

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.725 – 731

REVIEW ARTICLE

A Review on Offline Signature Verification and Recognition Using Neural Network

Ms. Shital S.Wagh¹, Prof. S.R.Gupta²

¹ Department of Computer Science and Engineering, PRMIT, Amravati, India

² Department of Computer Science and Engineering, PRMIT, Amravati, India

¹shitalwagh12@gmail.com; ²sunilguptacse@gmail.com

Abstract— Signature identification is an important research area in the field of person authentication. This paper discusses signature verification and recognition using neural network approach to recognize originality of signature. The scanned images are introduced into the computer, their quality is modified by image enhancement and noise reduction techniques along with feature extraction and neural network training. This paper focuses on image pre-processing, feature extraction and various approaches of signature verification along with neural network.

Keywords— Signature, Feature extraction, Neural network, Image processing, Signature verification and recognition

I. INTRODUCTION

This paper discusses the importance of signature identification with new approach that is neural network. The signature verification has an advantage over other forms of biometric security verification techniques; including fingerprint, voice, iris recognition, palm prints, and heart sound recognition. It is mostly used to identify a person carrying out daily routine procedures, i.e. bank operations, document analysis, electronic funds transfer, and access control, by using his handwritten signature.[1] In this area signature is a special case that provides secure means for authentication, attestation authorization in many high security environment. The objective of the signature verification system is to discriminate between two classes: the original and the forgery, which are related to intra and interpersonal variability. The variation among signatures of same person is called Intra Personal Variation. The variation between originals and forgeries is called Inter Personal Variation. This paper deals with feature point extraction and artificial neural network. The feature point extraction method is one of the most important technique, used in research work in the field of personal identification. Signature verification methods can be off-line and on-line. Off-line verification methods depend on the features that can be extracted from still images already available. On the other hand, in the on-line methods, the signature is verified in real time while the person is signing. The challenge of accepting or rejecting an offline signature, by a computer system,

is how to verify signatures with lowest error rate. Basically there are number of approaches for offline signature verification but this paper focuses on neural network. At present, a methods based on moment invariant method and Artificial Neural Network (ANN) which uses a four-step process: separates the signature from its background, normalizes and digitizes the signature, applies moment invariant vectors and finally implements signature recognition and verification, was successful in the verification of signatures that ANN was trained for, but has a poor performance when ANN was not trained for. [4]

II. TERMINOLOGIES IN SIGNATURE VERIFICATION AND RECOGNITION

A. *Types of forgeries*

There are three different types of forgeries to take into account.

1. Random forgery: Random forgery which is written by the person who doesn't know the shape of original signature.

2. Simple forgery: Simple forgery which is represented by a signature sample, written by the person who knows the shape of original signature without much practice.

3. Skilled forgery: Skilled forgery represented by a suitable imitation of the genuine signature model.

Fig. 1 shows the different types of forgeries and how much they vary from original signature.

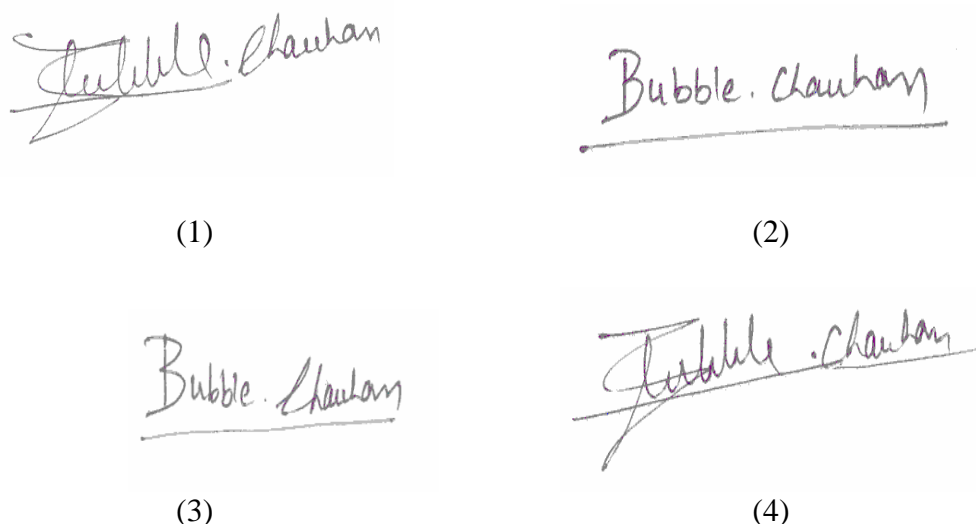


Fig 1: Original signature(1), Random forgery(2), Simple forgery(3), Skilled forgery(4)

B. *Signature verification techniques*

There are two main signature verification techniques

1. Offline Signature Verification Technique- Offline signature verification technique is also known as static signature verification. This approach is based on static characteristics of the signature which are invariant. The off-line recognition just deals with signature images acquired by a scanner or a digital camera. In general, offline signature recognition & verification is a challenging problem. Unlike the on-line signature, where dynamic aspects of the signing action are captured directly as the handwriting trajectory, the dynamic information contained in off-line signature is highly degraded. Handwriting features, such as the handwriting order, writing-speed variation, and skillfulness, need to be recovered from the grey-level pixels.[2]

2. Online Signature Verification Technique- Online signature verification technique is also known as dynamic signature verification. 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.

III. STEPS FOR OFFLINE SIGNATURE VERIFICATION ALONG WITH CLASSIFICATION

An offline signature verification scheme basically uses some network or mechanism as a classifier and a database in which some specimen signatures are stored. Features are extracted for each stored signature and when a new signature is employed it is matched using the classifier which classify it as genuine or forgery.

A. Steps involved in Signature verification process can be summarized as

1. Acquire the Signature images to create a database.
2. Perform image pre-processing to remove noise and blurring.
3. Extract the various features of stored images.
4. Use these features to train the classifier
5. Employ unknown Signature image and extract its features.
6. Perform the pattern matching with data set.
7. Do the classification and classify as genuine or forge.

B. Classification

Different researchers use different approaches for feature extraction and training method in signature verification. Some of the well known approaches are classified as

1. Template Matching Approach-

The template matching is the simplest and earliest but rigid approach to pattern recognition in which instances of pre-stored patterns are sought in an image. It is performed at the pixel level and also on higher level. This approach has a number of disadvantages due to its rigidity. It may fail if the patterns are distorted due to the imaging process, viewpoint change etc as in the case of signatures. It can detect casual forgeries from genuine signatures But cant verify between the genuine signature and skilled ones. The template matching method can be categorized into several forms such as graphics matching, stroke analysis and geometric feature extraction, depending on different features.[3]

2. Support Vector Machine Approach-

Support Vector Machine (SVM) was used to verify and classify the signatures and a classification ratio of 0.95 was obtained. With a set of examples from two classes, a SVM finds the hyperplane, which maximizes the distance from either class to the hyperplane and separates the largest possible number of points belonging to the same class on the same side. Therefore the misclassification error of data both in the training set and test set is minimized. Support Vector Machines (SVMs) are machine learning algorithms that uses a high dimensional feature space and estimate differences between classes of given data to generalize unseen data. The system in uses global, directional and grid features of the signature and SVM for classification and verification.

3. Hidden Markov Models Approach-

HMM has been used successfully to model speech and online signature in the past two decades. The success has been attributed to the fact that these biometric traits have time reference. Only few HMM based offline signature recognition systems have be developed

because offline signature lack time reference. The signature to be trained or recognized is vertically divided into segments at the centre of gravity using the space reference positions of the pixels. The number of segmented signature blocks is equal to the number of states in the HMM for each user notwithstanding the length of the signatures.[5]

4. Statistical Approach-

Using statistical knowledge, the relation, deviation, etc between two or more data items can easily be found out. To find out the relation between some set of data items we generally follow the concept of Correlation Coefficients. In general statistical usage refers to the departure of two variables from independence. To verify an entered signature with the help of an average signature, which is obtained from the set of, previously collected signatures, this approach follows the concept of correlation to find out the amount of divergence in between them. In this approach various features are extracted which include global features like image gradient, statistical features derived from distribution of pixels of a signature and geometric and topographical descriptors like local correspondence to trace of the signature. The classification involves obtaining variations between the signatures of the same writer and obtaining a distribution in distance space. For any questioned signature the method obtains a distribution which is compared with the available known and a probability of similarity is obtained using a statistical Kolmogorov-Smirnov test. Using only 4 genuine samples for learning, the method achieves 84% accuracy which can be improved to 89% when the genuine signature sample size is increased. This method does not use the set of forgery signatures in the training/learning.

5. Neural Network Approach-

At present, a methods based on moment invariant method and Artificial Neural Network (ANN) which uses a four-step process: separates the signature from its background, normalizes and digitizes the signature, applies moment invariant vectors and finally implements signature recognition and verification, was successful in the verification of signatures that ANN was trained for, but has a poor performance when ANN was not trained for. Neural network with back propagation is more efficient. Off-line signature recognition & verification using back propagation neural network is proposed, where the signature is captured and presented to the user in an image format. 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(input layer, output layer and hidden layer).

IV. WHY NEURAL NETWORK IS EFFICIENT THAN OTHER APPROACHES

Neural network is one of the most efficient technique for pattern recognition in general. 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. Neural networks are highly reliable when trained using a large amount of data. They are used

in applications where security is highly valued.[1] A neural network is one application of artificial intelligence, where a computer application is trained to think like a human being or even better. A neural network is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. The key element of this paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems.[6] Neural network uses back propagation for this purpose along with feature point extraction method.

A. **Back Propagation Artificial Neural Network**

Back propagation artificial neural network is easier to implement, it uses more than one input layers usually three. Those layers are as follows

1. Input layer- This layer holds the input for the network.
2. Output layer- This layer holds the output data, usually an identifier for the input.
3. Hidden layer- This layer comes between the input layer and the output layer. They serve as a propagation point for sending data from the previous layer to the next layer.

B. **Feature Point Extraction Method**

The choice of a powerful set of features is crucial in signature verification systems. In this system, three groups of features are used such as grid features, local features and global features. Grid information concerned with the overall appearance information of the signature. Global features describe the entire signature image such as width, height, aspect ratio. These features are used in combination with other features. These features are less sensitive to noise. Local features describe the properties of signature image in specific parts. They are calculated by partitioning the signature image into parts by help of geometric centre or some other means.[3] In this method feature points are extracted from the signature image based on the geometric centre of the image.

The geometric features are based on two sets of points in 2- dimensional plane. The vertical splitting of the image results thirty feature points ($v_1, v_2, v_3, \dots, v_{30}$) and the horizontal splitting results thirty feature points ($h_1, h_2, h_3, \dots, h_{30}$). These feature points are obtained with relative to a central geometric point of the image. Here the centered image is scanned from left to right and calculate the total number of black pixels. Then again from top to bottom and calculate the total number of black pixels. Then divide the image into two halves w.r.t. the number of black pixels by two lines vertically and horizontally which intersects at a point called the geometric centre. With reference to this point we extracted 60 feature points: 30 vertical and 30 horizontal feature points of each signature image.

The geometric features are based on two sets of points in 2- dimensional plane. The vertical splitting of the image results thirty feature points ($v_1, v_2, v_3, \dots, v_{30}$) and the horizontal splitting results thirty feature points ($h_1, h_2, h_3, \dots, h_{30}$). These feature points are obtained with relative to a central geometric point of the image. Here the centered image is scanned from left to right and calculate the total number of black pixels. Then again from top to bottom and calculate the total number of black pixels. Then divide the image into two halves w.r.t. the number of black pixels by two lines vertically and horizontally which intersects at a point called the geometric centre. With reference to this point we extracted 60 feature points: 30 vertical and 30 horizontal feature points of each signature image.

1. Feature point based on vertical splitting-

Thirty feature points are obtained based on vertical splitting with respect to the central feature point. The procedure for finding vertical feature points is given below:

Algorithm 1:

Input: Static signature image after moving it to the centre of the fixed sized frame.

Output: Vertical feature points: $v_1, v_2, v_3, v_4, \dots, v_{29}, v_{30}$.

The steps are:

- 1) Split the image with a vertical line passing through the geometric centre (v_0) which divides the image into two halves: Left part and Right part.
- 2) Find geometric centers v_1 and v_2 for left and right parts correspondingly.
- 3) Split the left and right part with horizontal lines through v_1 and v_2 to divide the two parts into four parts: Top-left, Bottom-left and Top-right, Bottom-right parts from which we obtain v_3, v_4 and v_5, v_6 .
- 4) We again split each part of the image through their geometric centers to obtain feature points $v_7, v_8, v_9 \dots v_{13}, v_{14}$.
- 5) Then we split each part once again to obtain all the thirty vertical feature points.

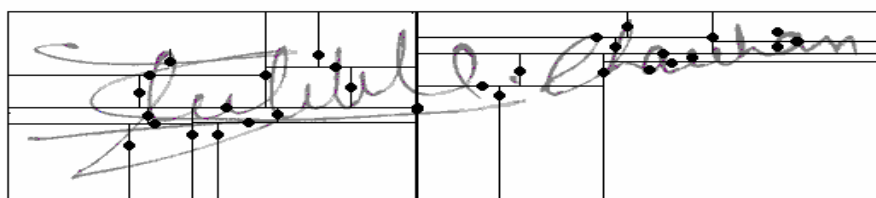


Fig 2 Vertical splitting of the signature image

2. Feature points based on Horizontal Splitting-

Thirty feature points are obtained based on horizontal splitting with respect to the central feature point. The procedure for finding horizontal feature points is given below:

Algorithm 2:

Input: Static signature image after moving it to the centre of the fixed sized frame.

Output: Horizontal feature points: $h_1, h_2, h_3, h_4, \dots, h_{29}, h_{30}$.

The steps are:

- 1) Split the image with a horizontal line passing through the geometric centre (h_0) which divides the image into two halves: Top part and Bottom part.
- 2) Find geometric centers h_1 and h_2 for top and bottom parts correspondingly.
- 3) Split the top and bottom part with vertical lines through h_1 and h_2 to divide the two parts into four parts: Left-top, Right-top and Left-bottom, Right-bottom parts from which we obtain h_3, h_4 and h_5, h_6 .
- 4) We again split each part of the image through their geometric centers to obtain feature points $h_7, h_8, h_9 \dots h_{13}, h_{14}$.
- 5) Then we split each part once again to obtain all the thirty vertical feature points.

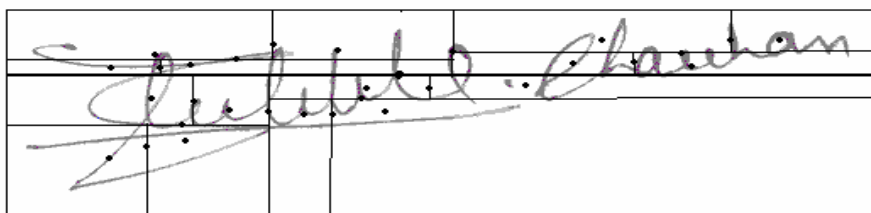


Fig 3 Horizontal splitting of the signature image

V. CONCLUSIONS

There are various approaches for offline signature verification, each technique has its different advantages and disadvantages. Among them artificial neural network is efficient for signature verification. This paper also focuses on feature point extraction method based on vertical and horizontal splitting.

REFERENCES

- [1] S.Odeh, M.Khalil, "Offline Signature Verification and Recognition: Neural Network Approach," IEEE, 2011, 978-1-61284-922-5/11.
- [2] Mahendra S. Chauhan, "Offline Signature Verification Scheme Using Feature Extraction Method" thesis, NIT, Rourkela, May 2007.
- [3] S.Khan and A.Dhole, "A Review on Off line signature verification and recognition Techniques", IJARCCCE, Vol.3, Issue 6, June 2014.
- [4] E. Özgündüz, T. Uentürk and M. E. Karşılıgil, "Off line signature verification and recognition by support vector machine", Eusipco 2005.
- [5] Dr.S.A.Daramola and Prof.T.S.Ibiyemi, "Offline Signature Recognition Using Markov Model (HMM)", IJCA(0975-8887), Vol 10-No.2, November 2010.
- [6] C. Stergiou, and D. Siganos, "Neural Networks. Computing". Surprise96 journal, vol. 4, 1996.