

Distance and Fuzzy Classifiers Alliance: The Solution to Off-line Arabic Signature Verification System for Forensic Science

Saad Mohamed Darwish^{a*}, Zainab H Noori^b

^a Department of Information Technology, Alexandria University Egypt

^b Department of Information University of Babylon-Iraq

¹ saad.darwish@gmail.com*

* corresponding author

ARTICLE INFO

Article history:

Received: 2018-05-11

Revised: 2018-07-16

Accepted: 2018-08-03

Keywords:

Offline signature,
verification system,
global and local feature fusion,
fuzzy logic approach

ABSTRACT

Signature of a person is one of the most popular and legally accepted behavioral biometrics that provides 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 forgery that is 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 writing process, it will be more difficult to obtain higher verification accuracy. This paper addresses the above difficulty by introducing a novel Off-Line Arabic signature verification algorithm. Different from state-of-the-art works that adopt one-level of verification or multiple classifiers based on statistical learning theory; this work employs two-level of fuzzy set related verification. The level one confirmation depends on finding the total difference between the features extracted from the test signature and the mean values of each corresponding elements in the training signatures (owning the same trademark). Whereas, the level two verification relies on the output of the fuzzy logic module depending on the membership functions that have been created from the signature features in the training dataset for a specific signer. It is concluded from the experimental results that the verification system performs well and can reduce both False Acceptance Rate (FAR) and False Rejection Rate (FRR).

Copyright © 2017 International Journal of Artificial Intelligence Research.

All rights reserved.

I. Introduction

Today, biometric verification systems are emergent because of their unique features that assists us to recognize people based on the extracted physical (e.g., Face, fingerprint, and iris) Behavioral (e.g., Voice, body odor, and signature) features. The two types of biometric features are hard to be replicated by another individual, and they can reliably discriminate between a genuine person and 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, collectability, and the charge to hire any biometric. Human verification is required for our routine events, especially in the forensic applications and many high-security environments [3].

However, the handwritten signature is one of the most natural behavioral attributes for self-verification of the person. The written name is viewed as the critical means of classifying the signer of a written document based on the fundamental assumption that a person's regular surname changes little by little and is very problematic to remove, modify or fake without revealing[4]. The signature verification problem is connected with determining if a specific signature is genuine or if it is a forgery [5]. In general, it is easier for people to transfer from using the personal pen-and-paper signature to one where the handwritten signature is booked and verified electronically. The

recognition of human name is vital when the focus is on improving the interface between human beings and computers; if the machine is intelligent sufficient to comprehend human name, it will deliver a smarter and economic man-computer interface.

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 off-line verification method that uses a static image of the signature. In this class, the information like width, height, aspect ratio, the center of gravity, etc., are measured to identify a person [5]. The off-line signature verification is more challenging than the on-line signature verification since the features are mined from the stationary 2D image of the signature and shortages of dynamic information [6]. Still, the performance of the off-line verification systems is usually lower than the on-line. Therefore it would be an excellent challenge to improve it.

Furthermore, document analysis generally relies on the off-line systems, e.g., verification of a check or signed document; so the work suggested in this paper is focused on an off-line verification system [4] [7]. The problem of signature verification turns out to be more and more challenging when departing from random to skilled and straightforward forgeries, the latter being so tricky job that even human beings create mistakes in several circumstances [1][3]. Real practical problems concerning off-line signature verification can be categorized into two main classes: (a) those related to the drawing out of signature's fingerprint from the document and (b) problem related to the verification task itself [4][5].

Many studies have been made which recommended that design using different classifiers offers to balance information about the patterns to be classified and 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 combine global functions that encode the signature's fingerprint. The three potential levels of biometrics fusion are: (i) *at feature extraction level*: The different features biometric parameter are joint to produce new set of features, (ii) *at matching score level*: The matching scores are acquired from different functions biometric parameter and are fused by various techniques and (iii) *at decision level*: The resulting elements from multiple biometric data are combined individually to classify either accept or reject [9]. The use of the fuzzy logic inference engine is to overwhelm the borderline limits of fixed thresholds and sweep away the uncertainties of thresholds for many users and to have a more human-like outcome [9].

This paper focuses on the research of Arabic offline signature verification system, which still is a challenging research topic and relatively less touched by researchers. The work presented in this study tries to prove that employing a two-level of signature verification 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 cursively that makes it more challenging than other languages. This paper is organized as follows. Section 2 introduces the related work. Chapter 3 shows the architecture of the proposed signature verification system. Chapter 4 shows experimental results and comparison between associated tasks and the proposed method. Section 5 summarizes the conclusion and outlines the future work.

II. Method

Recently, many approaches were introduced to verify types of signatures. These techniques utilize either a kind of feature (global, local, statistical, geometric, etc.) or a mixture of different kinds of functions, mined from the signature images [1][2]. The biometric identification system with information from a single feature extraction method has some limitations regarding FRR and FAR. These limitations can be eliminated by fusing two or more features to ensure an improved performance [9]. One of the main challenges in off-line signature verification systems is to make them robust against transformation (e.g., rotation, scale) of the signatures. A technique for rotation invariant feature extraction based on a circular grid is proposed in [10].

The authors in [11] recommended an off-line signature verification scheme that targets at authenticating Arabic and Persian signatures depend on the Discrete Wavelet Transform (DWT) to extract standard characteristics to help the verification step. The system reduces the number of DWT levels and the number of prerequisite training, with a low FAR and FRR percentage of 10.9%. The work in [12][13] studied an image clustering process based on Euclidian distance approach enabling to handle clusters of different sizes and shapes of signatures. While the work presented in [14] tried to hire Support Vector Machines (SVM) to mix different classifiers for an offline signature system. From the signature images, global and local properties are extorted, and the signatures are confirmed with the aid of Gaussian, Euclidean, and Mahalanobis distance-based classifiers.

Furthermore, the neural network is applied in [15] as a learning algorithm to form the mapping between signers and their signature's features. Here, the FAR and FRR can be compact further by increasing the reference sample size and also the number of elements. Researchers in [7] 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. In the classification stages, a GA-based method for optimization of linear classifiers is implemented and tested.

Recently, the fuzzy inference system is employed to adjust the weights for each signature features as affected by a way that resembles human thinking and allows intermediate values to be defined between similar and not similar via partial set membership. For instance, in [16] the signature features are fuzzified by an exponential membership function involved in the Takagi–Sugeno (TS) fuzzy model. The idea of fusing multi-classifiers for online signature verification problem using fuzzy inference was investigated in [8][17].

However, the efficiency of the algorithm depends on variations between training signatures so if the training signatures of the specific individual are not sufficiently analogous to each other, the algorithm cannot have good performance and FAR will raise. Lately, the researcher admits a challenge in designing such a system to refute intrapersonal and interpersonal variations [18]. In this paper, a technique for signature verification is proposed based on shape context that encapsulates the global signature features in a dominant local descriptor. The proposed system touches 98 % accuracy and handles the scalability problems as a result of the matching problem between the inquired signature and all the dataset signatures. To tackle the scalability problem of using shape perspective for signature matching, the proposed method improves the matching stage by signifying the shape context features as a feature vector and then utilizes two level of classification to allocate signatures to their matching classes(forgery or genuine). The official one verification depends on finding the total difference between the features extracted from the test signature and the mean values of each corresponding element in the training signatures (owning the same trademark). Whereas, the level two verification relies on the output of the fuzzy logic module depending on the membership functions that have been created from the signature' features in the training dataset for a specific signer.

III. Result

Off-line signatures are of different shapes and sizes, and the variation in them is so immense that it is difficult for a human being to discriminate a genuine name from a fake one by having a fleeting look at the title. Generally, signatures can be categorized as simple, cursive or graphical based on their contours. Signatures are behavioral biometric, alter more than a period and are influenced by physical and sentimental states of the applicants. The suggested system purposes to build an intelligent offline Arabic signature verification system by adapting the FL framework for multiple classifiers fusion.

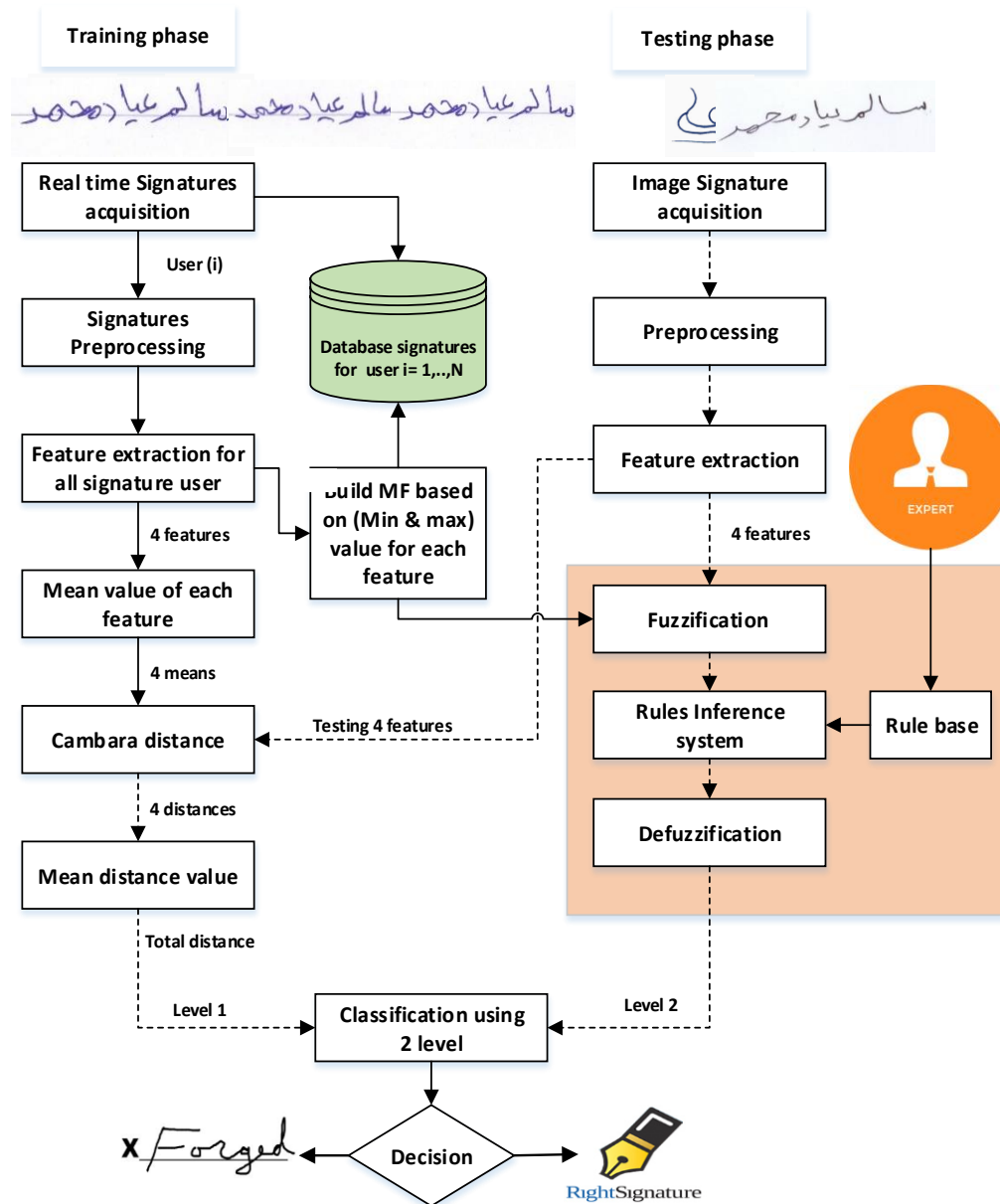


Fig. 1. The proposed Arabic offline signature verification system.

Generally, offline signature verification and authentication is a pattern recognition problem and a standard pattern recognition structure has the following phases [1][18]: (i) Data Acquisition – to catch the signature image (ii) Preprocessing – to make easier succeeding processes without missing significant processing (iii) Feature Extraction - to diminish the data by assessing specific features (iv) Verification – to evaluate the indication postured in the values of the elements attained from feature extraction and produced a conclusion for classification (iv) Performance Evaluation – to estimate the productivity of the signature verification system. The overall architecture of the suggested verification system is shown in Fig.1, and each step is discussed in details 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 human expert.

1) Signature Acquisition

In offline signature verification, distinct person's signatures are booked on A4 size paper and then scanned through a scanner with 300dpi and deposited in Portable Network Graphics (PNG) format. In the training phase, the database encompasses signatures from persons, including genuine signatures and forgeries. Names in the training phase (actual signatures collected from the signer

directly) containing signatures with different angles, and scales whether the signer is standing or sitting. The stamps are composed using either black or blue ink with 40 names per page. Scanned images are warehoused digitally for offline processing. In the testing phase, the person's name is captured from the document in which the validity of the signature in it be disputed. The same scanner scans this document, and later the stamp is separated for preprocessing (i.e., the document image is cropped to the bounding rectangle of the name). Fig.2 shows some samples signatures from the dataset that has been trained and tested on the proposed system

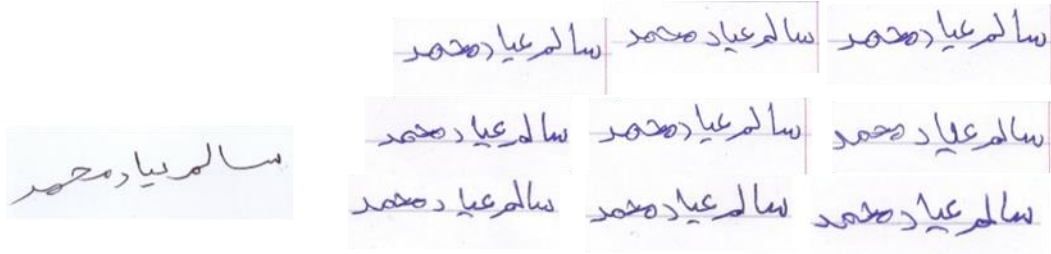


Fig. 2. A sample of individual titles (a) Forgery and (b) Genuine

2) Signature Preprocessing

The preprocessing stage is implemented both in the training and testing phases. The signature images need some handling before the application of any verification technique.

In this stage, signatures are made standard and ready for feature extraction. The preprocessing stage follows seven stages [19-22]:

- Grayscale conversion:** Since the verification system is concerned only with the signature pattern and not in its color, color information is inappropriate. That is why a color signature image is converted into a grayscale image. Besides reducing the calculations on the gray pictures
- Binarization:** The grayscale signature is treated by a histogram-based binarization to produce a binary image that contains only 0's and 1's.
- 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.
- Image cropping:** the binary image is isolated from the background to eliminate the white space nearby the signature by the segmentation technique of vertical and horizontal projections.
- Rotation and width normalization:** The cropped image is scaled using bi-cubic interpolation to a constant width, preserving the aspect ratio fixed. Usually, any person while stroking his signature uses a subjective baseline. The positional information of the name is standardized by computing an angle θ about the centroid (x,y) such that rotating the name by θ carries it back to a stable baseline. The size normalization in offline signature verification is vital because it forms a common ground for image comparison. Taylor's maximization is used for normalization.
- Thinning:** The goal of thinning is to remove the width variances of the pen by constructing the image one pixel thick. The aim of this is to diminish the character features to assistance in feature extraction and classification.
- Skeletonization:** is used to remove particular foreground pixels from the binary image. So the result is a depiction of a signature pattern by a collection of thin arcs and curves. The effect of the preprocessing phase is a noise-free, resized, binarized, thinned image.

3) Features extraction

After the signatures have been attained and pre-processed, the next step is to mine discriminant features from the signature images. When parameter features are utilized, the name is described as a vector of elements, each one descriptive of the value of a function. Usually, the success of a signature verification system critically is subject to feature extraction. A perfect feature extraction technique mines a minimal feature set that makes the most of the interpersonal distance between

signature examples of various persons while reducing intrapersonal gap for those belonging to the same person. Parameters are generally classified into two main categories global and local [1] [19].

Global features tag the signature image as a whole like a length, width, density, edge points of the signature and wavelet transforms. These features are less subtle to noise and signature differences. So it will not offer us a high accuracy for skilled counterfeits, but it would be appropriate for arbitrary forgeries, and it's better to be joint with other types of features [2][5][6]. Local parameters concern features extracted from specific parts of the signature (pixel-oriented parameters) which are obtained 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 compelling features, and the advantages of both can be used [9-11]. The suggested system uses the idea of features combined in a new vision by adapting the fuzzy concept to introduce fuzzy rules to combine global and local elements. Elements that will be mined and utilized for the signature verification are provided below as they are realized to better than other factors in distinguishing the variations.

Regarding the local characteristics, a circular chart enclosing the signature is divided into identical sectors, and pixel density with gray-level intensity features are computed for each segment [10]. The circular grid is centered at the center of mass of the binary image of the signature. In this case, the sector with the highest features values regarding pixel density and gray-level intensity will be selected to represent the local features of the stamp. The chief motivation behind the use of a signature circular grid is to divide the name into local regions or sectors which over a set of all samples of a writer form a fuzzy set. In this way, the system can capture the global behavior through the local features, which create an intelligent. The knowledge base of unique features for a particular individual. The other motivation for designing the grid is to reduce the area of focus to just the signature image.

F₁: Aspect ratio (global feature): the ratio of width to height of the signature. The bounding box coordinates of the name are defined, and the width and height are calculated using these coordinates.

F₂: Normalized area (global feature): the ratio of the space occupied by signature pixels to the area of the bounding box.

F₃: Pixel density distribution (local function): the ratio of the number of black pixels in the sector within the circular grid to the total number of pixels inside the industry.

f₄: 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 network calculated as the significant distance between extreme points of the signature.

After generating features vector for each signature in both training and testing phase; the proposed system uses these features as follows: (1) for all trademarks related to 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 elements 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) Attest phase, the feature vector that 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 trademarks within the database of the brands of this person. This outcome describes the extent of deviation of this signature from his total names within the database, which will be used in level 1 classification that will be explained later.

4) Building a fuzzy inference system

As there are complex deviations in the feature elements of each signature; thus to match a specific name with the database, the system needs to fuzzify the features [26][27]. 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 care of 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 acquired by training the system with the genuine signatures of the user. During training, the settings

are adjusted iteratively 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 personal input and production [8] [16]. In this, two fuzzy variables including ‘small,’ and ‘large’ are used to describe the local and local feature variation as illustrated in Fig.3.

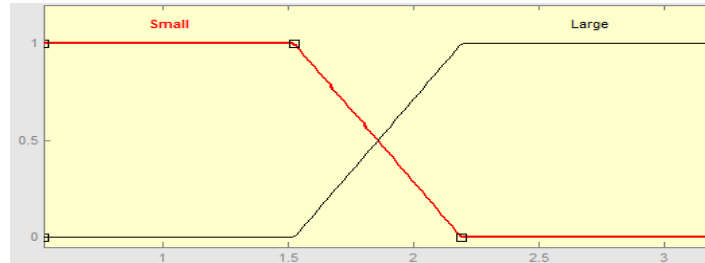


Fig. 3. Membership function for input features

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, offerings a grade of presence or absence of association or relations between the elements of two or more sets. In the proposed system, reasoning is carried out through the following rules that were built by an expert from the Egyptian Ministry of Justice- Department of forgery

Rule 1	IF (f1 is small) and (f2 is small) and (f3 is small) and (genuine)	(f4 is small) THEN (output is small) = Accept
Rule 2	IF (f1 is large) and (f2 is small) and (f3 is small) and (genuine)	(f4 is small) THEN (output is small) = Accept
Rule 3	IF (f1 is large) and (f2 is large) and (f3 is small) and (genuine)	(f4 is small) THEN (output is small) = Accept
Rule 4	IF (f1 is large) and (f2 is large) and (f3 is large) and (Forgery)	(f4 is small) THEN (output is large) = Reject
Rule 5	IF (f1 is large) and (f2 is large) and (f3 is large) and (Forgery)	(f4 is Large) THEN (output is large) = Reject
Rule 6	IF (f1 is large) and (f2 is large) and (f3 is small) and (Forgery)	(f4 is small) THEN (output is small) = Accept
Rule 7	IF (f1 is small) and (f2 is large) and (f3 is small) and (Forgery)	(f4 is small) THEN (output is small) = Accept
Rule 8	IF (f1 is small) and (f2 is small) and (f3 is small) and (Forgery)	(f4 is small) THEN (output is small) = Accept
Rule 9	IF (f1 is small) and (f2 is small) and (f3 is large) and (Forgery)	(f4 is large) THEN (output is small) = Accept
Rule 10	IF (f1 is large) and (f2 is large) and (f3 is large) and (Forgery)	(f4 is small) THEN (output is large) = Reject
Rule 11	IF (f1 is large) and (f2 is large) and (f3 is small) and (Forgery)	(f4 is small) THEN (output is small) = Accept
Rule 12	IF (f1 is small) and (f2 is large) and (f3 is large) and (Forgery)	(f4 is Large) THEN (output is large) = Reject
Rule 13	IF (f1 is large) and (f2 is small) and (f3 is large) and (Forgery)	(f4 is large) THEN (output is large) = Reject
Rule 14	IF (f1 is large) and (f2 is large) and (f3 is small) and (Forgery)	(f4 is Large) THEN (output is large) = Reject
Rule 15	IF (f1 is large) and (f2 is large) and (f3 is large) and (Forgery)	(f4 is small) THEN (output is large) = Reject
Rule 16	IF (f1 is large) and (f2 is large) and (f3 is large) and (Forgery)	(f4 is Large) THEN (output is large) = Reject

The numerical parameters of *MF* are determined based on the mean and standard deviation of features of training signatures. The sixteen rules altogether deal with the weight assignments impliedly in the same way as what 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 production 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 comprehensive defuzzification method is the centroid, which computes the center of gravity of the aggregated fuzzy set [8].

5) Verification

This is the ending stage where the tested input signature is verified against the sample signature deposited in the database. The proposed system performs this using two level of verification (classification) after that the final decision is based on the combination of two classifiers to determine whether the signature belongs to the whole class or the forgery class.

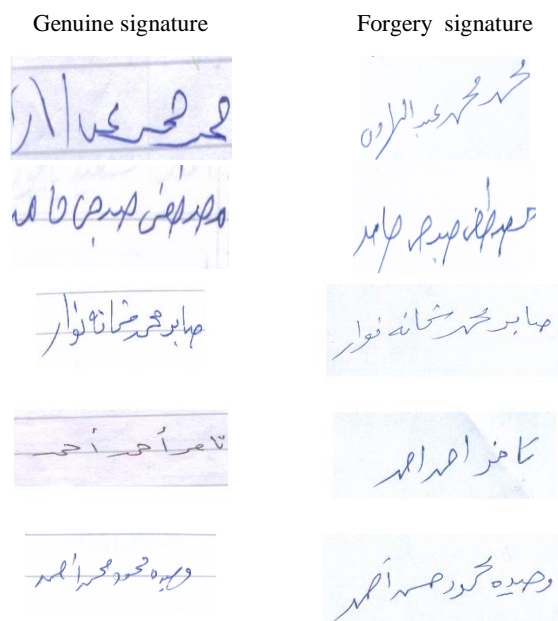
Level 1 verification: level one confirmation depends on finding the total difference between the features extracted from the test signature and the mean values of each corresponding element in the training signatures (owning the same trademark). At training phase, the mean value of each function from the name features vector for all stored names is computed resulting in a vector with four elements where each element M_{fi} represents the mean of the corresponding function ($i=1,\dots,4$). After that, the Canberra distance between this calculated vector and the features vector predefined in the test phase is measured. The rationale for choosing this measure is that it reflects not only the distance between two points but also their relative to the origin (i.e., more accurate test). If the output values of the length (ζ_1) ≤ 0.4 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' features in the training dataset for a specific signer. In this case, the fuzzy module acts as a fusing tool to merge different functions that are used as a component with the rest of the fuzzy logic components to form a classifier. If the output of the fuzzy classifier (defuzzification) (ζ_2) ≥ 0.7 then the signature is genuine.

Subsequently, the results of the two classifiers are combined. The final rule to decide the signature case is given experimentally as **If** $\zeta_1 \leq 0.4$ **and** $\zeta_2 \geq 0.7$ **then** the signature is genuine **else** name is a forgery. Herein, the system gets a total of 4 features based on signature global and local aspect that helps to classify name as fake or original.

6) Experiment Design

To investigate the efficiency and authority of the proposed system, the system was implemented by MATLAB language and credit the verification rules in C# language. The prototype verification technique was built in a modular fashion and has been implemented and tested in a DELL PC machine which has 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 the nature images were used in training phase (4 discriminative features for each signature), and 20 historical signature images were used for testing purposes (10 original names and ten forgery signatures). Fig. 4 shows sample le signatures from 10 individuals under different signature variations. False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the two parameters used for assessing the performance of any signature verification method. FAR which means a fake signature is considered as a real signature is the total number of false name recognized by the system concerning the total number of the comparison made. FRR, which means an actual name is deliberated as a phony signature, is the total number of original surname disallowed by the system concerning the total number of the comparison made.



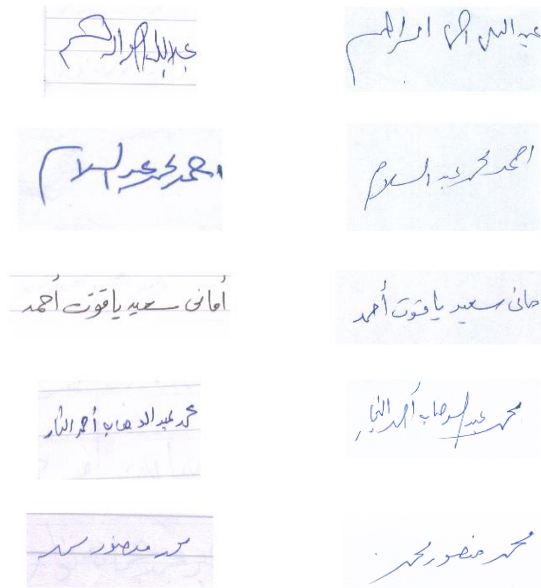


Fig. 4. Signatures samples (genuine and forgery) from 10 individuals

IV. Results and Analysis

The first set of experiments was implemented to match the verification performance of the proposed system that employs two verification levels: distance-based and fuzzy-based verification with traditional signature verification classifier using SVM [20] and NN [15] and fuzzy logic [28] using the same features. In the method in [28], each function is fuzzified using the TS model. Rules are written in fuzzy inference system to accept only correct signatures based on mean and variance values of the angle calculated for each image. The rules are combined such that to accept just exact stamps and reject the forgery. Table 1 illustrates the comparison between the systems. The results reveal that the use of two levels of verification generates a further verification rate improvement (accuracy) of 7–20%. The proposed method has the lowermost FAR percentage when matched to other methods. The performance improvement comes from the accurate verification of signatures because of using fuzzy variables to describe similarity degree of signature features as human thinking; this, along with traditional feature similarity distance classifier.

Table 1. Comparison of the verification results

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

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

Another set of experiments is conducted to test the ability of the suggested system to verify the signature in the presence of low style variation (slight change) across the same individual stamps. Table 2 shows the results across the original tested names, whereas Table 3 displays the results

across the approved forgery signatures. As is evident, the proposed system has a high ability to decrease both of FAR and FRR. However, in some cases and in particular in genuine signatures, the system ability is reduced by a small amount to verify the signatures as illustrated in Table 2. One explanation for this result is the style variations associated with some original names that result in a discrepancy in the extracted features compare with the features that have been used for training; unlike forged signatures that have high style variations with well-trained stamps.

Table 2. Accuracy for style variation across tested genuine signatures

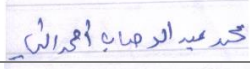
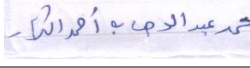
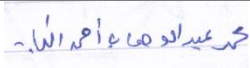
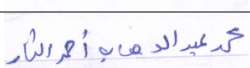
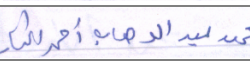

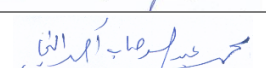
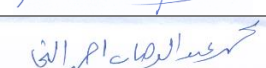
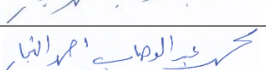
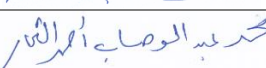
Genuine signature style variations	The value generated by the distance classifier	Value generated by fuzzy classifier	Final decision
	0.1874	1.0141	Accepted
	0.1884	1.0596	Accepted
	0.1581	0.9909	Accepted
	0.3341	0.7476	Accepted
	0.4923	0.8546	Rejected

Table 3. Accuracy for style variations across tested forgery signatures.

Forgery signature style variations	The value generated by the distance classifier	Value created by fuzzy classifier	Final decision
	0.5794	1.7291	Accepted
	0.7032	1.6937	Accepted
	0.3107	1.6877	Accepted
	0.3107	1.6877	Accepted
	0.6382	1.3976	Accepted

In general, the system's ability to determine the skilled forgery signatures is reduced because the system is unable to decide on the clear distinction between the extracted features in both of skilled forgery and original names. This problem can be avoided by increasing the number of elements removed from the names (e.g., Scale-invariant feature transform), which can add another dimension to the distinction between trademarks. But this will be at the expense of the computational time. Concerning with non-skilled names as shown in Fig. 5, the suggested system exhibits a high ability to recognize these signatures. This is due to, in addition to the use of two level of classifiers, the depending on geometric features that describe the particular geometry and topology of a signature thereby preserving both their global as well as local properties. These features have a high tolerance to alterations and style variations, and they can also tolerate a certain degree of translation and rotation variations.

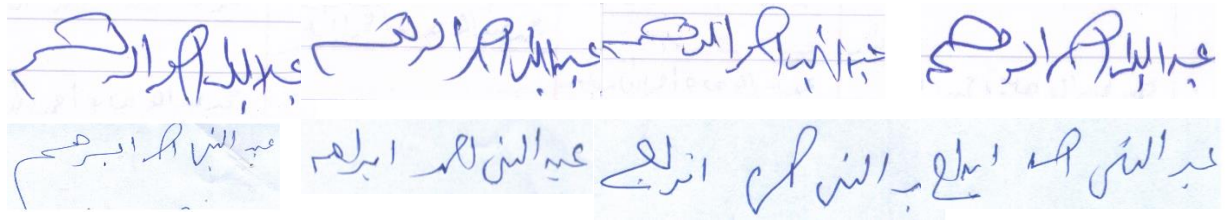


Fig. 5. Some genuine signatures (top) and forged trademarks (bottom) with high style variations.

Despite the adoption of the proposed system on the circular grid technique to extract the rotation invariant local features; some experiments were conducted to test the efficiency of the proposed method for handling rotated signatures. Fig. 6 clears that up to 10 degrees for the rotation of the name, the effectiveness of the system is not affected and the verification accuracy is still within 98%. The verification accuracy decreases as the angle of rotation increases and reaches 70% when the angle of rotation reaches approximately 42° . These results reflect the system's ability to handle the rotation of signatures. Furthermore, to test the extent of superiority of circular grid segmentation of the stamp with the rectangular grid segmentation to extract local features, the proposed system has been implemented with both configurations (8 sectors with 45° in circular grid and $25(5 \times 5)$ equal boxes) under different tested signatures and the FAR, FRR, and accuracy are observed. The results are exposed in Table 4, which reveals that circular grid segmentation achieves better results with an increase of at least a 2% percent in the verification accuracy. This is of course due to the ability of the circular grid segmentation to surround (catch sight of) style variations of the signatures.

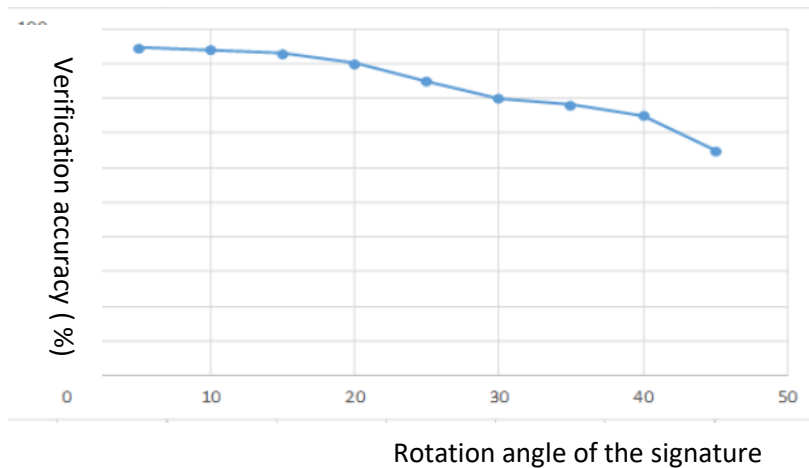


Fig. 6. system accuracy under different angle rotations of signature.

Table 4. System Accuracy under different grid segmentation.

Grid type	FRR	FAR	Accuracy
Circular grid	0.03	0.05	97 %
Rectangular grid	0.05	0.08	95 %

The last set of experiments was performed to show how verification rate of the proposed system be contingent on the number of signatures per signer: as every signer has more registered samples, the chance of correct hit increases. Up to 40 samples per singer, the incomes in performance are however lessening for every new example added due to the rise of intra-class signer's variability. As expected, the verification rate decreases as the number of signatures grow as a result of the reduction 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

V. Conclusion

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 labeled then preprocessing steps, and feature extraction for the verification process are inspected. An appropriate mixture of global and local features is utilized to yield more distinctive and useful 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 gaps 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 decide with a degree of certainty. Representing signature image by using a 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 to any signature shape. (3) It is simple, 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 the 4-tuple feature vector and coded is very active to remove all noise in the signature template. The experiments resulted in a verification rate of 98%. They also demonstrated the efficiency and robustness of the proposed system. Accurately selected distinguishing features of signatures shared with the use of two verification levels made the suggested approach more powerful compared to other existing systems both regarding success ratio, ease of implementation and optimized run time. Future work includes the examination of different features to enhance the performance of the system.

References

- [1] Y. Al-Omari, S. Abdullah, and K. Omar, "State-of-the-Art in Offline Signature Verification System", IEEE International Conference on Pattern Analysis and Intelligent Robotics, pp.59-64, 2011.
- [2] C. Prashanth, K. Raja, K. Venugopal, and L. Patnaik, "DWT based Off-line Signature Verification using Angular Features," International Journal of Computer Applications, 52(15):40-48, 2012.
- [3] C. Prashanth, K. Raja, K. Venugopal, and L. Patnaik, "Intra- modal Score level Fusion for Off-line Signature Verification", International Journal of Innovative Technology and Exploring Engineering, 1(2):179-187, 2012.
- [4] E. Justino, F. Bortolozzi, and R. Sabourin, "Off-line Signature Verification Using HMM for Random, Simple and Skilled Forgeries," IEEE Sixth International Conference on Document Analysis and Recognition, pp.1031 – 1034, 2001.
- [5] D. Jena, B. Majhi, and S. Jena, "Improved Offline Signature Verification Scheme Using Feature Point Extraction Method", Journal of Computer Science, 4(2):111-116, 2008.
- [6] J. Ravi, and K. Raja, "Concatenation of Spatial and Transformation Features for Off-Line signature Identification," International Journal of Innovative Technology and Exploring Engineering, 1(2):102-108, 2012.
- [7] E. Alsous, F. Nezam, S. Monadjemi, and N. Neamatbakhsh, "A Novel GA Based Approach to Farsi and Arabic Signature Verification," International Review on Computers and Software, 5(1):44-51, 2010.
- [8] M. Khalid, R. Yusof, and H. Mokayed, "Fusion of Multi-Classifiers for Online Signature Verification using Fuzzy Logic Inference", International Journal of Innovative Computing, 7(5):2709–2726, 2011.
- [9] Z. Zulkarnain, M. Rahim, and N. Othman, "Feature Selection Method for Offline Signature Verification" Journal of Technology, 75(4):79-84, 2015.
- [10] M. Parodi, J. Gomez and A. Belaid, "A Circular Grid-Based Rotation Invariant Feature Extraction Approach for Off-line Signature", IEEE International Conference of Document Analysis and Recognition, pp.1289-1293, 2013.
- [11] H. Hiary, R. Alomari, T. Kobbaey, and R. AL-Khatib, "Off-line Signature Verification System based on DWT and Common Features Extraction," Journal of Theoretical & Applied Information Technology, 51(2):165-174, 2013.
- [12] R. Jana, R. Saha, and D. Datta, "Offline Signature Verification using Euclidian Distance," International Journal of Computer Science and Information Technologies, 5(1):707-710, 2014.

- [13] D. Kisku, P. Gupta, and K. Sing, "Offline Signature Identification by Fusion of Multiple Classifiers using Statistical Learning Theory," *International Journal of Security and Its Applications*, 4(3):35-45, 2010.
- [14] E. Özgündüz, T. Şentürk, and M. Karşılıgil, "Off-line Signature Verification and Recognition by Support Vector Machine", *European Signal Processing Conference*, pp.1-4, 2005.
- [15] P. Shikha, and S. Shailja, "Neural Network based Offline Signature Recognition and Verification System," *Research Journal of Engineering Sciences*, 2(2):11-15, 2013.
- [16] M. Hanmandlu, M. Yusof, and V. Madasu, "Off-line Signature Verification and Forgery Detection using Fuzzy Modeling, " *Pattern Recognition*, 38(3):341–356, 2005.
- [17] A. Verma, D. Saha, and H. Saikia, "Forgery Detection in Offline Handwritten Signature Using Global and Geometric Features", *International Journal of Computer and Electronics Research*, 2(2):182- 188, 2013.
- [18] D. Impedovo, and G. Pirlo, "Automatic Signature Verification: The State of the Art ", *IEEE Transactions on Systems, Man, and Cybernetics*, 38(5):609 – 635, 2008.
- [19] S. Roy, and S. Maheshkar, " Offline Signature Verification using Grid based and Centroid based Approach," *International Journal of Computer Applications*, 86(8):35-39, 2014.
- [20] M. Mohammadzade, and A. Ghonodi, "Persian off-line signature Recognition with Structural and Rotation Invariant Features using by one-against-all SVM classifier", *Journal of Advances in Computer Research*, 4(2):87-96, 2013.
- [21] S. Khan, and A. Dhole, "An Offline Signature Recognition and Verification System Based on Neural Network", *International Journal of Research in Engineering and Technology*, 3(11):443-448, 2014.
- [22] D. Kumar, K. Raja, R. Chhotaray, and S. Pattanaik, " Off-line Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks", *International Journal of Engineering Science and Technology*, 2(12):7035- 7044, 2010.
- [23] K. Adhikary, and A. Kumar, "Proposal for Verification Using Neural Network", *Global Journal of Computer Application and Technology*, 1(4):717-720, 2011.
- [24] S. Ahmed, "Off-Line Arabic Signature Verification Using Geometrical Features", *National Workshop on Information Assurance Research, Saudi Arabia*, pp.1-6, 2012.
- [25] B. Shekar, and R. Bharathi, " LOG-Grid Based Off-Line Signature Verification System", *International Conference on Signal and Image Processing*, p.321, 2012.
- [26] J. Vélez, A. Sánchez, B. Moreno, and J. Esteban, " Fuzzy Shape-Memory Snakes for the Automatic Off-line Signature Verification Problem ", *Fuzzy Sets and Systems*, 160(2):182–197, 2009.
- [27] M. Nasiri, and A. Javaheri , "A Fuzzy Approach for the Automatic Off-line Persian Signature Verification Problem," *International Conference on Machine Vision and Image Processing*, pp.1-5, 2011.
- [28] P. Singh, and R. Patel, " Offline Signature Verification Using Fuzzy Logic", *International Journal of software & Hardware Research in Engineering*, 1(1):97-101, 2013.