Apply Multi-Layer Perceptrons Neural Network for Off-line signature verification and recognition

Suhail Odeh and Manal Khalil

Computer And Information Systems Department, Bethlehem University
Bethlehem, Palestine

Abstract

This paper discusses the applying of Multi-layer perceptrons for signature verification and recognition using a new approach enables the user to recognize whether a signature is original or a fraud. The approach starts by scanning images into the computer, then modifying their quality through image enhancement and noise reduction, followed by feature extraction and neural network training, and finally verifies the authenticity of the signature. The paper discusses the different stages of the process including: image pre-processing, feature extraction and pattern recognition through neural networks.

Keywords*: MLP Neural network; Feature extraction; Signature verification and recognition; image processing.*

1. Introduction

This paper discusses the importance of a signature verification and recognition system, it explains how it can be implemented and developed through certain specifically chosen features. 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, 2]. This paper deals with an automated method of verification an off line signature recognition by extracting features that characterizes the signature. The approach starts by scanning images into the computer, then modifying their quality through image enhancement and noise reduction, followed by feature extraction and neural network training, and finally verifies whether a signature is original or fake. [3, 4, 5, 6]

Data about the specifications and needs of this project have been collected by interviewing banking personnel; managers and employees. The aim of this project was to figure out exactly how this research work can contribute to enhancing their processes of signature verification and recognition.

There are many existing systems and studies that are based on different methods of identity verifications and recognition.[7] 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. [8] A support vector machine was used to verify and classify the signature using the global directional and grid features of signatures, the classification ratio was 0.95. Bromley [9] used a novel ANN, called “Siamese” neural network, which consists of two identical sub-networks joined at their outputs. Several ANN topologies were tested, [10] and their accuracies were compared, where the best had an error rate of 3.3%. This system extracted various static and dynamics signature features and used to train the ANN.

This research has been conducted using the “GPDS300signature database” offered for those doing research in the field of signature recognition at the Universidad de Las Palmas de Gran Canaria, Spain. The database contains data from 300 individuals, including 24 genuine signatures from individuals, and 30 forgeries. The 24 genuine specimens were collected in a single day of writing sessions. The forgeries were produced from the static images of the genuine signatures. Each forger was allowed to practice the signature for as long as she/he wished. Each forger imitated 3 signatures of 5 signers in a single day writing session. The genuine signatures were shown to each forger and were chosen randomly from the 24 genuine ones. Therefore, for each genuine signature, 30 skilled forgeries were produced by 10 forgers, from 10 different genuine specimens.

2. Methodology of Signature Verification and Recognition

The process of signature verification and recognition allows the user to detect whether a signature is original or forged. According to many studies that were done on signatures and types of signatures, there are 3 major categories of forged signatures:

- 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 [8].

It can be conclude that skilled signatures are the most difficult to detect, these can be very similar to the original signature, and the error rate might be very small.

There are 3 major steps in achieving signature verification and recognition, and each of these steps consists of many methods that contribute to improved results. These steps are:

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

2.1 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.

After an image is acquired, it goes through different levels of processing before it is ready for the next step of feature extraction. The following are the reasons why image pre-processing is important:

- It creates a level of similarity in the general features of an image, like the size aspect. This enhances the comparison between images.
- Signatures vary according to the tool that was used in writing; the type of pen/pencil, the ink, the pressure of the hand of the person making the signature, and so on. In off-line signature recognition, these facts are not important, and have to be eliminated and the matching should be based on more important offline features.
- Noise reduction, defects removal and image enhancement.
- Improves the quality of image information.
- It eases the process of feature extraction, on which the matching depends mainly.

Image pre-processing differs according to the genre that the image belongs to. The techniques used in this process may vary. There are 4 techniques that are used for signature recognition including; reading, displaying and resizing of the image, segmentation, binarization, fast fourier transform (FFT), enhancement and thinning

Fig. 1 Original Scanned Signature

Fig. 2 Segmented and binarized signature

Fig.3 Thinned Signature

2.2 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 results.

The term feature here refers to a certain characteristic that can be measured using designed algorithms; which can then be retrieved by "extraction".

For this signature recognition and verification research, four main features will be extracted. These features are: eccentricity, skewness, kurtosis, orientation.

2.2.1 Eccentricity

Eccentricity is defined as the central point in an object. In case of signature image, eccentricity is the central point of the signature. The importance of this feature is that we need to know the central point of 2 images in order to compare them. After identifying the central point, we can then compare the features around them. If there is a deviation in the central point of an image, this will indicate a possible imitation of the signature, but this is not enough evidence by itself.

The central point is acquired by applying the ratio of the major to the minor axes of an image.

2.2.2 Skewness

"Skewness is a measure of symmetry, or more precisely, the lack of symmetry. A distribution or data set, is symmetric if it looks the same to the left and right of the center point". [11]
The skewness can be defined according to univariate data $Y_1, Y_2, \ldots, Y_N$, as following:

$$skewness = \frac{\sum_{i=1}^{N}(Y_i - \bar{Y})s^3}{(N-1)s^3} \qquad (1)$$

Where $\bar{Y}$ is the mean, S is the standard deviation, and N is the number of data points.

The measurement of skewness allows us to determine how bowed are the lines in each segment of the signature. The percentage of this torsion is then calculated and extracted. Furthermore, this percentage is compared to that extracted from the other image.

The importance of this feature is that it measures the symmetry or the lack of it, which is an important aspect of a signature. Most signatures are complicated, with no edges but twists, and the width and height of these twists is a very important aspect for measurement and comparison.

2.2.3 Kurtosis

Kurtosis is a measure of whether the data are peaked or flattened, relative to a normal distribution. That is, data sets with high kurtosis tend to have a distinct peak near the mean, decline rather rapidly, and have heavy tails. Data sets with low kurtosis tend to have a flat top near the mean rather than a sharp peak. A uniform distribution would be the extreme case. [11]

The Kurtosis can be defined according to univariate data $Y_1, Y_2, \ldots, Y_N$, as following:

$$Kurtosis = \frac{\sum_{i=1}^{N}(Y_i - \bar{Y})s^4}{(N-1)s^4} \qquad (2)$$

Where $\bar{Y}$ is the mean, S is the standard deviation, and N is the number of data points. There are other definitions for excess kurtosis, but here in this paper the original definition is used.

The kurtosis measurement highlights the peaks in each segment of a signature. It also measures the existence, or the absence of tails, that are unconnected lines with no peaks.

As you can see, kurtosis and skewness are highly interlinked.

2.2.4 Orientation

Orientation defines the direction of the signature lines. This feature is important because it allows us to know how the signer wrote down the signature, which letters came first emphasizing the direction of angles and peaks. The orientation feature is used to compute the optimal dominant ridge direction in each block of a signature.

Orientation is acquired by applying the ratio of angle of major axis. The orientation of the signature can be found using the Matlab "regionprops" function, in which the angle between the x-axis and the major axis of the ellipse that has the same second-moments as the region.

Fig. 4 The orientation detection

Figure 4 illustrates the axes and orientation of the ellipse. The left side of the figure 4 shows an image region and its corresponding ellipse. The right side shows the same ellipse, with features indicated graphically; the solid blue lines are the axes, the red dots are the foci, and the orientation is the angle between the horizontal dotted line and the major axis.

2.3 Pattern Recognition through Neural Network

Neural networks are known for being a very accurate and efficient technique for pattern recognition in general. In this section, we will explain more about the idea and structure of neural networks, their types, and how they contribute to pattern recognition.

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. [12]

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. [13] 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.

In this research we used Multi Layer Perceptrons MLPs neural network. The structure of this neural network depends on the multi layer feed forward, where all the nodes in any layer have connections to all the nodes in the next layer and so on, but these nodes do not have any connections with the previous layers. Then, it was modified to function as a back-propagation neural network, using the BP algorithm.

The Node is a processing element which produces an output based on a function of its inputs. In Figure 5 the neuron are represented with the node, where the neuron has N weighed inputs and a single output. [14] The neuron calculates a weighted sum of inputs and compares it to a threshold. If the sum is higher than the threshold, the output is set to 1, otherwise to -1.

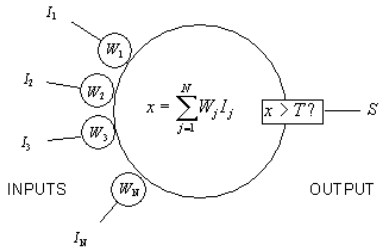

Fig. 5 The architecture of artificial neuron

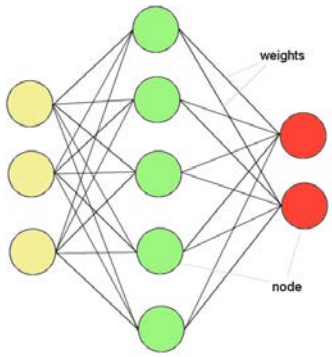

Fig.6 The Architecture of MLP

Figure 6 shows a three-layer perceptron with an input layer, one hidden layer and an output layer. Classification and recognition capabilities of MLP come from the nonlinearities used within the nodes. $I_1,I_2,\ldots,I_N$ these are the input signals, $w_1,\ldots,w_N$ are the synaptic weights, x the activation potential, θ the threshold and y the output signal and f the activation function:

$$x = \sum_{i=1}^{N} w_i I_i \qquad (3)$$

$$y = f(x - \theta) \qquad (4)$$

Defining $w_0=\theta$ and $I_0=-1$, the output of the system can be reformulated as:

$$y = f\left(\sum_{i=0}^{N} w_i I_i\right) \qquad (5)$$

The activation function f defines the output of the neuron in terms of the activity level at its input. The most common form of activation function used is the sigmoid function. [14]

The implementation of BP learning, updates the network weights and biases in the direction in which the performance function decreases most rapidly, the negative of the gradient. The equation for this algorithm, for one iteration, can be written as follows:

$$X_{k+1} = X_k - \alpha_k g_k \qquad (6)$$

Where X_k is a vector of current weights and biases, g_k is the current gradient and α_k is the learning rate. In this paper, the gradient is computed and the weights are updated, after each input to the network. [12, 15]

The network was then trained using the set of data available in the database as an input to input layer, which include the images and their extracted features of eccentricity, skewness, kurtosis, and orientation. The output layer consists of a single node that calculates the weighted sum of the connections coming to the output layer [10]. The number of the neurons in the hidden layer is double of the neurons in the input layers, so that the neural network can learn the technique of recognition based on these previously mentioned features.

The final output from MLPs networks is a confidence value indicating the likelihood that the test signature was performed by the same person that provided the reference signatures used in training. The confidence value is compared to a threshold and the test signature is verified. If the confidence exceeds this threshold it is accepted or otherwise is rejected. Then the classification rate or the error can be calculated in percentage rate.

3.4 Recognition

As a result of all previous processes, recognition of a signature is achieved. The following are the steps detailing how exactly the recognition process is designed and operates:

- The trained neural network – which has learned how to work on signatures and their features through training – compares the features of the given signature with those of the signatures in the database.
- The differences between the extracted features from the new signature and those in the database are calculated. The outcome of the total of these differences is calculated.
- The tag of the signature with least differences is then returned, with a number showing the percentage of similarity.
- Based on the similarity percentage, it is decided whether the signature is original or not.
- If the percentage of similarity ranges between 85-100%, the signature is considered original. This is based on the natural signature recognition method, which says that there are natural differences in the signature of a single person, in the multiple tries.
- If the percentage of similarity ranges between 75-85%, the signature is considered relatively suspicious.
- If the percentage of similarity is lower than 75%, the signature is considered highly suspicious.

3. Results and Accuracy

As mentioned earlier in this paper, security is one of the most critical issues when it comes to signature recognition, especially if used by banks. One fraud signature, can mess up transactions, causes the bank and customers financial losses, and affect the security reputation of the bank, which is a damage that cannot be easily fixed.

For those reasons, 4 features were used in the feature extraction section of this project, and were applied to all the samples tested. In addition to that, the following table shows the accuracy rates and error rates calculated as an average of the calculations made for over more than 200 samples.

Table 1: The results of MLPs NN.

	Accuracy rate	Error rate
Trainng	64%	36%
Test	78.8%	21.2%

4. Conclusions

This paper presents a method for offline signature verification and recognition by using MLP neural network that used four features; eccentricity, skewness, kurtosis, and orientation, which can be extracted by image processing. The neural network was trained using back-propagation algorithm. A 21.2% error rate is hereby reported by this approach, a great improvement over other published studies that reported error rates of around 44.9% [10]. This indicates that our approach and the four features

are working well with a good optimization of 'verification the offline signature'. [16]

References

[1] C. Allgrove and M.C. Fairhurst, "Majority Voting for Improved Signature Verification," IEE Colloquium on Visual Biometrics 2000, (Ref No. 2000/018), pp. 9/1 –9/4.

[2] J. F. Vargas, M. A. Ferrer, C. M. Travieso, J. B. Alonso , "Offline Signature Verification Based on Pseudo-Cepstral Coefficients ", 10th International Conference on Document Analysis and Recognition, IEEE, DOI 10.1109/ICDAR.2009.68, 2009, pp. 126–130.

[3] M. Ferrer, J. Alonso, and C. Travieso, "Offline geometric parameters for automatic signature verification using fixedpoint arithmetic". IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.27, No.6, 2005, pp. 993–997.

[4] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, and J. Ortega-Garcia, "An off-line signature verification system based on fusion of local and global information", In Workshop on Biometric Authentication, Springer LNCS-3087, 2004, pp. 298–306.

[5] N. S. Kamel, S. Sayeed, and G. A. Ellis, "Glove-Based Approach to Online Signature Verification", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 30, No. 6, 2008, pp. 1109-1113.

[6] A. A. Zaher and A. Abu-Rezq, "A Hybrid ANN-Based Technique for Signature Verification", Proceedings of the 4th WSEAS International Conference on COMPUTATIONAL INTELLIGENCE, Universitatea Politehnica, Bucharest, Romania, 2010, pp. 13-19.

[7] C. Oz, F. Ercal, and Z. Demir, "Signature Recognition and Verication with ANN", in Proc. of Third In-ternational Conference on Electrical and Electronics Engineering, (ELECO'03), Bursa, Turkey, 2003.

[8] E. 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.

[9] J. Bromley, J. W. Bentz, L. Bottou, I. Guyon, Y. L. Cun, C. Moore, E. Säckinger and R. Shah, "Signature Verification using a Siamese Time Delay Neural Network", International Journal of Pattern Recognition and Artificial Intelligence, Vol. 7, No.4, 1993.

[10] A. McCabe, J. Trevathan and W. Read, "Neural Network-based Handwritten Signature Verification", Journal of computers, Vol. 3, No. 8, 2008, pp. 9-22.

[11] NIST/SEMATECH e-Handbook of Statistical Methods, http://www.itl.nist.gov/div898/handbook/, 2010.

[12] C. Stergiou, and D. Siganos, "Neural Networks. Computing", Surprise96 journal, Vol. 4, 1996.

[13] T. Keit, R. Palaniappan, P. Raveendran and F. Takeda, "Signature Verification System using Pen Pressure for Internet and E-Commerce Application", Proceedings of ISSRE 2001, Organized by Chillarge Inc, USA.2001.

[14] E. Martinez, A. Sanchez and J. Velez "Support Vector Machines versus Multi-Layer Perceptrons for Efficient Off-Line Signature Recognition" Engineering Applications of Artificial Intelligence, Vol. 19, No. 6, September 2006, pp. 693-704.

[15] B. D. Ripley, "Pattern Recognition and Neural Networks", 1 ed., New York: Cambridge University Press, 2008.

[16] S. Odeh and M. Khalil, "Off-line signature verification and recognition: Neural network approach", INISTA 2011, Istanbul, Turkey, 15-18 June 2011, 2011, pp. 34 – 38.

Suhail Odeh Born in Bethlehem, after completing his Bachelor degree in Physics and Electronic Technology and Master Degree in Physics (2001) from Al-Quds University, he completed another Master degree (2004) and PhD degree (2006) in the Computer Engineering from the Department of Computer Architecture and Technology, University of Granada, Spain. Get an award for his thesis from University of Granada. Dr. Suhail Odeh Joins the Bethlehem University community as an Assistant professor in the Computer and information System Department in the Faculty of science at (2006).

He is a member of investigation group in Granada University and has many publisher papers in international conference and journals. He is an active researcher in the field of Artificial intelligence, Brain Computer Interface, Image processing, pattern recognition.

Manal Khalil A Palestinian graduate from Bethlehem University who received her Bachelor of Science in Computer and Information Systems in 2010. She work now as an administrative assistance in the Applied Research Institute-Jerusalem ARIJ.