Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Offline Prompt Signature Recognition and Verification

Shradha Chadokar
M. Tech. Scholar, Department of CSE
O.I.S.T,Bhopal(M.P), India

Mr. Jijo S Nair
Asst. Professor, Department of CSE
O.I.S.T,Bhopal(M.P), India

Abstract*— In the age of growing technology, security is the major concern to avoid fraud and forgeries. The Person's Signature is an important biometric feature of a human being which is basically used to authenticate human personality. A number of biometric techniques have been proposed for personal identification in the past, Such as face recognition, voice recognition, iris scanning, fingerprint recognition, and retina scanning. Signature recognition or signature verification are the most widely known. In this paper issues regarding off-line signature recognitions, existing system, their performance and method for feature extraction are assumed. –There are various methods to signature recognition with a lot of scope to investigate. The method presented in this paper consists of image pre-possessing, feature extraction, image enhancement and noise reduction techniques and finally verifies the authenticity of the signature.

Keywords*— Biometrics, Image Pre-processing, Feature Extraction, noise reduction technique and Off-line Signature Recognition and Verification.

I. INTRODUCTION

Signature recognition is a behavioural biometric. It can be operated in two different behaviour: static: in this form, users write their signature on paper, digitize it through an optical scanner and may be a camera, and the biometric system recognizes the signature analyzing its shape. This group is also known as "off-line". Dynamic: in this mode, users write their signature in a digitizing tablet, which acquires the signature on real time. Another possibility is the acquisition by means of stylus-operated PDAs. Dynamic recognition is also known as "on-line".

This paper discusses the importance of a signature verification and recognition system, it describe 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 examination, electronic funds transfer, and access control, by using his handwritten signature [1, 2]. This paper deals with an automated method of verifying an off line signature recognition system by extracting features that characterizes the signature. The approach starts by scanning images into the computer, then modifying their quality during image enhancement and noise reduction, followed by feature extraction and finds the correlation based similarities, and finally verifies whether a signature is original or fake.

II. SIGNATURE RECOGNITION

The signature recognition is the process of verifying the writer's identity by checking the signature against samples kept in a database. The outcome of this process is usually a number between 0 and 1 which represents a fit ratio (1 for match and 0 for mismatch). The threshold range is used for confirmation/rejection decision depends on the nature of the application. We use signatures every day to authorise legal documents, contracts and to validate bank checks. While financial institutions and other commercial organisations primarily focus on the visual appearance of our signature for verification purposes, Signature Recognition examines behavioural aspects that manifest themselves when we sign our name. This article examines how Signature Recognition technology and analyses its strengths and weaknesses.

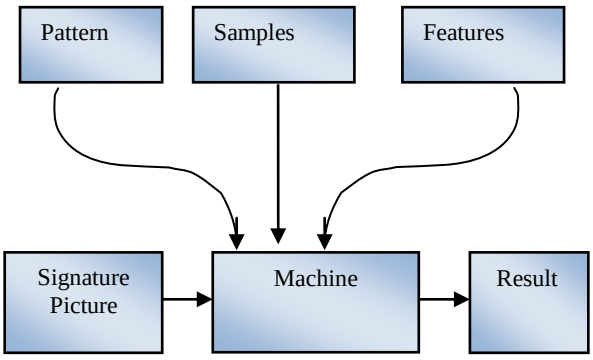

Figure 2.1 Signature Recognition System

There are some important phases about Signature Recognition:

- Signature Samples
- Algorithm to compare Similarity
- Input Signature to check
- Result based on Speed, Accuracy and depends on method which we are using like Offline and Online.

Today thousands of financial and business transactions are being authorized via signatures. Signature verification finds its application in a large number of fields starting from passport verification systems to even authenticating applicants in public examinations from their signatures and online banking. Human signatures can be assumed as an image and recognized using computer vision and neural network techniques.

III. SIGNATURE VERIFICATION AND RECOGNITION

The process of signature verification and recognition agree to the user to detect whether a signature is original or forged. A signature is any written variety in a person's own handwriting meant to be used for identification. A signature verification (SV) system authenticates the identity of any person, based on an analysis of his/her Signature through a set of processes which differentiates a genuine signature from a forgery signature. According to many studies that were done on signatures and types of signatures, there are 3 major categories of forged signatures:

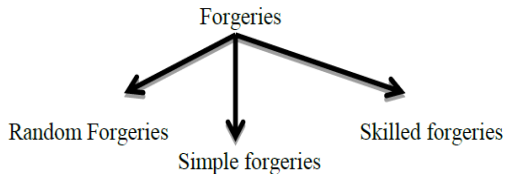

Figure 3.1 Classifications of Forgeries

1. Random: these signatures are not based on any knowledge of the original signature.
2. Simple: these signatures are based on an assumption of how the signature looks like by knowing the name of the signer.
3. Skilled: an imitation of the original signature, which means that the person knows exactly how the original signature looks like.

We can tell 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. Signature verification cannot be done by character recognition because the alphabets of signature cannot be read out separately and it appears as an image with some curves representing the writing style of an personage. So, a signature image can be considered as a special distribution of pixels representing writing style rather than a collection of alphabets. Thus, separate methods were required for signature recognition and character recognition.

IV. SIGNATURE VERIFICATION BASIC CONCEPTS

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

- Image pre-processing
- Feature extraction
- Methodology

A. Image Pre-Processing:-

Image pre-processing represents a broad 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 outputs 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:

- This enhances the comparison between images. It creates a level of similarity in the general features of an image, like the size phase.

- There are two types of Signatures which differ according to the tool that was used in writing such as the type of pen/pencil, the ink, the pressure of the hand of the person making the signature is known as Dynamic Signature recognition. 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.

- Enhance the superiority of image information.

- Image pre-processing vary according to the field that the image belongs to that field. It eases the process of feature extraction, on which the matching depends mainly. The techniques used in this process may diverge. Some basic

techniques that are used for signature recognition including; reading, displaying and resizing of the image, it also uses the segmentation, Binarization, enhancement and thinning.

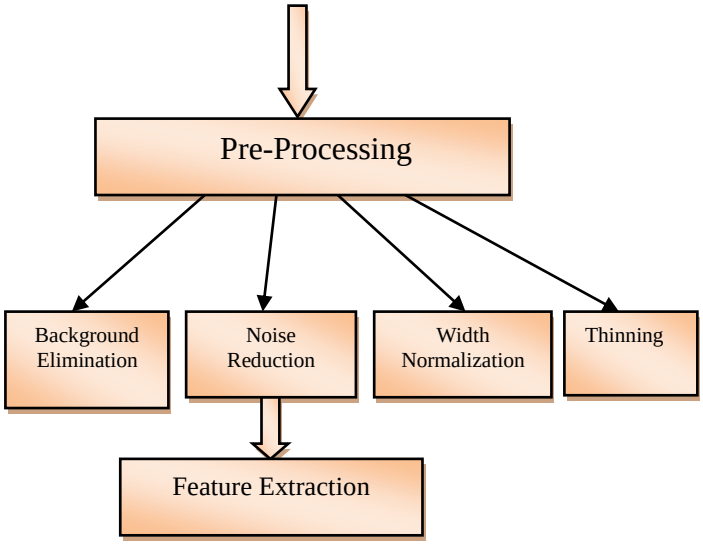

Figure 4.1 Feature Extractions from Signature

B. Feature Extraction:-

Feature extraction is the second major step in signature recognition and verification. The key function of this step is to generate features which can be used for comparison. 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, Orientation.

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 significance 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) Skewness:- Skewness is a compute of symmetry, or more precisely, the lack of symmetry. A distribution, or a data set, is symmetric if it looks the same to the left and right of the centre point". The skewness can be defined according to univariate data Y1,Y2,…,YN, as following:

$$skewness = \frac{\sum_{i=1}^{N}\left(Y_i - \overline{Y}\right)s^3}{(N-1)s^3}$$

Where *Y* is the mean, *N* is the number of data points and *S* is the standard deviation. The measurement of skewness allows us to determine how bowed are the lines in each segment of the signature. The percentage of this position is then calculated and extracted. In addition, this percentage is compared to the image available in database.

The importance of this feature is that it measures the symmetry which is an important aspect of a signature. Most signatures are complicated with edges, twists, width and height, from which twists is a very important aspect for measurement and comparison.

3.) 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.

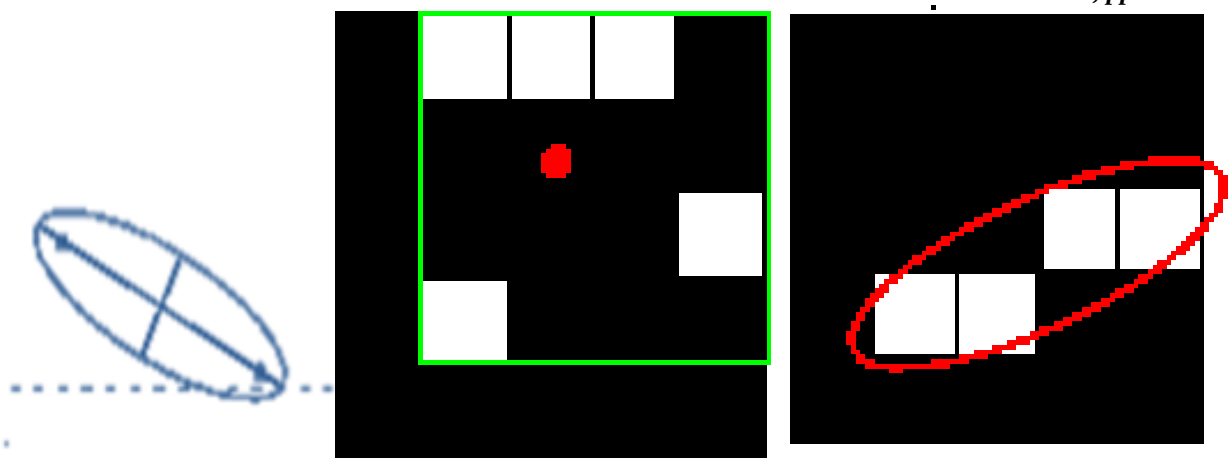

Figure 4.2 Pixel features Eccentricity, Skewness, Orientation

V. LITERATURE SURVEY

Luiz S Oliveira *et al*., [2]in 2007 proposed a writer independent model which reduces the pattern recognition problem to a 2-class problem. Receiver operating characteristic curves are used to improve the performance of the system. The impacts of fusion strategies to combine the partial decisions are classified by SVM.

D. Jena, B Majhi *et al*., [4] in 2008 proposed a off-line signature verification system which is based on selecting 60 feature points element. The classification of the feature points uses statistical parameters like mean and variance to identify skilled and unskilled forgeries.

Ning-Ning Liu; Yi-Ding Wang [7] in 2008 proposed on-line signature verification system exploiting local and global information using two-stage fusion is presented. At the first stage, global information is extracted as 13-dimensional vector and recognized by majority classifiers, and then local information is extracted as time functions of various dynamic properties and recognized by BP neural network classifier. By fusing global and local information and introducing an enhanced dynamic time warping algorithm and a normalized feature measure, our method obtained an average EER of 4.02% on public database SVC2004 (first signature verification competition 2004) Task2 compared to 6.90% the first place at SVC2004.

Ramachandra *et al*., [1] in 2009 proposed robust off-line signature verification based on global features for skilled and random forgeries. The model extracts the features which are preprocessed by normalization, binarization and thinning. The feature extraction technique consists of global features such as maximum horizontal histogram, aspect ratio and maximum vertical histogram, horizontal and vertical centre of signature and signature area.

Ghandali and moghaddam [3] in 2009 proposed a model based on image registration, discrete wavelet transform and image blend. Training signatures of each person are registered to overcome shift and scale problems. The several registered instances of each signature are fused together to generate reference pattern of signatures. In the classification phase euclidean distance is used.

V. Nguyen *et al*., [5] in 2009 proposed a signature verification using global features, which are derived from total energy a writer uses to create signature. The global features are vertical and horizontal projection of a signature, distance between keystrokes in an image and aspect ratio of signature. Support vector machine is used for classification of extracted features.

Ahmed, K.; El-Henawy, I. M.; Rashad, M. Z.; Nomir, O., [6] in 2010 presented a novel online signature verification method that uses PCA for dimensional-reduction of signature instant. The resulting vectors from PCA are submitted to a multilayer perceptron (MLP) neural network with EBP and sigmoid activation function. In the other hand, Dynamic features such as x, y coordinates, pressure, velocity, acceleration, pen down time, distance, altitude, azimuth and inclination angles, etc. are processed statistically. During enrolment, five reference signatures are captured from each user. One-way ANOVA is used to analyze relative X-Coordinates in 6 groups (5 reference group, 1 testing group). ANOVA test will be repeated for relative Y-Coordinates, pressure value, azimuth and inclination angles. Thus, the algorithm will fill up a vector of five distances (F-scores) between all the possible pairs of testing and reference vectors. The resulting vector is compared to a threshold vector. Our database includes 130 genuine signatures and 170 forgery signatures. Our verification system has achieved a false acceptance rate (FAR) of 2% and a false rejection rate (FRR) of 5%.

Pal, S.; Chanda, S.; Pal, U.; Franke, K.; Blumenstein, M.[8] in 2012, proposed a work in the field of biometric authentication, automatic signature identification and verification has been a strong research area because of the social and legal acceptance and extensive use of the written signature as an easy method for authentication. Signatures provide a secure means for confirmation and authorization in legal documents. This feature encoding is based on the amalgamation of Gabor filter-based features with SURF features (G-SURF). Features generated from a signature are applied to a Support Vector Machine (SVM) classifier. For experimentation, 1500 (50×30) forgeries and 1200 (50×24) genuine signatures from the GPDS signature database were used. A verification accuracy of 97.05% was obtained from the experiments.

Table: Summary of Literature Review

Year	Author	Title	Methodology
2007	Luiz S Oliveira *et al*.	Signature Verification using Writer Independent Approach	Support Vector Machine Classification
2008	D. Jena, B. Majhi, and S. K. Jena	Improved Off-line Signature Verification Scheme using Feature Point Extraction Method	Classification of Feature Points
2008	Ning-Ning Liu; Yi-Ding Wang	Fusion of global and local information for an on-line Signature Verification system	BP neural network classifier
2009	A. C. Ramachandra, J. S. Rao, K. B. Raja, K. R. Venugopal, and L. M. Patnaik	Robust Off-line Signature Verification Based On Global Features	Image normalization, binarization and thinning.
2009	Ghandali and M. E. Moghaddam	Off-line Persian Signature Identification and Verification Based on Image Registration and Fusion	Phase Eucladian Distance
2009	V. Nguyen, M. Blumenstein, and G. Leedham	Global Features for the Off-line Signature Verification Problem	Vertical and Horizontal Global Features classification using SVM
2010	Ahmed, K.; El-Henawy, I. M.; Rashad, M. Z.; Nomir, O.	On-line signature verification based on PCA feature reduction and statistical analysis	PCA and MLP Neural Networks
2012	Pal, S.; Chanda, S.; Pal, U.; Franke, K.; Blumenstein, M.	Off-line signature verification using G-SURF	Gabor filter-based features with SURF features (G-SURF).

VI. GENERAL METHODS FOR SIGNATURE VERIFICATION SYSTEM

The design of a Signature Verification system is divided into two stages:

1. Training Phases
2. Testing Phases

A training phase consist of four major steps

1) Retrieval of a signature sample from a local database
2) Image pre-processing
3) Feature extraction
4) Machine training

A testing phase consists of five major steps

1) Retrieved signature to be tested from local database
2) Image pre-processing
3) Feature extraction
4) Use the application of extracted features to a trained neural network
5) Checking result generated from a neural network.

Fig. 6.1 shows one of the original signature samples taken from a database and all the subsequent figures show the resultant signature image obtained after performing the steps mentioned in an algorithm.

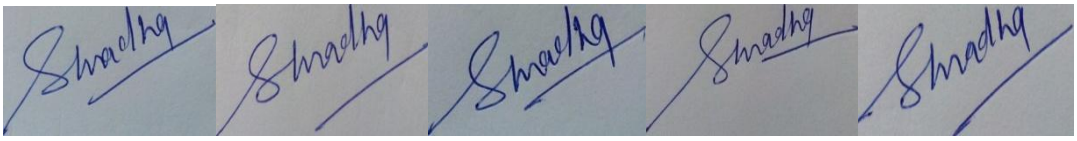

Fig. 6.1 Signature Templates to Train System

A popular means of authentication historically has been the handwritten signature. however such signatures are never the same for the same person at different times, due to which it becomes difficult to discriminate visually the real signature from the forged one. The development of computer–aided handwritten signature verification systems has been ongoing for decades. Different approaches are developed to deal with the handwritten signature recognition problem.

VII. SYSTEM MODEL

The general Signature Verification Model consist of retrieving the signature images from database using feature extraction method which is based on the similar features present in the signatures. The block diagram of general Signature Verification System in fig 2. The first block is the input query image i.e. test image which the system want to search for similar images from databases. Then pre-process the test image to compare with the database images. The comparison from database with lots of images takes time so there is a need which reduces the size of database to compare. The pre processing of database is the actual process of extracting features only from images. Then prepare another database which contains features only.

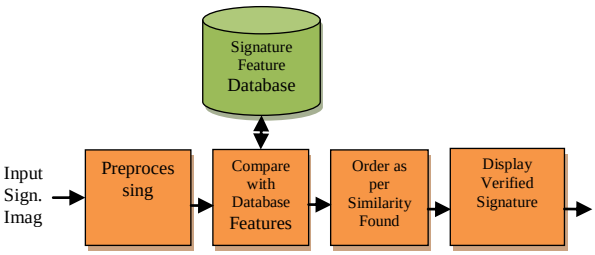

Figure 7.1. Signature Verification System

A. Pattern Recognition through Different Types of Technique:

There are several types of technique mention in this paper which provides the huge amount of training for machine for pattern or signature recognition. Major techniques are Signature Recognition using Clustering Technique, Contour Method, Back-Propagation Neural Network Prototype, Hidden Markov Model and Cross-Validation technique, Kernel Principal Component Self regression, Parameterized Hough Transform, Support Vector Machine, Genetic Algorithm and Artificial neural network based technique.

A neural network is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, paradigm of process information. The key element of this concept is the narrative structure of the information processing system. It comprises of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems.[17]

Neural networks are known for being a very accurate and efficient technique for pattern recognition in general. A neural network is one application of artificial intelligence, where a application of computer is trained to think like a human being or even better.

B. Recognition by help of Neural Network:

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, the system 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 label of the signature with least differences is then returned, with a number showing the percentage of similarity.
- Generally, it is Based on the similarity percentage, it is decided whether the signature is original or not.
- Condition first- 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 on its own person's signature, in the multiple tries.
- Condition Second- If the percentage of similarity ranges between 75-85%, the signature is considered relatively suspicious.
- Condition third- If the percentage of similarity is lower than 75%, the signature is considered highly suspicious.

Signature Database:

The database contains data from N individuals, including for comparision in Signature Verification System. some genuine signatures from individuals, and other some forgeries. The genuine specimens were collected in a single day of writing sessions. The forgeries were produced from the static images of the legitimate signatures. Each forger was allowed to practice the signature for as long as she/he wished.

VIII. CONCLUSIONS

Every Signature Verification System is given a high rate of Authentication in digital world. It actually effects the user in such a way that, if the Signature Verification System does not work properly on the percentage of similarities between the input signature and signature present in database then the user is blocked from availing the services rendered to System. There are various methods for offline signature verification and recognition by using different types of

approaches such as support vector machine, Neural network which uses three features; eccentricity, skewness, and orientation which can be extracted by image processing. Neural network uses Back Propagation Algorithm. The neural network gives better performance but for future use it is quite complex approach to find out the greater similarity between the features of signatures. At the same time it does not provide the very fast speed of recognition so we have to measure the higher similarity between the signature sample with greater accuracy and less time consumption by using different methods to find the accurate similarities.

REFERENCES

[1]. A. C. Ramachandra, J. S. Rao, K. B. Raja, K. R. Venugopal, and L. M. Patnaik, "Robust Off-line Signature Verification Based On Global Features," IEEE International Advance Computing Conference, pp. 1173-1178, March 2009.

[2]. Luiz S Oliveira, "Signature Verification using Writer-Independent Approach," in Proceedings of International Joint Conference on Neural Networks, pp. 2539-2544, August 2007.

[3]. S. Ghandali and M. E. Moghaddam, "Off-line Persian Signature Identification and Verification Based on Image Registration and Fusion," Journal of Multimedia, vol. 4, no. 3, pp.137-144, June 2009.

[4]. D. Jena, B. Majhi, and S. K. Jena, "Improved Off-line Signature Verification Scheme using Feature Point Extraction Method," Journal of Computer Science, pp. 111-116, 2008.

[5]. V. Nguyen, M. Blumenstein, and G. Leedham, "Global Features for the Off-line Signature Verification Problem," tenth International Conference on Document Analysis and Recognition, pp. 1300-1304, 2009.

[6]. Ahmed, K.; El-Henawy, I. M.; Rashad, M. Z.; Nomir, O., "On-line signature verification based on PCA feature reduction and statistical analysis," *Computer Engineering and Systems (ICCES), 2010 International Conference on* , vol., no., pp.3,8, Nov. 30 2010-Dec. 2 2010.

[7]. Ning-Ning Liu; Yi-Ding Wang, "Fusion of global and local information for an on-line Signature Verification system," *Machine Learning and Cybernetics, 2008 International Conference on* , vol.1, no., pp.57,61, 12-15 July 2008.

[8]. Pal, S.; Chanda, S.; Pal, U.; Franke, K.; Blumenstein, M., "Off-line signature verification using G-SURF," *Intelligent Systems Design and Applications (ISDA), 2012 12th International Conference on* , vol., no., pp.586,591, 27-29 Nov. 2012.

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

[10]. 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, pages 298–306, May 2004.

[11]. 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.

[12]. 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, April 20-22, 2010, pp. 13-19.

[13]. C. Şenol and T. Yıldırım, "Signature Verification Using Conic Section Function Neural Network", Computer And Information Sciences – ISCIS 2005 2005, Volume 3733/2005, pp. 524-532.

[14]. D. Zhang, J. Campbell, D. Maltoni, and R. Bolle. Special issue on biometric systems. IEEE Trans. Systems, Man and Cybernetics - C, 35(3):273–275, August 2005.

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

[16]. 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.

[17]. M. Ferrer, J. Alonso, and C. Travieso, "Offline Geometric Parameters for Automatic Signature Verification Using Fixed-Point Arithmetic", IEEE transactions on pattern analysis and machine intelligence, vol. 27, no. 6, June 2005.

[18]. G. Dimauro, S. Impedovo and G. Pirlo, "Component- Oriented Algorithms for Signature Verification," Int. J. Pattern Recogn. Artif. Intell. , vol. 8, no. 3, 1994, pp. 771-793.

