Automatic Static Signature Verification Systems: A Review", International Journal Of Computational Engineering Research ,2013
[9] Rapanjot Kaur, Gagangeet Singh Aujla" Review on: Enhanced Offline Signature Recognition Using Neural Network and SVM", International Journal of Computer Science and Information Technologies, 2014
[10] Jacques Philip Swanepoel" Off-line Signature Verification using Classifier Ensembles and Flexible Grid Features", 2009