Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2015, 2(4): 46-50

Review Article ISSN: 2394 - 658X

Static Signature Verification and Recognition using Neural Network Approach-A Survey

Komal Pawar and Tanuja Dhope

Department of Electronics and Telecommunication Engineering, GHRECEM, Pune, Maharashtra, India
pwrkomal2@gmail.com

ABSTRACT

A number of biometric techniques have been used for personal identification such as face recognition, fingerprint recognition, voice recognition and signature recognition. However signature verification is most widely used. Signature being the most prominent handwritten proof of identity is used for authentication of documents in the fields of financial, commercial and legal transactions which requires high level of secured authentication. This paper discusses signature verification and recognition using neural network approach. The method uses scanned signature fed to computer where its image quality is enhanced and compared, finally verifies the authenticity using neural network training. The system involves several stages: image preprocessing, feature extraction and neural network training.

Key words: Biometrics, image processing, feature extraction, neural network, signature verification and recognition

INTRODUCTION

In recent years biometrics has emerged as important aspect in personal authentication and identification. A hand written signature is a biometric attribute of a human being which is a primary means of personal identification. There are others methods of identification such as face recognition, iris recognition and fingerprint recognition. Each of these approaches has its importance in respective fields. Signature verification may face challenges as its verification depends on behavioural and physical characteristics such as mood, fatigue, ageing etc.

Manual verification of signature requires analysis by human therefore there is a need for automated signature verification. The automated signature system will not only improve signature authentication process but will also provide secure means for authorization of legal documents. A system has to be developed in such a way that it should be able to detect forgeries. A system should neither be sensitive nor coarse. The signature verification and recognition can be done using two methods: static and dynamic. The static signature verification uses optical scanner which acquires handwritten signature written onto the paper. The static signature verification is also known as Off-Line. The dynamic signature verification uses signature acquired onto handheld devices to extract information about the signature using dynamic characteristics. The dynamic signature verification is also known as On-Line.

Online/dynamic signature verification obtains dynamic characteristics of the signature using handheld device and a stylus. The dynamic characteristics are then obtained according to x co-ordinate, y co-ordinate, location, velocity, pen pressure etc. Various approaches are used in online signature verification such as: Dynamic time wrapping
Offline/static signature verification known as static is used to obtain static characteristics. In this process signature is taken on piece of paper and scanned using digital scanner. The digital scanner converts the signature into image and feeds to computer for further processing. In offline systems, a 2-D image is developed which has complexity due to absence of stable dynamic characteristics, illness, and emotional state of a person. These factors cause large interpersonal variation. Offline system uses classifiers for verification purpose include: Neural network, template matching. There are many method of offline signature recognition as: surf features, NN-Fuzzy logic, Support Vector Machine, Linear Discriminate analysis, multi-linear analysis.

SIGNATURE VERIFICATION AND RECOGNITION

The objective of signature verification system is to discriminate between two classes: the original and the forged. The signature forgery is the act of falsely replicating the signature of another person. Signature Forgery can be classified into following types -

- Random: original signature is unknown.
- Simple: assumptions are made by knowing name of signer.
- Skilled: an imitation of original signal.

The skilled signatures are most difficult to detect as they can be similar to original signature with less error rate. However the skilled signature requires dynamic features for its detection therefore simple and random forgery can be detected using offline method.

The steps involved in signature verification and recognition are:

- Image acquisition
- Image pre-processing
- Feature extraction
- Neural network training
- Verification

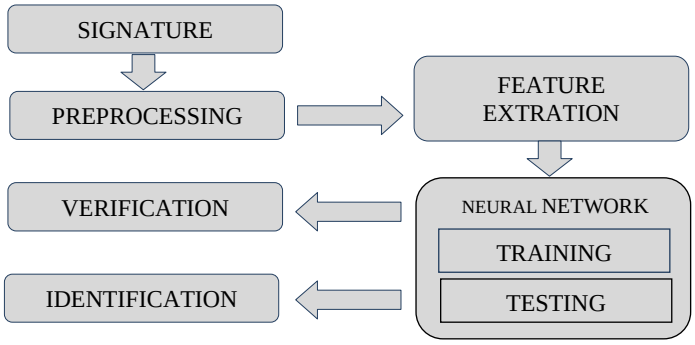


Fig.1 Steps for signature verification and recognition

Image Acquisition

In this phase signature from the user is acquired using digital scanner. The digital scanner scans handwritten signature and converts it to digital image. The acquired signature is stored in database for pre-processing.

Image Pre-Processing

Image pre-processing involves series of steps used for manipulation and interpretation of the image. It improves quality of image and makes it suitable for feature extraction. Several steps in pre-processing include: binarization, removal of noise, thinning and signature normalization.

- Binarization: a colour image is converted into black and white image.
- Removal of noise: filtering function used for noise reduction.
- Thinning: makes extracted features invariant to image characteristics. It is similar to segmentation.
- Signature normalization: standard signature size for all signatures is obtained.

Feature Extraction

It is a process through which vital information and details of image are captured for interpretation. Feature extraction is used to generate features that can be used for comparison. In this system, three groups of feature are used. Grid features: concerned with overall appearance of signature. Local features: describes properties of signature image in specific parts. Global features: describes entire signature features such as aspect ratio, height, weight.

- *Eccentricity*: It is defined as central point in an object. The central point is acquired by applying the ratio of major axis to minor axis of an image.
- *Skewness*: Skewness a measure of symmetry. Skewness can be defined according to univariate data $Y_1, Y_2 \ldots Y_N$

$$Skewness = \frac{\sum_{i=1}^{N}(Y-Y^{-1})s^3}{(N-1)s^3} \quad (1)$$

- *Kurtosis*: Kurtosis means of whether the data are peaked or flattened, relative to normal distribution. Kurtosis measurement highlights the peaks in each segment of signature.

$$\text{Kurtosis} = \frac{\sum_{i=1}^{N}(Y-Y^{-1})s^4}{(N-1)s^4} \quad (2)$$

- *Orientation*: Orientation defines the direction of the signature lines.
- *Image Area*: Total number of black pixels in test image.
- *Aspect ratio*: It is the ratio of width to height component of an image

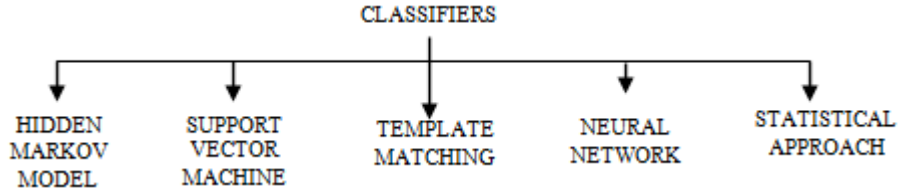
$$\text{Aspect ratio} = \frac{\text{width of signature}}{\text{height of signature}} \quad (3)$$

- *Signature width*: maximum of exact no of black pixels present in each horizontal scan line.
- *Signature height*: maximum of exact no of black pixels present in each vertical scan line.

- *Tri surface feature*: signature is divided into three equal parts and area for each part is calculated and then used to calculate normalized area of each part.
- *Six fold surface feature*: divide the signature into three equal parts and find bounding box for each part. Then calculate centre of mass for each part. Draw horizontal line passing through centre of mass of each part and calculate area of signature above and below centre of mass within bounding box. This provides six features.

CLASSIFICATION

The approach used for signature verification depends on number of factors such as features extracted, training method and models used. These models are also called as classifiers. The various approaches used are:



Hidden Markov Model Approach

Markov model can be defined as mathematical model used to study stochastic processes. Stochastic processes produce random outcomes as per associated possibilities. A hidden Markov model presents only sequence of outputs or emissions, but hides the sequence of the sequence of the states the model underwent to produce the emission. Hidden Markov Model (HMM) is a probabilistic pattern matching technique that has ability to absorb both the variability and the similarity between signature samples. Hidden Markov Models (HMM) represent a signature as a sequence of states. In each state an observation vector can be generated, according to the associated probability distribution. Transitions among the states are governed by a set of probabilities called transition probabilities. The probabilities, or parameters, of an HMM are trained using observation vector extracted from a representative sample of signature data. Recognition of an unknown signature is based on the probability that a signature was generated by the HMM. A well-chosen set of feature vectors for HMM could lead to design of an efficient signature verification system. Justino et al. [4] proposed basic and robust system for offline verification using simple features. The simple and random forgery error rates have shown to be low and close to each other. An FFR of 2.83% and an FAR of 1.44%, 2.50 % and 22.67% are reported for random, causal, and skilled forgeries, respectively.

Support Vector Machine

The support vector machine is a state of art classification introduced by Guyon, Boser, and Vapnik. SVM algorithm is based on statistical learning theory. It is a kernal based technique used in machine learning algorithms for classification or regression. Support vector machine is based on concept of decision planes that define decision boundaries. A decision plane separates set of objects having different class memberships. The system in [5] uses global, directional and grid features and SVM for classification and verification. The database of 1320 signatures is collected from 70 writers. 40 writers are used for training with each 8 signature. For initial testing, the approach uses 8 original signature and 8 forgeries to achieve FFR 2% and FAR 11%.

Template Matching Approach

A process of pattern comparison, is often called “Template matching”. Fang et. al [6] proposed two method for detection of skilled forgeries using template matching. One method is related to optimizing matching of one dimensional projection profiles of signature patterns and other is based on elastic matching of strokes in 2-Dimensional signature patterns. Given a test signature to be verified, positional variations are compared with statistics of straining set and a decision based on distance measure is made. Both binary and grey level signature images are tested. Verification performance is affected by variation of signature stroke width and registered signature selected from a set of reference sample in offline signature verification using a pattern matching.

Neural Network

Neural networks are accurate and efficient means for pattern recognition. Artificial neural network simulated using software provides soft-computational tools for application in a range of areas from financial to pattern recognition. Neural network are designed to realize specific computational tasks/problem. ANN’s use neuron for information processing which form basis for designing neural network. The neural network is trained with the known samples of data which is digital in nature. Then the neural network is ready to recognize a similar pattern when presented to the network. The network learns given data while trying to minimize error between the training set data and its own output. The learning is accomplished using back propagation (BP) algorithm. Three basic elements of neuron model as follows: Interconnection Weights, Summing function and Transfer or activation function. Neural Network can be classified into two main categories: Feed-Forward (Non-recurrent) and Feedback (Recurrent). In feed forward network there are no feedback loops whereas in recurrent network there are feedback loops. Feed forward networks

are used to extract important properties of input data and map input data into representation domain. Feedback network is tasked to learn or process temporal features of input data and their internal state evolves with time. Depending on architecture feed forward network is further classified into Multilayer Perceptron's (MLPs), Counter-propagation networks and Radial basis function network. The works of Alan McCabe [7] 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.

Neural Network Architecture

The neuron model shows a number of inputs x_i multiplied by connecting weights which are summed before applying it to a mapper called the activation function which generates response of neuron. Weights are associated with the inputs. The basic architecture consists of three types of neuron layers.

Input layer: it consists of set of sensory units that receive inputs from external environment. *Output layer*: the output layer consists of neurons that communicate the output of system to the user. *Hidden layer*: these are usually hidden between input and output layers.

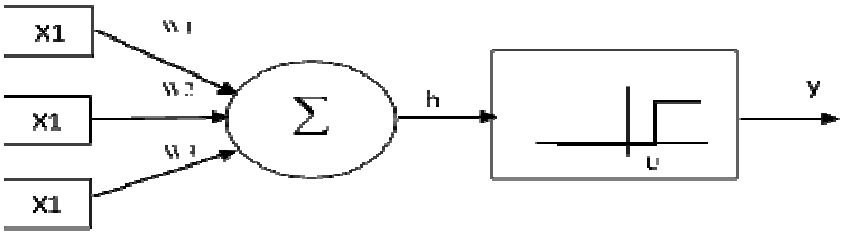


Fig.2 Neural network model

Mathematically it is given by $y = \theta\left(\sum_{j=1}^{n} \text{wixi} - \mu\right)$ (4)

Statistical Approach

Statistical approach is used to find relation and variation between 2 or more data that can easily be determined. Statistical models summarize different aspects of signature shape and dynamics of signature production. It extracts global features like image-gradient, statistical features are derived from distribution of pixels of a signature. Hidden Markov Model, Bayesian are some statistical approach commonly used in pattern recognition. This approach can be used to detect causal as well as skilled forgeries from the genuine ones.

Verification

In the verification stage features are extracted from the specimen signature and compared with the signature stored in database. A certain amount of deviation is allowed between two signatures. While evaluating test signature, its features are compared with corresponding templates. After feature extraction it is fed to trained neural network which will classify the signature genuine or forged.

PERFORMANCE PARAMETERS

There are two types of parameters depending on which we can calculate the performance of the system: false rejection rate (FAR), false acceptance rate (FAR). These two are inversely related. The false rejection rate, false acceptance rate and average rate are used for performance measures.

False Rejection Rate (FRR): It is the ratio of number of genuine signatures rejected to total number of genuine signatures submitted [10].

False Acceptance Rate (FAR): It is the ratio of number of forged signatures accepted to the total number of forged signatures submitted [10].

Average Error Rate (AER): It is the average of FAR and FRR [10].

CONCLUSION

This paper presents the brief survey on offline signature verification and recognition. Various classifiers can be used to train the system. The method uses features extracted from pre-processed signatures images. The extracted features are used to train a neural network. Each technique has its own advantages and disadvantages. However a lot of work is already been done yet there are many challenges in verification field.

COMPARISON

The various approaches used for signature verification are compared on the basis of characteristics, verification techniques. Following table list the comparison between such approaches.

Table - 1 List of Comparison between Different Approaches

Sr.No	Approach	Characteristics	Verification Techniques	Advantage	Disadvantage
1	Hidden Markov Model	Suited for sequence analysis in signature verification.	-left to right -Ergodic -Ring	Easily detects simple and random forgeries	Poor at detecting skilled forgeries
2	Support vector machine	Kernal based technique for classification and regression.	2 classes used- linear and classification	Effective in high dimensional spaces.	If no of features is much greater than no. of samples, the method is likely to give poor performance.
3	Template matching	Employs pattern comparison process	-Euclidean distance -Dynamic time wrapping -Displacement functions	Suitable for detecting genuine signature via rigid matching.	Not appropriate for detecting skilled forgeries.
4	Neural network	-Used to model complex functions. -Suitable for modelling global features.	-Multilayer perceptrons -Feed-forward network -Back Propagation -Radial basis function	Widely accepted classifiers for pattern recognition	Requires a highly representative dataset.
5	Statistical approach	Uses statistical method to determine the relationship, deviation etc between two or more data.	-Distance statistics -Membership function.	Good at identifying random & simple forgeries.	Use of static features limits it from detecting skilled forgery

REFERENCES

[1] Suhail M Odeh and Manal Khalil, Offline Signature Verification and Recognition: Neural Network Approach, *IEEE Trans on Neural Network* (INISTA) 2011, Istanbul, Turkey,15-18 June 2011**,2011**, pp. 34-38

[2] Meenakshi K. Kalera, Sargur Srihari and Aihua Xu, ―Offline Signature Verification and Identification using Distance Statistics‖, *International Journal of Pattern Recognition and Artificial Intelligence*, Vol.18, No.7, pp.1339-1360, **2004.**

[3] Plamondon and SN Srihari, Online and Offline Handwriting Recognition: A Comprehensive Survey, *IEEE Tran. on Pattern Analysis and Machine Intelligence*, **2000,** 22 (1), 63-84.

[4] R Edson, F Justino, Bortolozzi and R Sabourin, An Off-Line Signature Verification using HMM for Random, Simple and Skilled Forgeries, *Proc. Sixth International Conference on Document Analysis and Recognition*, 1031-1034,Sept.**2001.**

[5] Martinez LE, Travieso CM, Alonso JB and Ferrer M, Parmetrization of a Forgery Handwritten Signature Verification using SVM, *IEEE 38th Annual International Carnahan Conference on Security Technology*, **2004**, 193-196.

[6] B Fang, YY Wang, CH Leung, YY Tang, PCK Kwok, KW Tse and YK Wong, A Smoothness Index based Approach for Off-line Signature Verification, Pattern recognition, vol. 36, pp.91-101,**2003.**

[7] Alan McCabe, Neural Network-based Handwritten Signature Verification, *Journal of Computer*, Vol.3, No.8, August **2008,** 3 (8), pp.9-22.

[8] M Blumenstein, S Armand and Muthuk kumarasamy, Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural based Classification, *International Joint Conference on Neural Networks*, (IJCNN' 04), **2004,** pp. 2983-2987.

[9] MI C Fairhurst, Signature Verification Revisited: Promoting Practical Exploitation of Biometric Technology, *Electronics & Communication Engineering Journal*, (ECEJ), **1997,** pp. 273-280.

[10] B Herbst, J Coetzer and J Preez, Online Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model, *EURASIP Journal on Applied Signal Processing*, **2004**, 4, 559–571.

[11] Miguel A Ferrer, Jesus B Alonso and Carlos M Travieso, Offline Geometric Parameters for Automatic Signature Verification Using Fixed Point Arithmetic, *IEEE Transactions on Pattern Analysis And Machine Intelligence*, **2005,** 27 (6).

[12] MS Arya and VS Inamdar, A Preliminary Study on Various Offline Handwritten Signature Verification Approaches, *Proceeding of International of Computer Applications*, **2005,** 1 (9), 1377-1385.

[13] Jacek M. Zurada, *An Introduction to Artificial Neural Systems*, West Publishing Company, **1992**.