جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences

Naif Arab University for Security Sciences
Arab Journal of Forensic Sciences & Forensic Medicine
www.nauss.edu.sa
http://ajfsfm.nauss.edu.sa

الجمعية العربية لعلوم الأدلة الجنائية والطب الشرعي
Arab Society for Forensic Sciences and Forensic Medicine

Original Article

Automated Offline Arabic Signature Verification System using Multiple Features Fusion for Forensic Applications

Saad M. Darwish[1], Ashraf M. El-Nour[2*]

[1] *Department of Information Technology, Institute of Graduate Studies and Researches, Alexandria University, Alexandria, Egypt.*

[2] *Departmnet of Forgery and Researches, Forensic Medicine, Ministry of Justice, Alexandria, Egypt.*

Recieved 05 Jan. 2016; Accepted 15 Nov. 2016; Available Online 30 Dec. 2016

Open Access

Abstract

The signature of a person is one of the most popular and legally accepted behavioral biometrics that provides a secure means for verification and personal identification in many applications such as financial, commercial and legal transactions. The objective of the signature verification system is to classify between genuine and forged signatures that are often associated with intrapersonal and interpersonal variability. Unlike other languages, Arabic has unique features; it contains diacritics, ligatures, and overlapping. Because of lacking any form of dynamic information during the Arabic signature's writing process, it will be more difficult to obtain higher verification accuracy. This paper addresses the above difficulty by introducing a novel offline Arabic signature verification algorithm. The key point is using multiple feature fusion with fuzzy modeling to capture different aspects of a signature individually in order to improve the verification accuracy. State-of-the-art techniques adopt the fuzzy set to describe the properties of the extracted features to handle a signature's uncertainty; this work also employs the fuzzy variables to describe the degree of similarity of the signature's features to deal with the ambiguity of questioned document examiner judgment of signature similarity. It is concluded from the experimental results that the verification system performs well and has the ability to reduce both False Acceptance Rate (FAR) and False Rejection Rate (FRR).

Keywords: Forensic Science, Offline Signature, Verification, Fusion; Features Extraction; Arabic Signature.

* Corresponding author: Ashraf M. El-Nour
Email: ashraf20022004@gmail.com

doi: 10.12816/0033136

Production and hosting by NAUSS

نظام تحقق آلي من التواقيع العربية باستخدام مجموعة من الميزات والخصائص الخطية المدمجة للتطبيقات الجنائية

المستخلص

يعد توقيع الانسان من أكثر القياسات البيومترية شيوعا

وانتشارا ويتميز بالمصداقية القانونية وبأنه وسيلة آمنة في التحقق و التعرف على الهوية الشخصية في العديد من التطبيقات الاقتصادية والتجارية و الشرعية. إن الهدف من نظام التحقق من التواقيع هو تصنيف التواقيع إلى صحيحة ومزورة، والتي تكون في الغالب مصاحبه إلى التباين لذات الشخص الواحد أو التباين بين أشخاص مختلفين. وعلى خلاف اللغات الأخرى نجد أن اللغة العربية لها خصائص فريدة ومميزة مثل التشكيل، أدوات الربط، الحروف المتداخلة. ونظراً لغياب الخصائص الخطية الديناميكية أثناء عملية التوقيع فإنه من الصعوبة الحصول على درجة دقة عالية من التحقق. وتعالج هذه الورقة البحثية هذه المشكلة بتقديم طريقة جديدة للتحقق من التواقيع العربية غير المتزامنة. والمفتاح الرئيسي يكون باستخدام مجموعة من المميزات والخصائص الخطية المدمجة مع النموذج الضبابي والتي تستخرج مختلف السمات الخطية للتواقيع المختلفة وذلك من أجل تحسين دقة التحقق. وتتميز هذه الدراسة عن الدراسات السابقة والتي تكيف المنطق الضبابي لاستخراج المميزات والخصائص الخطية لمعالجة عملية عدم التيقن في وصف خصائص التواقيع، بأن النظام المقترح يجلب المنطق الضبابي كذلك لوصف درجة التشابه للمميزات الخطية للتواقيع وذلك لمعالجة الغموض في التواقيع المتشابهة، واتخاذ قرار بشأنها بمعرفة خبراء التزييف والتزوير. وتوضح التجارب المستنتجة كفاءة النظام المقترح حيث أثبتت النتائج التجريبية الأداء الجيد لنظام التحقق وقدرته على تقليل معدل قبول و رفض الخطأ.

الكلمات المفتاحية: الأدلة الجنائية، التواقيع العربية، نظام التحقق، الخصائص الخطية المدمجة، استخراج الخصائص، المنطق الضبابي.

1. Introduction

Today, biometric verification systems are emerging because of their unique features that assist us to recognize people based on the extracted physical (e.g. face, fingerprint, and iris) and behavioral (e.g. voice, keystroke, dynamics, gait and signature) features. The two types of biometric features are hard to be replicated by another individual and they have the capability to reliably discriminate between a genuine person and an imposter [1-2]. These features change over time due to aging and other developmental factors. These features should have specific characteristics such as individuality, stability, satisfactoriness and collectability. Human verification is required for our routine events, especially in the forensic applications and many high-security environments [3].

The handwritten signature is one of the most familiar behavioral attributes for self-verification of identity. The written signature is viewed as the key means of classifying the signer of a written document based on the inherent hypothesis that a person's normal signature changes slowly and is very difficult to erase, alter or forge without detection [4]. In the signature recognition (or identification) problem, a given signature is looked up in the database to establish the signer's identity. The signature verification problem is concerned with determining if a particular signature is genuine or if it is a forgery [5]. In general, it is easier for people to transfer from using the popular pen-and-paper signature to one where the handwritten signature is taken and tested electronically. The recognition of human signature is vital when the focus is on improving the interface between human beings and computers; if the computer is intelligent enough to understand human signature, it will provide a smarter, quicker and more economic way to verify human signatures.

Typically, the signature verification system can be divided into two main classes based on the acquisition of the signature: 1- dynamic or online verification method where the signature is captured during the writing process on a digitizing tablet and stored to a computer to evaluate the dynamic information like writing speed, pressure points, velocity, acceleration and distance travelled etc., to identify a person; 2- Static or offline veri-

fication method that uses a static image of the signature. In this class, information like width, height, aspect ratio, the center of gravity etc., are measured to identify a person [5]. The offline signature verification is more challenging than the online signature verification because the features are extracted from the static 2D image of the signature and it lacks dynamic information [6]. Still, the performance of the offline verification systems is usually lower than the online system; therefore, it needs to be improved. Furthermore, document analysis generally relies on the offline systems, e.g. verification of a check or signed document; so the work suggested in this paper is focused on an offline verification system [4, 7].

Skilled forgeries are made by criminals after reviewing original examples of the signature, trying to reproduce it as closely as possible. This type is the riskiest kind of counterfeiting. Obviously, the problem of signature verification becomes more and more difficult when passing from random to simple and skilled forgeries, the latter being so difficult a task that even human beings make errors in several cases [1, 3]. Real practical problems concerning offline signature verification can be categorized into two main categories: (a) Problems related to the extraction of a signature's fingerprint from the document and (b) problems related to the verification task itself [4-5].

Many previous studies have recommended that design using different classifiers offers balanced information about the patterns to be classified. These studies highlighted that the application of different types of classifiers instantaneously enhanced the verification accuracy [8]. The research results motivate multi-level signature verification, where decisions based on individual signature features are fused. A fuzzy logic inference engine is designed to fuse global features that encode a signature's fingerprint. The three potential levels of biometrics fusion are: (i) at feature extraction level: where the biometric parameters of each different feature are joined to produce a new set of features, (ii) at matching score level: at which the matching scores are acquired from the biometric parameters of each different feature and are fused by different techniques and (iii) at decision level: where the resulting features from multiple biometric data are fused individually to classify either accept or reject [6]. The use of the fuzzy logic inference engine is to overcome the boundary limitations of fixed thresholds and the uncertainties of thresholds for various users, and to have a more human-like output [6].

This paper focuses on the research of an Arabic offline signature verification system, which is still a challenging research topic and relatively less addressed by researchers. The work presented in this study attempts to prove that employing a two-level signature verification apptoach with the help of fuzzy logic as a tool used to fuse extracted features from scanned images of signatures and to handle the inherent existing imprecision of human decision about signatures similarity achieves better identification performance compared to other approaches. One of the reasons for slow advancements in Arabic signature verification is the characteristics of this script, such as cursive characters, that make it more challenging than other languages.

2. Literature Review

Recently, many new techniques have been introduced to verify various types of signatures. These techniques use either a unique single feature (global, local, statistical, geometric, etc.) or a combination of different types of features extracted from the signature images [1-2]. The biometric identification system with information from a single feature extraction method has some limitations in terms of FRR and FAR. These limitations can

be eliminated by fusing two or more features to ensure improved performance [6]. One of the main challenges in off-line signature verification systems is to make them robust against transformation (e.g. rotation, scaling) of signatures. A technique for rotation invariant feature extraction based on a circular grid is proposed by Parodi et al. [9]. Graph metric features for the circular grid are defined by adopting similar features available for rectangular grids, and the property of rotation invariance of the Discrete Fourier Transform (DFT) is used in order to achieve robustness against rotation.

Tan et al. [10] presented an off-line signature verification system that aims at verifying Arabic and Persian signatures based on DWT to extract common features to aid the verification step. The system consists of four steps: preprocessing, signature registration, feature extraction, and signature verification. The system starts with image preprocessing. In this step, the noise is removed to eliminate unwanted information that negatively influences the accuracy of verification and validation. Next, a registration step is performed where the signature is scaled into an appropriate form to gain a better and more accurate result. After that, the shifting operation is invoked using the center of gravity to determine the centric of the signature. After applying shifting operation, the rotation is performed to align the signature to the correct position. The system decreases the number of DWT levels and the amount of required training, with a low FAR and FRR percentage of 10.9%.

An effective offline signature verification using texture and topological features (e.g. baseline slant angle, aspect ratio, the center of gravity of the whole signature image and the slope of the line joining the center of gravities of two halves of a signature image) from signature images is proposed by Jana R et al. [11]. The authors studied an image clustering process based on Euclidian distance approach enabling investigators to handle clusters of different sizes and shapes of signatures. Kisku et al. (2010) attempted to employ Support Vector Machines (SVM) to fuse multiple classifiers for an offline signature system [12]. From the signature images, global and local features are extracted and the signatures are verified with the help of the Gaussian empirical rule, and Euclidean and Mahalanobis distance-based classifiers. SVM is used to fuse matching scores of these matchers. Finally, recognition of query signatures is done by comparing it with all signatures in the database [13]. Furthermore, neural network is utilized by Khalid et al. (2011) as a learning algorithm to build the mapping between signers and their signature's features [8]. Here, the FAR and FRR can be reduced further by increasing the reference sample size and/or the number of features [14].

Alsous et al. (2010) studied the Farsi and Arabic signature recognition and verification problem and introduced an offline method based on genetic algorithm (GA) to increase the accuracy and decrease the running time [7]. After analyzing the structures of typical Farsi signatures, a variety of features are proposed, extracted, and tested to determine a high-performance feature set for signature verifications. In the classification stages, a GA-based method for optimization of linear classifiers is implemented and tested. Researchers started with a simple un-weighted Euclidian distance classifier and continued with a multi-stage one, but the performance was limited.

Recently, the fuzzy inference system has been employed to adjust the weights for the features of each signature as affected by a way that resembles human thinking and allows intermediate values to be defined between similar and non-similar features via partial set membership. For instance, Hanmandlu et al. (2005) pro-

posed another method in which the signature features are fuzzified by an exponential membership function involved in the Takagi–Sugeno (TS) fuzzy model [15]. The authors have also derived two TS models by considering a rule for each input feature in the first formulation (Multiple rules) and by considering a single rule for all input features in the second formulation. Finally, the above study found that the TS model with multiple rules is better than the TS model with the single rule for detecting three types of forgeries; random, skilled and unskilled from a large database of sample signatures in addition to verifying genuine signatures.

The idea of fusing multi-classifiers for online signature verification problems using fuzzy inference was proposed by Khalid et al. (2011) [8]. The system was developed with a robust validation module based on Pearson's correlation algorithm in which more consistent sets of signatures are enrolled. The system incorporated local features based on x, y and pressure signals as well as two global features to provide a more spoof-free system. In most cases, signatures are forged based on shapes, but the time and length of the signatures are not easy to be determined even by experienced forgers. Therefore, the inclusion of the global features is to ensure that the FAR is lower, thereby increasing the performance of the system.

Many researchers examined the importance of features extracted from signatures in relation to the performance of the verification system. For example, Nasiri and Javaheri (2011) extracted control points on the boundary of the signature which clearly show the structural characteristics of a signature [16]. Four types of local features are extracted from these control points that in turn represents the inputs of the fuzzy logic module. According to the output of the fuzzy inference system, the decision is made that the test signature is forged or genuine. However, the efficiency of the algorithm depends on variations between training signatures. So if

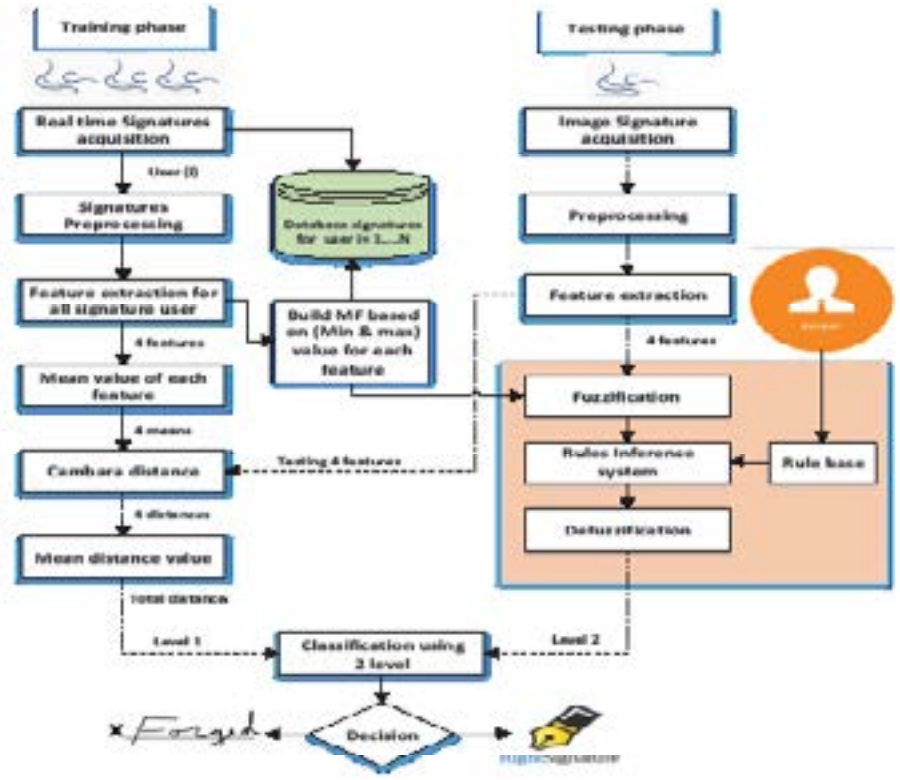

Figure 1- *The proposed Arabic offline signature verification system.*

the training signatures of the specific person are not similar enough to each other, the algorithm cannot have good performance and FAR will grow.

Currently, there is a need to develop an efficient signature verification system for authenticating an individual successfully. The processing of signature strokes is difficult due to highly stylish and unconventional writing styles. The nature and the variety of the writing pen may also affect the nature of the signature obtained. The non-repetitive nature of variation of the signatures because of age, illness, mood, stress levels, geographic location and perhaps to some extent the emotional state of the person, accentuates the problem. All these factors combined cause large intra-personal signature variation. The researcher faces a challenge in designing such a system to counter intrapersonal and interpersonal variations [17].

In this paper, a technique for signature verification is proposed based on shape context that summarizes the global signature features in a rich local descriptor. The proposed system reaches 98 % accuracy and deals with the scalability problems as a result of the correspondence problem between the queried signature and all the data set signatures. To address the scalability problem of using shape context for signature matching, the proposed method enhances the matching stage by representing the shape context features as a feature vector and then applies two levels of classification to assign signatures to their corresponding classes (forged or genuine). The level one verification depends on finding the total difference between the features extracted from the test signature and the mean values of each corresponding features in the training signatures (owning the same signature). Whereas, the level two verification relies on the output of the fuzzy logic module depending on the membership functions that has been created from the signature's features in the training dataset for a specific signer.

3. Proposed System

Off-line signatures are of different shapes and sizes and the variations in them are so immense that it is difficult for a human being to distinguish a genuine signature from a forged one by visual examination. Broadly speaking, signatures can be classified as simple, cursive or graphical based on their shapes. Signatures are behavioral, biometric, evolve over a period of time and are influenced by physical and emotional conditions of the signatories. The suggested system aims to build an intelligent offline Arabic signature verification system by adapting FL framework for multiple signature's fea-

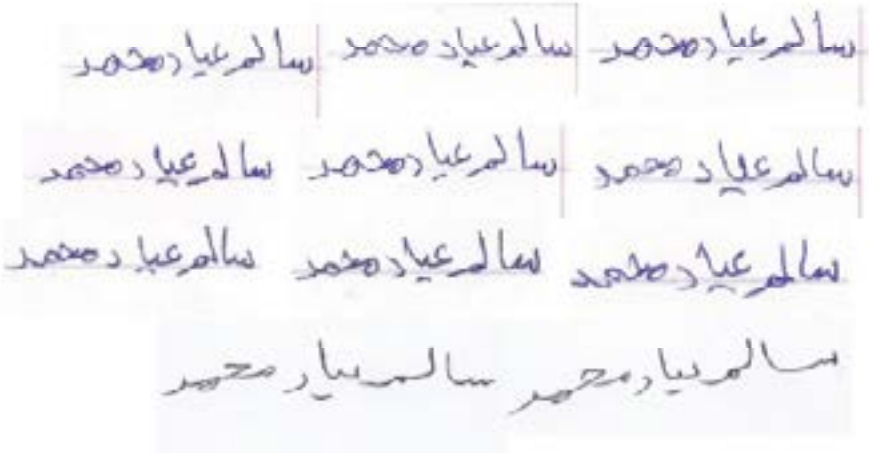

Figure 2- *Sample of individual signatures (Original and Forgery).*

tures fusion. Fuzzy inference is utilized to deal with the vagueness and ambiguity of human judgment of an image's signature similarity.

In general, offline signature verification is a pattern recognition problem and a typical pattern recognition system has the following steps [1, 17]: (i) Data Acquisition – to capture the signature image (ii) Preprocessing – to simplify subsequent operations without losing relevant processing (iii) Feature Extraction - to reduce the data by measuring certain "features" or "properties" (iv) verification – to evaluate the evidence presented in the values of the features obtained from feature extraction and make a final decision for classification (iv) Performance Evaluation – to evaluate the efficiency of the signature verification system. The overall architecture of the suggested verification system is shown in Figure-1 and each step is discussed in detail in the next sections. The advised system has the following properties: (i) adopting the fuzzy language variables to describe the image signature features, so as to infer the image signature as human thinking; (ii) the final decision based on two classification levels that can achieve better precision, since it can model the operation of a human expert.

A. Signature Acquisition

In offline signature verification, an individual person's signatures are taken on A4 size paper and then scanned by a scanner having 300 dpi and stored in Portable Network Graphics format. In the training phase, the database contains signatures from individuals, including genuine signatures and forgeries. Signatures in the training phase (active signatures collected from the signer directly) contain signatures with different angles and scales whether the signer is standing or sitting. The signatures are collected using either black or blue ink with 40 signatures per page. Scanned images are stored digitally for offline processing. In the testing phase, the person's signature is captured from the document in which the validity of the signature on it is disputed. This document is scanned by the same scanner, and the signature is later separated for preprocessing (i.e. the document image is cropped to the bounding rectangle of the signature). Figure-2 shows some samples of signatures from a database according to the suggested technique that has been tested.

B. Signature Preprocessing

The preprocessing stage is implemented both in the training and testing phases. The signature images need some processing before the application of any verification technique. In this stage, signatures are made standard and ready for feature extraction. The preprocessing stage follows seven steps [18-21]:

1. Grayscale conversion: Since the verification system is concerned only with the signature pattern and not in its color, therefore, color information is inappropriate. That is why a color signature image is converted into a grayscale image.

2. Binarization: The grayscale signature is treated by a histogram-based binarization to produce a binary image that contains only 0's and 1's.

3. Noise reduction: Once the original image is binarized, the next step is to remove the noise from signature image caused during scanning (extra pen dots other than a signature) via median filtering method.

4. Image cropping: The binary image is segmented from the background to remove the white space surrounding the signature using the segmentation method of vertical and horizontal projections.

5. Rotation and width normalization: The cropped image is scaled using bi-cubic interpolation to a constant width, keeping the aspect ratio fixed. Normally,

any person while writing his signature uses an arbitrary baseline. The positional information of the signature is normalized by calculating an angle θ about the centroid (x,y) such that rotating the signature by θ brings it back to a uniform baseline. The size normalization in offline signature verification is important because it establishes a common ground for image comparison. Taylor's maximization is used for normalization.

6. Thinning: The goal of thinning is to remove the width variances of the pen and paper by constructing the image one pixel wide. The aim of thinning is to diminish the character features to assist in feature extraction and classification.

7. Skeletonization: This is used to eliminate certain foreground pixels from the binary image so the outcome is a representation of a signature pattern by a group of thin arcs and curves.

The result of the preprocessing phase is a noise free, resized, binarized, thinned image.

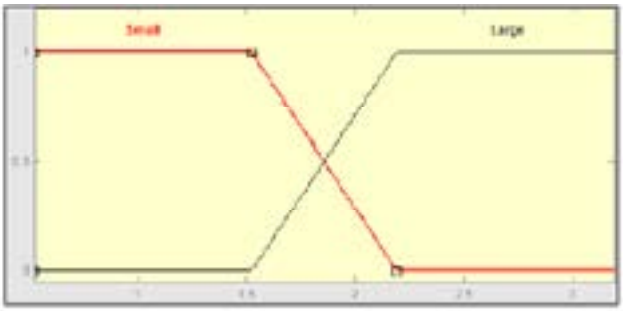

Figure 3- *Membership function for input features.*

C. Features extraction

After the signatures have been attained and preprocessed, the next step is to mine discriminant features from the signature images. When parameter features are utilized, the signature is described as a vector of elements, each one descriptive of the value of a feature. Usually, the success of a signature verification system is critically subject to feature extraction. A perfect feature extraction technique mines a minimal feature set that makes the most of the inter-personal distance between signature examples of various persons while reducing intrapersonal distance for those belonging to the same person. Parameters are generally classified into two main categories, global and local [1, 18].

Global features label the signature image as a whole like length, width, density, edge points of the signature and wavelet transforms. These features are less sensitive to noise and signature variations. Therefore, it will not give us a high accuracy for skilled forgeries, but it would be suitable for random forgeries and it is better to be combined with other types of features [2, 5-6]. Local parameters concern features extracted from specific parts of the signature (pixel-oriented parameters) which are extracted at the pixel level (i.e., grid-based information, pixel density, gray-level intensity, texture, etc.). A suitable combination of global and local features will produce more distinctive and effective features, and the idea of localizing global features will allow the system to avoid the major drawbacks of both and the advantages of both can be exploited [6-11].

The suggested system uses the idea of features combination in a new vision by adapting the fuzzy concept to introduce fuzzy rules in order to combine global and local features. Regarding the local features, a circular chart enclosing the signature is partioned into identical sectors, and graphometric features are computed for each sector. Since dimensions of signatures belonging to different writers, or even the same writer, may differ, a width normalization of the signature image is performed before gridding. This normalization maintains the original height-to-width ratio of the signature image. The circular grid is centered at the center of mass of the binary image of the signature. Features that will be extracted and used for the signature verification are given below

as they are found to be better than other features in distinguishing the variations [9, 18, 20, 22-24]:

1. Aspect ratio (global feature): the ratio of width to height of the signature. The bounding box coordinates of the signature are determined and the width and height are computed using these coordinates.

2. Normalized area (global feature): the ratio of the area occupied by signature pixels to the area of the bounding box.

3. Pixel density distribution (local feature): the ratio of the number of black pixels in the sector within the circular grid to the total number of pixels inside the sector.

4. Gravity center distance (local feature): the ratio of the distance between the gravity center and the center of the grid to the radius of the grid calculated as the major distance between extreme points of the signature.

After generating features vector for each signature in both the training and testing phases, the proposed system uses these features as follows:

1- For all signatures related to a specific signer in the training phase, the features vector is utilized to build the membership function for each feature according to the minimum and maximum values of that feature. These membership functions are used later in the testing phase to fuzzify the extracted features from the test image signature within the fuzzy logic module that is used to fuse different features in a unified framework for level 2 classification. Herein, the aim of using fuzzy logic is to handle the inherent existing imprecision of human decision about the appearance of signature features.

2- At test phase, the feature vector which is extracted from the test's image signature is used to find the distance (Canberra Distance) between this vector and the average values of the extracted features for the same signer for all signatures within the database of the signatures of this person. This outcome describes the extent of deviation of this signature from it's total signatures within the database, which will be used in level 1 classification that will be explained later.

D. Building fuzzy inference system

As there are complex deviations in the feature elements of each signature in order to match a specific signature with the database, the system needs to fuzzify the features [25-26]. This approach uses the Mamdani model for fuzzy analysis that is implemented for level 2 classification. The proposed system has combined the structural parameters of the signatures to take into account the local variations in the signature characteristics resulting from different signing styles of the user. Each feature is fuzzified by a trapezoidal Membership Function (MF). The parameters for the MFs are obtained by training the system with the genuine signatures of the user. During training, the parameters are tuned iteratively in order to minimize the mean square error of the output of the TS model. The Mamdani method is widely used because it is intuitive and suitable for subjective input and output [8, 15]. Two fuzzy variables including 'small', and 'large' are used to describe the global and local feature variation. Their respective MFs are trapezoidal function as illustrated in Figure-3.

Once the system obtains the fuzzy explanations of the signature features, the rule base (fuzzy reasoning) can be constructed to create an interpretation of their similarity. Fuzzy reasoning, which is formulated by a group of fuzzy IF–THEN rules, presents a degree of presence or absence of association or interaction between the elements of two or more sets. In the proposed system, reasoning is carried out through the following rules:

Rule 1- If f1, f2, f3 and f4 are small then output is small = Accept (Genuine)

Rule 2- If f1 is large and f2, f3 and f4 are small then

output is small = Accept

Rule 3- If f1 and f2 are large and f3 and f4 are small then output is small = Accept

Rule 4- If f1, f2 and f3 are large and f4 is small, then output is large = Reject (Forgery)

Rule 5- If f1, f2, f3 and f4 are Large then output is large = Reject

Rule 6- If f1 and f2 are large and f3 and f4 are small then output is small = Accept

Rule 7- If f1, f3 and f4 are small and f2 is large then output is small = Accept

Rule 8- If f1, f2, f3 and f4 are small then output is small = Accept

Rule 9- If f1 and f2 are small and f3 and f4 are large then output is small = Accept

Rule 10- If f1, f2 and f3 are large and f4 is small then output is large = Reject

Rule 11- If f1 and f2 are large and f3 and f4 are small then output is small =Accept

Rule 12- If f1 is small and f2, f3 and f4 are large then output is large = Reject

Rule 13- If f1, f3 and f4 are large and f2 is small then output is large = Reject

Rule 14- If f1, f2 and f4 are large and f3 is small then output is large = Reject

Rule 15- If f1, f2 and f3 are large and f4 is small then output is large = Reject

Rule 16- If f1, f2, f3 and f4 are large then output is large = Reject

The numerical parameters of MF are determined based on mean and standard deviation of features of training signatures. The sixteen rules altogether deal with the weight assignments impliedly in the same way as humans experience thinking. The fuzzy inference processes all of the cases in a parallel manner, which makes the decision more reasonable. The output of the fuzzy system is the similarity between the scanned signature for a specific signer and the stored signatures for him in the training database. The output is also described by two fuzzy variables, including 'accept' and 'reject' with trapezoidal MFs. The outputs of fuzzy values are then defuzzified to generate a crisp value for the variable. The most popular defuzzification method is the centroid, which calculates and returns the center of gravity of the aggregated fuzzy set [8].

E. Verification

This is the final phase where the tested input signature is verified against the sample signature stored in the database. The proposed system performs this using two levels of verification (classification). After that, the final decision is based on the combination of two classifiers to determine whether the signature belongs to the genuine class or to the forgery class.

Table 1- *Comparison of the verification results.*

Classifier	FRR	FAR	Accuracy
Neural Network	0.24	0.18	79%
Support vector machine	0.10	0.15	83%
Fuzzy-based classifier	0.09	0.11	91%
Two levels classifier	0.02	0.05	98%

Level 1 verification: Level one verification depends on finding the total difference between the features extracted from the test signature and the mean values of each corresponding feature in the training signatures (owning the same signature). At training phase, the mean value of each feature from the signature features vector for all stored signatures is computed, resulting in a vector with four elements where each element Mfi represents the mean of the corresponding feature (i=1…,4). After that, the Canberra distance between this calculated vector and the features vector predefined in the test phase is measured. The rationale of choosing this measure is that it considers not only the distance between two points but also their relation to the origin (i.e. more precise measure). If the output values of the distance then the signature is genuine.

Level 2 verification: Level two verification relies on the output of the fuzzy logic module depending on the membership functions (see subsection D) that has been created from the signature's features in the training dataset for a specific signer. In this case, the fuzzy module acts as a fusing tool to merge different features that is used as a component with the rest of the fuzzy logic components to form a classifier. If the output of fuzzy classifier is defuzzified then the signature is genuine.

Subsequently, the results of the two classifiers are combined. The final rule to make a decision about a signature case is given as: If and then the signature is genuine. Otherwise, the signature is forged. Herein, the system gets a total of 4 features based on the signature's global and local aspects that helps to classify the signature as fake or original.

4. Experimental Design

In order to test the efficiency and validity of the proposed system, the system by MATLAB language and credit the verification rules in C# language was implemented. The prototype verification technique in a modular fashion was built and it was implemented and tested using a DELL PC machine which had the following features: Intel (R) Core (TM) i5-2450M CPU @ 2.50GHz, and 4.00GB of RAM, 64-bit Windows 8 Pro. In this work, 40 signature images were used in the training phase, and one historical signature image was used for testing purposes. FAR and FRR were the two parameters used for measuring performance of any signature verification method. FAR, which means a fake signature, is considered as a real signature when the total number of fake signatures accepted by the system with respect to the total number of comparisons made. FRR, which means a real signature, is considered as a fake signature when the total number of original signatures rejected by the system with respect to the total number of comparisons made [1, 17].

5. Results and Discussion

The first set of experiments was performed to compare the verification performance of the proposed system that employs two verification levels: distance-based and fuzzy-based verification with conventional signature verification classifier using SVM [19], NN [14] and fuzzy logic [26] using the same features. In the method described by Singh and Patel (2013), each feature is fuzzified using the TS model [26]. Rules are written in fuzzy inference system to accept only true signatures based on mean and variance values of the angle calculated for each image. The rules are combined to accept only true signatures and reject the forgery. Table-1 illustrates the comparison between the systems. The results of the present study revealed that the use of two levels of verification generates a further verification rate improvement (accuracy) of 7–20%. The proposed tech-

nique has the lowest FAR percentage when compared to other methods. The performance improvement comes from the correct verification of signatures because of using fuzzy variables to describe degree of similarity of signature features along with the traditional feature similarity distance classifiers.

The second set of experiments was conducted to determine the capability of the introduced system to verify signature data from multiple scripts. This is so because the proposed system requires no language-specific geometrical analysis (i.e. text-independent) in contrast to many presented systems that need connected component analysis to extract allographic features. For English signatures, verification moves towards 100%. Nevertheless, it seems that the results obtained on Arabic script are somewhat lower than the ones obtained on the Western script. A possible explanation for the difference is that there seems to be more style variation across individuals in English signatures compared to Arabic ones. Automatic signature verification on Arabic script appears to be more difficult.

The last set of experiments was performed to show how the verification rate of the proposed system depends on the number of signatures per signer because if the signer has more enrolled samples, the chance of a correct hit increases. The maximum allowed limit of sample signatures is 40 per signer. If the number of sample signature is above 40 then the returns in performance are however diminishing for every new sample added due to the increase of intraclass signer's variability. As expected, the verification rate decreases as the number of signatures grows as a result of the decrease in inter-class writer's variability. Accuracy rate drops approximately by 2–5% for every doubling of the number of signatures in the dataset after 40 samples.

6. Conclusion and Future Work

In this paper, an adaptive method for signature recognition is introduced. Also, the problem of fake signature verification in off-line systems is tackled using two levels of verification based on similarity distance and fuzzy concepts in the decision-making process. In the beginning, the signature database is described then preprocessing steps and feature extraction for the verification process are examined. An appropriate mixture of global and local features is utilized to yield more distinctive and effective features by merging the advantages of both. A verification technique is developed based on a multi-classifier. One of them depends on similarity distance between the feature vectors in which the distances between the feature vector of the input signature and the mean of each signer signatures in the database are calculated and matched. The other classifier relies on fuzzy concepts where a set of fuzzy rules is used to make a decision with a degree of certainty.

Representing signature image by using feature fusion method has several advantages which are as follows: 1- It is a compact coding technique. 2- It is a general application, meaning that it can be applied for any signature shape. 3- It is simple meaning, that can be used to code the signature straightforward and fast; most of them can be executed in fractions of a second on commercially available equipment. 4- The operation of extracting 4-tuple feature vector is very active to remove all noise in the signature template. The experiments resulted in a verification rate of 98%.

Carefully chosen discriminating features of signatures combined with the use of two verification levels made the proposed system more powerful compared to other existing systems both in terms of success ratio and ease of implementation and optimized run time.

Future work includes the examination of different

features to enhance the performance of the system.

References

1. Al-Omari YM, Abdullah SN, Omar K. State-of-the-art in offline signature verification system. In Pattern Analysis and Intelligent Robotics (ICPAIR), 2011 International Conference on IEEE. 2011;1:59-64.
2. Prashanth CR, Raja KB, Venugopal KR, Patnaik LM. DWT based Offline Signature Verification using Angular Features. Int J Comput Appl 2012;52.
3. Prashanth CR, Raja KB, Venugopal KR, Patnaik LM. Intra-modal Score level Fusion for Off-line Signature Verification. Int J Inno Tech Exp Eng 2012;1:179-87.
4. Justino EJ, Bortolozzi F, Sabourin R. Off-line signature verification using HMM for random, simple and skilled forgeries. In Document Analysis and Recognition, 2001. Proceedings. Sixth International Conference on IEEE 2001:1031-34
5. Jena D, Majhi B, Panigrahy SK, Jena SK. Improved offline signature verification scheme using feature point extraction method. In Cognitive Informatics, 2008. ICCI 2008. 7th IEEE International Conference 2008:475-480.
6. Ravi J, Raja KB. Concatenation of Spatial and Transformation Features for Off-Line signature Identification. Int J Inno Technol Exp Eng 2012:2278-3075.
7. Alsous E., Nezam F., Monadjemi S.A., Neamatbakhsh N. A Novel GA Based Approach to Farsi and Arabic Signature Verification," IRECOS 2010; 5: 44-51.
8. Khalid M, Yusof R, Mokayed H. Fusion of multi classifiers for online signature verification using fuzzy logic inference. Int J Innov Comput Inf Control 2011;7:2709-26.
9. Parodi M, Gomez JC, Belaïd A. A circular grid-based rotation invariant feature extraction approach for off-line signature verification. In 2011 International Conference on Document Analysis and Recognition 2011:1289-1293.
10. TAN X, JAAFAR AA, YAHYA A, AHMAD R, ZAIN A, SALMAN M, YONG L, DING F, SUPRIYANTO C, BASUKI RS, SHIDIK GF. Off-line signature verification system based on dwt and common features extraction. J Theor Appl Inf Technol 2013;51.
11. Jana R, Saha R, Datta D. Offline signature verification using Euclidian distance. Int J Comp Sci Inf Technol 2014;5:707-10.
12. Kisku DR, Gupta P, Sing JK. Offline signature identification by fusion of multiple classifiers using statistical learning theory. arXiv preprint arXiv 2010:1003;5865.
13. Özgündüz E, Şentürk T, Karslıgil ME. Off-line signature verification and recognition by support vector machine. InSignal Processing Conference, 2005 13th European 2005:1-4.
14. Shikha P, Shailja S. Neural Network Based Offline Signature Recognition and Verification System. Res J Eng Sci 2013;2:11-5.
15. Hanmandlu M, Yusof MH, Madasu VK. Off-line signature verification and forgery detection using fuzzy modeling. Pattern Recognit 2005;38:341-56.
16. Verma AC, Saha D, Saikia H. Forgery Detection in Offline Handwritten Signature Using Global and Geometric Features. IJCER 2013;2:182-8.
17. Impedovo D, Pirlo G. Automatic signature verification: the state of the art. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). 2008;38:609-35.
18. Roy S, Maheshkar S. Offline signature verification using grid based and centroid based approach. International Journal of Computer Applications. 2014;86.
19. Mohammadzade M, Ghonodi A. Persian off-line

signature recognition with structural and rotation invariant features using by one-against-all SVM classifier. JACR 2013;4:87-96.

20. Khan S, Dhole A. An Offline Signature Recognition and Verification System Based on Neural Network.
21. Kumar S, Raja KB, Chhotaray RK, Pattanaik S. Offline signature verification based on fusion of grid and global features using neural networks. Int j eng sci technol 2010;2:7035-44.
22. K. Adhikary, and A. Kumar, "Proposal for Verification Using Neural Network", Global J Comp Sci Technol 2011; 4: 717-20.
23. Ahmed SM. Off-line Arabic signature verification using geometrical features. InWIAR'2012; National Workshop on Information Assurance Research; Proceedings of VDE 2012:1-6.
24. Vélez J, Sánchez Á, Moreno B, Esteban JL. Fuzzy shape-memory snakes for the automatic off-line signature verification problem. Fuzzy Set Syst 2009;160:182-97.
25. Nasiri M, Javaheri A. A fuzzy approach for the automatic off-line persian signature verification problem. In 2011 7th Iranian Conference on Machine Vision and Image Processing IEEE 2011:1-5.
26. Singh P, Patel R. Offline signature verification using fuzzy logic. signature 2013;1.