

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/380487900>

A New Paradigm for Decision Making under Uncertainty in Signature Forensics Applications based on Neutrosophic Rule Engine

Article · May 2024

DOI: 10.54216/IJNS.240224

CITATIONS

0

READS

18

4 authors, including:



Oday Ali Hassen

Ministry of Education, Wasit Education Directorate, Iraq

34 PUBLICATIONS 218 CITATIONS

[SEE PROFILE](#)



Shahlaa Mashhadani

University of Baghdad

7 PUBLICATIONS 3 CITATIONS

[SEE PROFILE](#)



A New Paradigm for Decision Making under Uncertainty in Signature Forensics Applications based on Neutrosophic Rule Engine

Oday Ali Hassen^{1*}, Shahlaa Mashhadani², Iptehaj Alhakam², Saad M. Darwish³

¹ Ministry of Education, Wasit Education Directorate, Kut 52001, Iraq

² Department of Computer, College of Education for Pure Sciences Ibn Al-Haitham, University of Baghdad, 10071, Iraq

³ Department of Information Technology, Institute of Graduate Studies and Research, Alexandria University, 163 Horreya Avenue, El Shatby 21526, P.O. Box 832, Alexandria, Egypt

Emails: odayali@uowasit.edu.iq; shahlaa.t@ihcoedu.uobaghdad.edu.iq; ibtihaj.a.a@ihcoedu.uobaghdad.edu.iq; saad.darwish@alexu.edu.eg

Abstract

One of the most popular and legally recognized behavioral biometrics is the individual's signature, which is used for verification and identification in many different industries, including business, law, and finance. The purpose of the signature verification method is to distinguish genuine from forged signatures, a task complicated by cultural and personal variances. Analysis, comparison, and evaluation of handwriting features are performed in forensic handwriting analysis to establish whether or not the writing was produced by a known writer. In contrast to other languages, Arabic makes use of diacritics, ligatures, and overlaps that are unique to it. Due to the absence of dynamic information in the writing of Arabic signatures, it will be more difficult to attain greater verification accuracy. On the other hand, the characteristics of Arabic signatures are not very clear and are subject to a great deal of variation (features' uncertainty). To address this issue, the suggested work offers a novel method of verifying offline Arabic signatures that employs two layers of verification, as opposed to the one level employed by prior attempts or the many classifiers based on statistical learning theory. A static set of signature features is used for layer one verification. The output of a neutrosophic logic module is used for layer two verification, with the accuracy depending on the signature characteristics used in the training dataset and on three membership functions that are unique to each signer based on the degree of truthiness, indeterminacy, and falsity of the signature features. The three memberships of the neutrosophic set are more expressive for decision-making than those of the fuzzy sets. The purpose of the developed model is to account for several kinds of uncertainty in describing Arabic signatures, including ambiguity, inconsistency, redundancy, and incompleteness. The experimental results show that the verification system works as intended and can successfully reduce the FAR and FRR.

Keywords: Signature forensics; neutrosophic reasoning; offline signature verification; decision making under uncertainty; context-based verification.

1. Introduction

Biometric verification systems are becoming more popular because of their ability to accurately and reliably identify individuals based on a combination of their unique physical (such as face, fingerprint, and iris) and behavioural (such as voice, and signature) characteristics. Both kinds of biometric traits are reliable in distinguishing actual persons from impostors, and neither can be replicated simply by another person [1]. It's preferable if every given biometric has unique characteristics, including dependability, satisfaction, collectability, and the cost associated with its use. Human verification of routine events is required in many high-security contexts, such as forensic applications. Among the most often used behavioural features utilized in self-verification is a handwritten signature. The signature verification problem is how to tell whether a signature is genuine or not.

Human signature recognition is vital to the development of a better human-computer interface because a computer that can decipher a person's signature will provide a more efficient and insightful human-computer interaction.

Based on the method used to get the signature, signature verification systems may be divided into two broad categories: (1) the online or dynamic verification technique, whereby the signature is taken in real time on a digitizing tablet and subsequently stored on a computer for assessment of dynamic information such as velocity, pressure points, acceleration, distance traversed, etc. to identify a person; and (2) the offline verification approach "static," which relies on a "still" image of the signatures and compares it to a database of known signatures [2]. Verifying a signature offline is more challenging than doing it online due to the fact that features are mined using a static 2D image of the signature and there is a lack of dynamic information. Offline verification systems often have lower performance than online systems, making it an intriguing challenge to improve their capabilities. Since document analysis often employs offline techniques, such as authenticating signed documents, the strategy presented in this study is centred on an offline validation system. Clearly, the difficulty of offline signature verification grows from seeing random forgeries to spotting basic and sophisticated forgeries.

Offline signature verification has two main categories of practical problems: (a) difficulties in extracting the signature's fingerprint from the document (feature extraction process) and (b) difficulties in doing the verification itself (building classification model), as illustrated in Fig. 1 [3]. Multiple classifiers (ensemble learning) have been shown to enhance verification accuracy because they give a more thorough understanding of the patterns to be categorized. Multi-level signature verification, in which decisions are made based on a combination of several features of a signature, is supported by the results of this research [4]. The three potential combinations of offline signature verification are as follows: (i) on the feature extraction level: by merging the many offline signature features (fingerprint) already in use, a new set of characteristics is generated; (ii) at the matching score level: methodologies for obtaining and fusing matching scores for offline signature parameters with varying characteristics are available; and (iii) at the decision level: the acceptance or rejection decision is reached by separately combining features acquired from many biometric data sources.

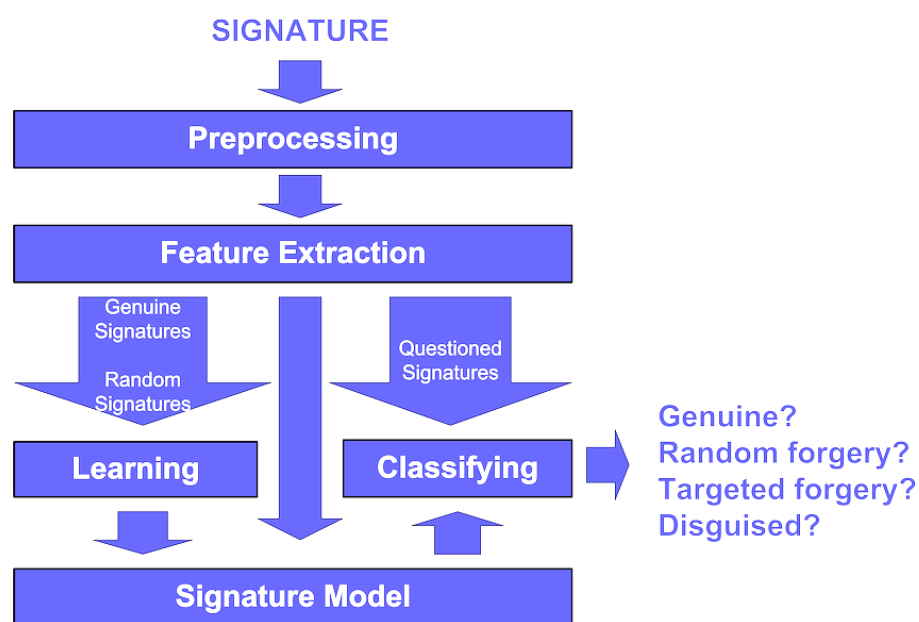


Figure 1: Schematic diagram of a signature –based biometric verification system

Automated offline signature verification is still a difficult problem, despite its widespread use. Signature variability is one of the biggest obstacles to signing verification. Signatures captured at various periods from the same user exhibit large variations (high intra-class variability), yet expert forgers may create convincingly similar copies (low inter-class variability) of genuine signatures. Signature verification is also impacted by a wide range of other parameters, including the complexity of signature patterns and the availability of reference samples. In general, formal verification of biometric systems is made more difficult by uncertainty. Invalid verification results and a lower degree of trust in these systems might emerge from unexpected changes and alterations in their biometrics' attributes. However, uncertainty management has seen little research so far. The first step in dealing with uncertainty is identifying, de-fining, and categorizing the many types of uncertainty present in offline signature

verification. Numerous crucial and ground-breaking studies have already been conducted, and there are numerous approaches to dealing with these uncertainties, including the use of fuzzy and intuitionistic fuzzy sets [5].

All kinds of uncertainty, such as indeterminate and inconsistent information, remain unaddressed by fuzzy logic and its versions, despite their usefulness in dealing with incomplete information in a wide range of practical difficulties. Fuzzy sets and intuitionistic fuzzy sets are only a few of the many types of fuzzy sets that are further generalized by neutrosophic theory [6][7]. The idea here is to add a neutrosophic representation of the data and a neutrosophic reasoning system to the fuzzy representation and reasoning system, thus expanding its possibilities. Fig. 2 shows how fuzzy expert systems vary from neutrosophic expert systems. The degrees of truth (T), indeterminacy (I), and falsity (F) are assigned to propositions in neutrosophic logic. In order to solve the uncertainty issue, fuzzy set theory states that there is a membership function for each component level of participation. When dealing with indeterminate data, neutrosophic sets are superior to fuzzy sets and intuitionistic fuzzy sets. In light of the above, it is clear that neutrosophic logic has a good shot of being used for signature verification in the real world [7-11].

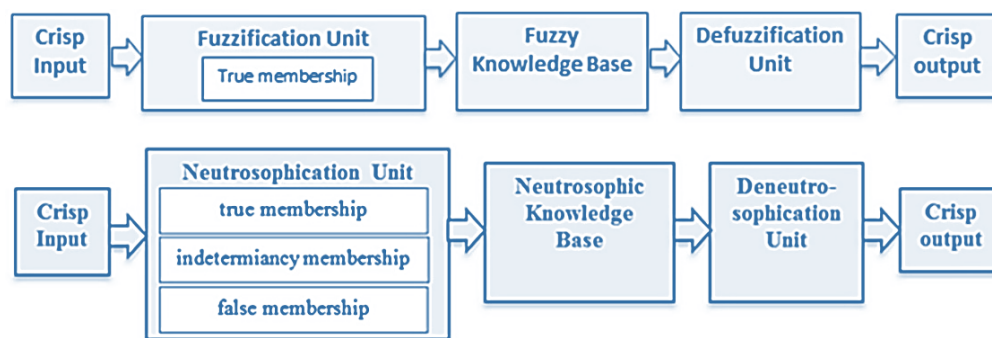


Figure 2: A Comparison of fuzzy and neutrosophic expert systems

1.1 Motivation and Contribution

Arabic offline signature verification systems are still difficult to study as the characteristics of Arabic signatures are not very clear and are subject to a great deal of variation (features' uncertainty) and have been the subject of very little academic attention until now, which is why this work is dedicated to investigating the matter in depth. Using neutrosophic logic to fuse extracted features from scanned signature images and to deal with the inherent imprecision of human decisions about signature similarity, this research aims to demonstrate that a two-tiered strategy for signature verification yields superior identification performance.

Arabic signature verification has been hard to develop because of the difficulties presented by the script, which include cursive writing and other features. The pro-posed approach accounts for individual users' signatures' natural variation by using a user-dependent threshold, which helps to decrease both false acceptances and false rejections. In behavioural biometrics, where there are more opportunities for error due to differences in authentic samples than in physiological biometrics, the user-specific threshold is preferred over the global threshold. Another benefit of user-dependent thresholds is that when a new user is added to the database, only the new user's signature samples are needed in the training process, whereas with global thresholds, the entire system must be retrained to obtain an updated threshold. In contrast to the global threshold, the time needed for this operation is not proportional to the size of the database or the number of users currently logged in to it.

The structure of this article is as follows: The relevant literature is presented in Section 2. The suggested signature verification system's design is presented in Section 3. Results from experiments and comparisons to relevant literature and the suggested methodology are presented in Section 4. The conclusion and plans for further research are summarized in Section 5.

2. Related Work

Verifying various types of signatures has become much more complicated in recent years. These methods extract characteristics from the signature images, which might be of a single kind (global, local, statistical, geometric, etc.) or a combination of types. The single feature extraction approach used in the biometric identification system has several limitations in terms of FRR and FAR. When two or more features are fused together, these restrictions disappear, resulting in optimal performance. Making offline signature verification systems resilient against transformation (e.g., rotation, scale) of the signatures is a significant difficulty [12]. The work presented in

Ref. [13] overcomes such obstacles by utilizing quantum-inspired GA (QIGA) to perform multi-feature fusion and discriminant feature selection. Three signature databases (SID-Arabic handwritten signatures, CEDAR, and UTSIG) are used to test the investigated method. As a result, the presented offline signature verification based on the QIGA enhanced the equal error rate (EER) by 10% to 20% relative to the GA without affecting the computational complexity.

An effective approach for signature identification using local binary patterns (LBP) features was given in Ref. [14]. The signature is contained in a symmetrical and suitable shape using morphological methods. This study used a local dataset consisting of 60 test signature patterns and found that 10% were accepted incorrectly, yielding a FAR of 0.169. A local dataset of signature images is used in the experiments. In the past, the KNN classifier was used for signature verification. The KNN classifier outperformed its predecessors in terms of FARs and recognition accuracies. In Ref. [15], the authors introduced a new biometric method for signature verification dubbed the Extended Beta-elliptic Model that uses fuzzy elementary perceptual codes (FEPC) to extract static and dynamic features from signature pictures. Their technology has been tested, and the results seem good for increased efficiency.

An offline signature verification system based on a convolutional neural network (CNN) architecture has been presented by the authors in Ref. [16]. The research aims to construct a CNN-based, flexible system capable of verifying offline signatures written in many scripts. The model has been trained and tested using signatures in Hindi, Bengali, and English from two publicly accessible datasets (CEDAR and BH-Sig260). The suggested model has been put through its paces, with results showing verification accuracies of 90%, 95%, 98.33%, and 93.33% for individual signature classes of distinct scripts and a combination of these scripts, respectively. Their model surpasses the verification accuracy of various established models, and the results of the experiments are convincing.

In Ref. [17], a signature recognition model was built using a minimal amount of samples and an enhanced AlexNet and transfer learning architecture to validate offline signatures. The samples were created using the signatures of eight distinct people, and the model's generalizability was evaluated for those signatures. Initially, the model's accuracy was improved from 77.50 to 96.87% by using visualization technologies to fine-tune the model's architecture, activation function, and normalization. The issue of a lack of data was addressed by using transfer learning, and the model's feature extraction was enhanced by adjusting the number of channels. Multiple authentic signatures, as well as both simple and skilled forgeries, were examined to see whether the model could identify them; the results showed identification rates of 91.25%, 95.63%, and 85.63%, respectively.

In Ref. [18], the authors developed a hybrid approach to feature extraction from signature images, which combined the usage of a convolutional neural network (CNN) and a histogram of oriented gradients (HOG) with a feature selection technique (decision trees) to isolate the most significant features of the images. The performance of the hybrid approach was examined using three different classifiers (long short-term memory, support vector machine, and K-nearest neighbour). With (95.4%, 95.2%, and 92.7%, respectively) on the UTSig dataset and (93.7%, 94.1%, and 91.3%, respectively) on the CEDAR dataset, the experimental results showed that their model functioned effectively in terms of efficiency and predictive capacity. The work published in Ref. [19] presented a way for identifying offline signatures using deep learning algorithms under varied uncertainties, such as variable experimental conditions and external noises. In order to extract features from raw data, a deep neural network is built using transfer learning networks. The suggested approach has the advantage of being equally useful for right- and left-handed individuals. The results of the research demonstrate that the suggested network is able to learn features hierarchically from raw signature data, outperforming previous approaches in the process.

An open writer signature identification system was discussed utilizing a novel scheme of the one-class symbolic data analysis (OC-SDA) classifier and a small number of reference signatures in Ref. [20]. In order to create additional information for developing the symbolic representation model (SRM) unique to each writer, the authors include intra-class feature dissimilarities produced by the curvelet transform. Feature differences boost inter-personnel variability by facilitating the effective collection of the intra-personnel variability that a writer's natural output naturally produces. The OC-SDA model is constructed not using the mean and standard deviation but rather a new weighted membership function based on the actual probability distribution of training intra-class feature dissimilarities, one for each author. The presented OC-SDA classifier achieves 98.31%, 98.06%, and 99.89% accuracy on the GPDS-300, CEDAR-55, and MCYT-75 public signature datasets with only five reference signatures, outperforming the existing classifiers even when combining multiple classifiers or employing learned features. Further, testing using well produced signatures demonstrates that the suggested writer identification method can identify both genuine and forged signatures.

In Ref. [21], an automated approach based on multi-level feature fusion and optimal feature selection is presented for offline signature verification. Twenty-two Grey Level Co-occurrences Matrix (GLCM) features and eight geometric features are computed from signature samples in the pre-processing phase to achieve this goal. A novel parallel method is utilized to combine these features; it is predicated on an index feature with high priority. A skewness-kurtosis-based feature selection technique is also employed to pick the optimal features for final classification into forged and authentic signatures. In Ref. [22], the authors have created an offline signature verification model that is language-independent and may be used in both writer-dependent and writer-independent settings. First, an offline signature is captured in the form of an image for later use in the singular value decomposition of a matching signal. After the signature image's signal has been processed, four distinct types of features—statistical, shape-based, similarity-based, and frequency-based—are retrieved. Next, they've developed a new wrapper feature selection technique using the Red Deer Algorithm to retain just the appropriate features to be employed throughout the signature authentication and verification process, therefore reducing the feature dimension. Finally, a confidence score from the Naïve Bayes classifier has been employed to execute the authentication and verification procedure. The results obtained demonstrate the superior performance of the presented model compared to its predecessors.

As a method for handwritten signature recognition, the authors in Ref. [23] offered a formal model of the signature that incorporates fuzzy aspects of the curvature of discrete signatures. They introduced a prospective strategy for building membership functions from fuzzy features and used it to design an algorithm for creating reference templates for handwritten signatures. The implementation of a reasonable collection of features has reduced the false acceptance rate to as low as 0.05% and the equal error rate to as low as 0.36%, both of which are vast improvements over the performance of previously available handwritten signature recognition systems. In Ref. [24], the authors analysed the essential signature features and verified signatures with more certainty. Fuzzy genetic algorithms (FGA) provide fuzzy templates for the identification of the smallest subset of features, hence solving the conventional difficulties in feature classification and selection. Using FGA, the algorithm can focus down on the most important features, which can then be discretized using the class-dependent discretization technique. Two forms of signature variability, intra-class and interclass, affect many signatures. Two significant benefits may be gained by using a fuzzy genetic algorithm. At first, it was possible to rank the significance of the individual features that made up the key signature. To add to that, the classifier's efficiency might be enhanced.

A formal model of a human handwritten signature with many fuzzy features is suggested in Ref. [25]. Both reference templates for handwritten signatures and algorithms for recognizing handwritten signatures were suggested. Potentials were employed to derive membership functions for fuzzy features, allowing for the construction of a reference template even in the face of a limited training set. In comparison to the assessment results obtained by many other methods, our FAR value of 2.8%, FRR value of 0.4% for random fake patterns, and FRR value of 0.8% for skilled fake patterns are all much superior. In Ref. [1], the authors introduced a novel methodology for extracting both static and dynamic features from signature data by combining fuzzy elementary perceptual codes. In order to identify a user's signature as genuine or forged, they used the sum rule combiner to compare the results of three separate models: a deep bi-directional long short-term memory (deep BiLSTM), a support vector machine (SVM) with dynamic time warping (DTW), and an SVM with a newly suggested parameter comparator. Their technology has been tested on two open-source signature databases, and the results are encouraging.

With the help of a random oracle model, the authors in Ref. [26] analysed the security of a novel lightweight, provably secure partial discrete logarithm (DL)-based subtree-based short signature with fuzzy user data sharing for human-centred IoT systems. Better security is guaranteed by the proposed method compared to previously implemented short-signature techniques. The novel, provably secure, and lightweight subtree-based short-signature technique is ideal for low-storage, low-computation, and low-bandwidth communication settings. In comparison to previous efforts, the outcomes highlight the superiority of the suggested approach. In Ref. [27], an additive fuzzy and TS modelling-based signature verification and forgery detection system was reported. In order to create a reliable authentication system, it is necessary to sample aspects of different handwritten signatures, analyse them, and then encapsulate them. In order to identify fakes and authenticate signatures, the authors employed the grid approach to extract feature angles. The generated functions were fuzzified using an exponential membership function, and their structural parameters were adjusted so that they could account for differences in handwriting and other aspects associated with signature scripting. Forty individuals' signatures are used to evaluate the method given here. In Ref. [3], a comprehensive survey of the literature on the methods used to verify handwriting, including signatures, the results of different approaches have been explored in detail, drawing attention to current research priorities and future directions.

2.1 The Need To Extend The Related Work

In order to solve the problems of scalability caused by the matching problem between the inquired signature and all the signatures in the data set and verification uncertainty caused by variation in signature features, the proposed method uses two levels of verification to classify signatures as either genuine or forgeries, in contrast to the state-of-the-art offline signature verification methods, which depend on a single level of verification. To verify at the first level, we need to calculate the variance between the extracted features of the test signature and the average values of those features in the training signatures. Level two verification, on the other hand, uses the neutrosophic logic module's output based on the three membership functions derived from the signature's features in the training dataset associated with a given signer.

This work mainly aims to provide neutrosophic logic shifts to the commonly used offline signature verification method based on fuzzy logic. Neutrosophic systems, similar to their fuzzy counterparts, may benefit from the knowledge of human operators. Neutrosophic sets (NS) handle truth, indeterminacy, and falsity membership grades independently, in contrast to fuzzy sets (FS) that use the membership grade to handle uncertainty. As a result, when there is a possibility of indeterminacy and incompleteness in the acquired data (signatures in our case), a neutrosophic controller is proposed to deal with these situations.

3. Methodology

One branch of pattern-based science, signature forensic analysis, looks for patterns in questioned writers' signatures by analysing their distinctive, recurring features, or handwriting habits and comparing these features to existing writing. Offline signatures come in a wide variety of sizes and shapes, and the variety is so great that a human being would have a hard time telling a genuine signature from a fake one with just a quick glance. On the basis of their contours, signatures are often classified as simple, cursive, or graphic. Applicants' signatures are behavioural biometrics that change over time and are affected by their physiological and emotional states. The proposed method seeks to construct an intelligent offline Arabic signature verification system by extending the neutrosophic logic framework for multiple classifier fusion.

Offline signature authentication and verification often follow the standard pattern recognition framework, which consists of the following steps [28]: (1) capturing the signature image through data acquisition; the purpose of pre-processing is to enhance the image's quality for more effective analysis; (2) Pre-processing phase: through the use of pre-processing, we are able to eliminate unwanted distortions and improve certain features that are critical to our current application; (3) extraction of salient features: a method for diminishing data by assessing selected features; (4) final conclusion for classification is reached by verification, which entails checking the value of the features obtained during feature extraction. (5) evaluation of performance—to calculate an approximation of the signature verification system's efficiency.

The proposed model accounts for the wide variety of offline signatures by using neutrosophic logic to distinguish between three types of uncertainty: first, due to incomplete knowledge, acquisition errors, or stochasticity; second, due to a lack of clear contours; and third, due to imprecision of knowledge or linguistic inexactitude received by different observers [7][11]. In Fig. 3, we can see the general architecture of the proposed verification system, and in the following sections, we will go over each individual phase. Following are characteristics of the suggested system: (i) basing the final decision on two classification levels that can replicate the operation of human experts and so achieve higher accuracy; (ii) using neutrosophic language variables to define the aspects of the image signature in order to infer the image signature as human thinking.

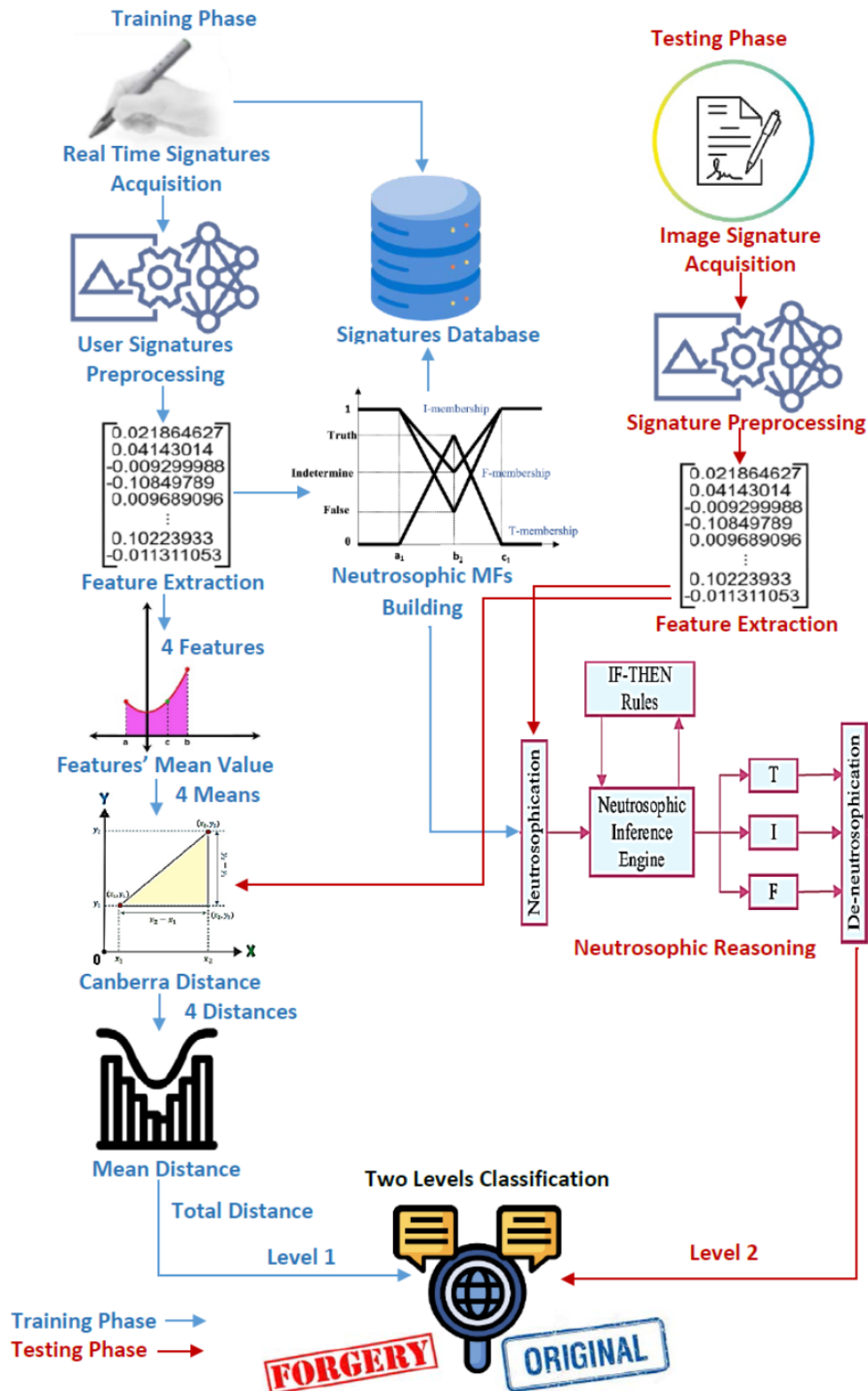


Figure 3: The proposed Arabic offline signature verification system

3.1 Step 1: Real-Time Signatures Acquisition

Offline signature verification involves collecting original signatures from several signers, recording them on A4-sized paper, scanning them at 300 dpi, and saving the resulting Portable Network Graphics (PNG) file. The

database in the training phase contains signatures from people, both authentic and forged. There are a variety of signature angles and scales, depending on whether the signer is standing or seated, in the training phase (active signatures received directly from the signer). Each page has 40 signatures, written in either black or blue ink. Digital archives of scanned images are stored for later offline processing. During the testing phase, the signature is retrieved from the document, and the signature's legitimacy is questioned. Using the same scanner, this document is scanned before the signature is extracted for pre-processing. This is accomplished by cropping the document image to the signature's bounding rectangle. Some representative examples of signatures used in the proposed system's training and testing are shown in Fig. 4.

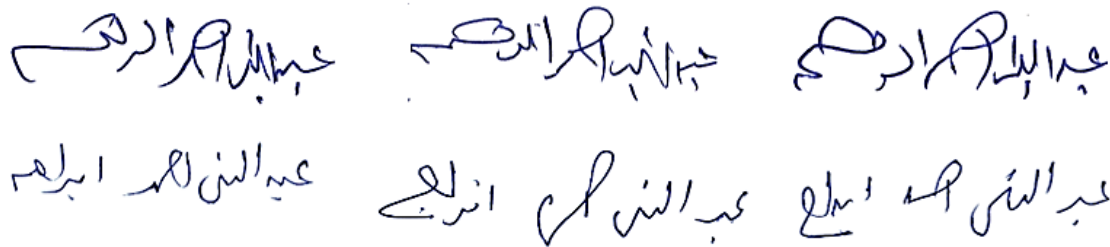


Figure 4: Sample of individual signatures (Top) Genuine and (Bottom) Forgery

3.2 Step 2: Signature Pre-processing

Training and testing both make use of the pre-processing step. Signatures are prepared for feature extraction and standardization at this step. Seven steps make up the pre-processing phase, which include converting to a grayscale image, binarization, noise reduction, cropping, rotation and width normalization, thinning, and skeletonization. See [18] for more details. A resized, binarized, and thinned image free of noise is the end product of the pre-processing step.

3.3 Step 3: Features Extraction

Finding discriminant features in the acquired and pre-processed signature images is the next stage. A vector of items describing the value of a feature is used to describe the signature when parameter features are used. The extraction of features is often the key component of signature verification systems [15][29][30]. To maximize the interpersonal distance between different people's signature instances and minimize the intrapersonal distance within the same person's examples, an ideal feature extraction method uses a minimum number of features. Global and local features are the two most common types of features. Features such as wavelet transformations, signature edge points, width, density, and length serve as global descriptors for the whole signature image. Noise and signature variations are not effectively handled with these features. However, it is suitable for random forgeries and works better when paired with other features; it will not provide us with a high degree of accuracy for skilled counterfeiters. Local features refer to features that are retrieved at the pixel level from specific regions of the signature (pixel-oriented features). In order to create more distinctive and effective features, a proper combination of global and local features might be applied.

The proposed approach takes a new direction in feature combination by adopting the neutrosophic notion of merging local and global features. Within the context of the local features, a circular grid pattern is employed to partition each pre-processing signature image into identical sectors, and pixel density with gray-level intensity features is calculated for each sector [31]. Here, the system builds an intelligent knowledge base of unique features for a single person based on local features, which allow it to capture global behaviour. Reducing the area of focus to only the signature image was another driving force for the grid's design. The following features will be mined and used for signature verification; they outperformed other features in differentiating inter- and intra-personal signature variations [12] [18] [29].

- f_1 : Aspect Ratio (AR_{global}) is the signature's width to height ratio. The signature's width and height are computed using the provided bounding box coordinates.
- f_2 : Normalized Area (NA_{global}) determines how much of the bounding box is covered by signature pixels as a percentage.

- f_3 : Pixel Density (PD_{local}) is the percentage of pixels that are black inside a certain sector of the circular grid as a percentage of all pixels within that sector.
- f_4 : Gravity Distance (GD_{local}) this is the ratio of the distance between the center of gravity and the grid to the radius of the grid, where the radius is the primary distance between the extreme points of the signature.

The suggested approach makes use of the feature vectors generated for each signature during training and testing in the following ways:

- In the training phase, the neutrosophic membership functions for each feature is built using the feature vector, taking into consideration the lowest and maximum values of that feature. This is done for all signatures associated with a given signer. The features collected from the test image signature are fuzzified using these membership functions later on in the testing phase. The features are fused in a unified framework for level 2 classification inside the neutrosophic logic module. In this case, the goal of implementing neutrosophic logic is to deal with the fact that human judgments on the physical appearance of signature features are inherently inaccurate.
- To determine the distance (Canberra Distance) between the feature vectors obtained from the test image signature and the average values of the extracted features for all signatures of the same signer in the database, the feature vector is used during the test phase. This result will be used in the level 1 classification that will be discussed later; it explains the degree to which this signature deviates from his total signatures in the database.

3.4 Step 4: Building Neutrosophic Inference System

Fuzzifying the features is necessary for the system to match a particular signature with the database due to the complicated variances in the feature components of each signature [32]. To account for local variations in signature features caused by various user signing methods, the proposed system has merged the signatures' structural properties. The neutrosophic analytic model is used for level 2 classification in our technique. A neutrosophic three membership functions (MFs) with a trapezoidal shape is used to fuzzy each feature. Due to its intuitive nature and suitability for subjective input and output, the trapezoidal shape has seen extensive application. The system is trained using the users' genuine signatures in order to get the MFs' parameters. The goal of training the neutrosophic inference engine is to minimize the mean square error of its output by repeatedly adjusting the parameters [7]. The local and global signature's feature variation is described using three neutrosophic variables, "low", "normal", and "high", as shown in Fig. 5. Truth, indeterminacy, and falsity are the three values that neutrosophic logic uses to express various forms of knowledge and the relationships between signatures' features. The standard deviation and mean of the features in the training signatures are used to identify the numerical parameters of MF. The MFs' corresponding equations are expressed as follows [33].

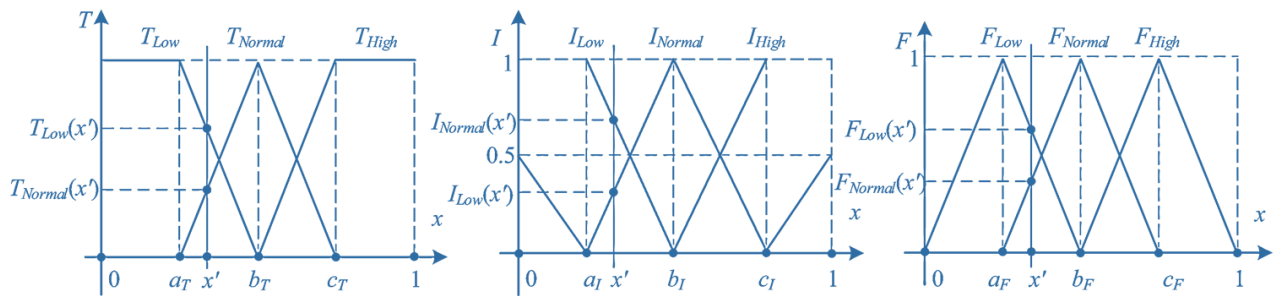


Figure 5: (left) Truth, (middle) indeterminacy and (right) falsity-membership functions for each signature feature

$$T_{low} = \begin{cases} 1, & 0 \leq x < a_T \\ \frac{b_T - x}{b_T - a_T}, & a_T \leq x < b_T \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

$$T_{medium} = \begin{cases} \frac{x - a_T}{b_T - a_T}, & a_T \leq x < b_T \\ \frac{c_T - x}{c_T - b_T}, & b_T \leq x < c_T \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

$$T_{high} = \begin{cases} \frac{x-b_T}{c_T-b_T}, & b_T \leq x < c_T \\ 1, & c_T \leq x \leq 1 \\ 0, & otherwise \end{cases} \quad (3)$$

$$I_{low} = \begin{cases} \frac{a_I-x}{2a_I}, & 0 \leq x < a_I \\ \frac{x-a_I}{b_I-a_I}, & a_I \leq x \leq b_I \\ 0, & otherwise \end{cases} \quad (4)$$

$$I_{medium} = \begin{cases} \frac{b_I-x}{b_I-a_I}, & a_I \leq x < b_I \\ \frac{x-b_I}{c_I-b_I}, & b_I \leq x < c_I \\ 0, & otherwise \end{cases} \quad (5)$$

$$I_{high} = \begin{cases} \frac{c_I-x}{c_I-b_I}, & b_I \leq x < c_I \\ \frac{x-c_I}{2(1-c_I)}, & c_I \leq x < 1 \\ 0, & otherwise \end{cases} \quad (6)$$

$$F_{low} = \begin{cases} \frac{x}{a_F}, & 0 \leq x < a_F \\ \frac{b_F-x}{b_F-a_F}, & a_F \leq x < b_F \\ 0, & otherwise \end{cases} \quad (7)$$

$$F_{medium} = \begin{cases} \frac{x-a_F}{b_F-a_F}, & a_F \leq x < b_F \\ \frac{c_F-x}{c_F-b_F}, & b_F \leq x < c_F \\ 0, & otherwise \end{cases} \quad (8)$$

$$F_{high} = \begin{cases} \frac{x-b_F}{c_F-b_F}, & b_F \leq x < c_F \\ \frac{1-x}{1-c_F}, & c_F \leq x \leq 1 \\ 0, & otherwise \end{cases} \quad (9)$$

The rule base (neutrosophic reasoning) may be constructed to provide an interpretation of the signature features' similarity after the system has obtained their neutrosophic explanations. A grade of presence or absence of connection or relations between the signatures' features of two or more sets is offered by neutrosophic reasoning, which is expressed by a collection of IF-THEN rules [7-11]. Using four layers of linguistic variables, sixteen rules are formulated to classify data from AR_{global} , NA_{global} , PD_{local} , and GD_{local} signature's feature interpretations. Experts from Egypt's Ministry of Justice's Department of Forgery were considered throughout the creation process of neutrosophic logic's IF-THEN rules. Each rule is listed in Table 1. The rule to be executed may be decided when the membership degree of each antecedent component has been received. The AND operator is used to obtain a single value when an antecedent occurs in a rule with more than one component. After this is completed, there will be just one value of truth. In this instance, the AND operator is represented by min , which means minimal. A final judgment is reached about the identification of genuine from forged signatures (signatures' similarity) using the fired IF-THEN rules and the min operator.

$$\mu_{r,t} = \min(\mu_{S1,r,t}, \mu_{S2,r,t}, \mu_{S3,r,t}, \mu_{S4,r,t}) \quad (10)$$

$$\mu_{r,i} = \min(\mu_{S1,r,i}, \mu_{S2,r,i}, \mu_{S3,r,i}, \mu_{S4,r,i}) \quad (11)$$

$$\mu_{r,f} = \min(\mu_{S1,r,f}, \mu_{S2,r,f}, \mu_{S3,r,f}, \mu_{S4,r,f}) \quad (12)$$

$$\mu_r = \min(\mu_{r,t}, \mu_{r,i}, \mu_{r,f}) \quad (13)$$

$\mu_{r,t}$ is the truth membership value for the r^{th} rule, $\mu_{r,i}$ is the indeterminacy membership value for the r^{th} rule, $\mu_{r,f}$ is the falsify membership value for the r^{th} rule, and μ_r is the final aggregate value of the r^{th} rule. $\mu_{S1,r,t}$, $\mu_{S2,r,t}$, $\mu_{S3,r,t}$, and $\mu_{S4,r,t}$ are the truth membership values of $f_1: AR_{global}$, $f_2: NA_{global}$, $f_3: PD_{local}$ and $f_4: GD_{local}$ signature features respectively for r^{th} rule. $\mu_{S1,r,i}$, $\mu_{S2,r,i}$, $\mu_{S3,r,i}$, and $\mu_{S4,r,i}$ are the indeterminacy

membership values of f_1, f_2, f_3 and f_4 signature features respectively for r^{th} rule. $\mu_{S1,r,f}, \mu_{S2,r,f}, \mu_{S3,r,f}, \mu_{S4,r,f}$ are the falsify membership values of f_1, f_2, f_3 and f_4 signature features respectively for r^{th} rule.

The sixteen rules collectively deal with the weight assignments implicitly in the same manner as the experience-based thinking assignments. The decision is more reasonable since neutrosophic inference considers all the cases in parallel. A signer's signature similarity to his signatures recorded in the training signature database is the output of the neutrosophic inference engine system. Signature similarity is the output variable (consequent), representing the expected verification decision. Similarity expressions are also given in linguistic variables that include "low," "normal," both of which 'represent' 'reject' or forgery signature, and "high," which represents 'accept' or genuine signature.

$$\text{Similarity} = \max((\mu_r, \text{Accept}); (\mu_r, \text{Reject})) \quad (14)$$

The outputs of neutrosophic values are then de-neutrosophicated to generate a crisp value for the variable. The de-neutrosophication of the linear trapezoidal neutrosophic number is provided by using the area removal approach for the de-neutrosophication of the single-valued trapezoidal neutrosophic number [34].

Table 1: Neutrosophic logic-based signature verification: a set of basic rules

Rule	Antecedent $f_1: AR_{global}$	Antecedent $f_2: NA_{global}$	Antecedent $f_3: PD_{local}$	Antecedent $f_4: GD_{local}$	Consequent Similarity
1	[Low,0,0]	[Low,0,0]	[Low,0,0]	[Low,0,0]	Accept (Genuine)
2	[High,0,Low]	[Low,0,Low]	[Low,0,Low]	[Low,0,Low]	Accept
3	[Low,0,Low]	[High,0,Low]	[Low,0,Low]	[Low,0,Low]	Accept
4	[High,0,Low]	[High,0,Low]	[Low, Low,0]	[Low, Low, 0]	Accept
5	[High,0,Low]	[High,0,Low]	[High,0,Low]	[Low,0,Low]	Reject (Forgery)
6	[High,0,Low]	[High,0,Low]	[High,0,Low]	[High,0,Low]	Reject
7	[Low, Normal,0]	[Low, Normal, 0]	[Low, Normal,0]	[Low, Normal,0]	Accept
8	[High, 0,0]	[High, 0, 0]	[Low, 0,0]	[Low, 0,0]	Accept
9	[Low,0,Low]	[Low,0,Low]	[High,0,Low]	[High,0,Low]	Accept
10	[High,0, Normal]	[High,0, Normal]	[High,0, Normal]	[Low,0, Normal]	Reject
11	[High, Low, 0]	[High, Low, 0]	[Low,0,Low]	[Low,0,Low]	Accept
12	[Low,0, low]	[High,0, low]	[High,0, Normal]	[High,0, Normal]	Reject
13	[High,0, Normal]	[Low,0, Normal]	[High,0, Normal]	[Large,0, Normal]	Reject
14	[High, Normal, 0]	[High, Normal, 0]	[Low,0, Normal]	[Large,0, Normal]	Reject
15	[High, Normal, 0]	[High, Normal, 0]	[Large,0, Normal]	[Low,0, Normal]	Reject
16	[High,0,0]	[High,0,0]	[High,0,0]	[High,0,0]	Reject

3.5 Step 5: Verification

This is the last step, and it involves comparing the input signature that has been checked with the sample signature that is stored in the database. The suggested approach does this using a two-stage verification process (classification). The last step is to use a combination of the two classifiers to decide whether the signature is genuine or a forgery.

- **Level 1 verification:** Finding the sum of the differences between the extracted test signature's feature (four features) and the training signatures' feature mean values (the same signer's signatures) is the basis of level one verification. During the training phase, a four-element vector is created by averaging the values of all the features in the signature features vector for all the stored signatures. Each element M_{fi} represents the mean of its associated feature, with i ranging from 1 to 4. Following that, we measure the Canberra distance between the computed vector and the feature vector that was specified during the test phase. This metric was selected because it provides a more precise reflection of the relationship between the two points and their distance from the origin, in addition to the absolute distance between them. The authenticity of the signature may be determined by examining the output values of the distance function $\zeta_1 \leq 0.4$.
- **Level 2 verification:** The output of the neutrosophic logic module is dependent on the three membership functions (Truth, indeterminacy, and falsity MFs) that have been built from the features of the signature in the training dataset for a given signer. These features are used in level two verification. The neutrosophic module here serves as a fusing tool, combining various features with the other neutrosophic logic components to create

a classifier. If the output of neutrosophic classifier (de-neutrosophication) $\zeta_2 \geq 0.7$ then the signature is genuine. We next merge the output from the two classifiers. In the end, the experimentally-derived criterion for deciding whether a signature is genuine or forged is as follows: if $\zeta_1 \leq 0.4$ and $\zeta_2 \geq 0.7$ the signature is genuine. In this case, four features derived from signature global and local factors aid in the system's ability to distinguish between original and false signatures.

4. Results and Discussions

A MATLAB (Release 2022a) implementation was used to examine the proposed system's efficiency. A modularly constructed prototype verification approach was used and evaluated on a Dell PC computer, which had the following characteristics: The system requirements are Intel (R), Core (TM) i7 CPU, L640 @ 2.31 GHz 2.31 GHz with RAM: 4 GB. System type: 64-bit operating system. Microsoft Windows 8.1 Enterprise as the running operating system, and Hard Disk: 500 GB. Forty signature images were used in the training phase of this study, with four discriminative features assigned to each signature. Twenty historical signature images were employed for testing, with ten genuine signatures and ten forged ones included. Fig. 6 displays a sample of individual's signatures under various signature variants. To measure how well a signature verification technique works, two metrics are used: the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). The FAR, which indicates that a forgery is treated as genuine, is the sum of all the forgery signatures detected by the system as genuine divided by the total number of comparisons. The FRR is the sum of all the original signatures that the system rejected relative to the total number of comparisons. This suggests that a genuine signature is regarded as a fake signature [35].

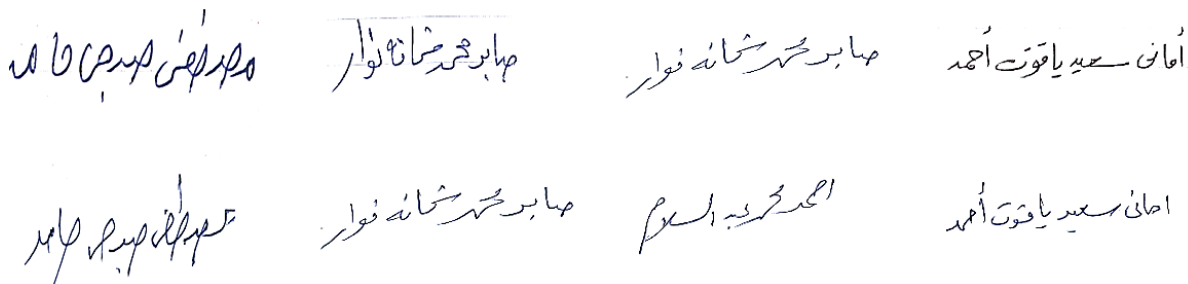


Figure 6: A sample of signatures for a group of people (top) original and (bottom) forged

With conventional signature verification classifiers utilizing SVM [21] and CNN [35] as well as fuzzy logic [32] with the same features, the initial set of experiments was conducted to replicate the proposed system's verification performance. The suggested system utilizes two levels of verification: distance-based and neutrosophic -based verification. The comparison of the verification systems is shown in Table 2. The results show that another 6-18% increase in verification rate (accuracy) is achieved by using two stages of verification. Among the alternatives, the suggested technique yields the lowest FAR percentage. The accurate verification of signatures improves performance because, in addition to the classic feature similarity distance classifier, neutrosophic variables are utilized to indicate the similarity degree of signature features in human thinking. In general, neutrosophic sets take into consideration the in-determinacy component that captures any vagueness and uncertainty and has the ability to deal with information that comes from different data sources.

Table 2: Comparison of the signature verification classifiers

Classifier	FRR	FAR	Accuracy
Neural Network (Machine Learning)	0.22	0.16	80%
Support vector machine (Distance classifier)	0.11	0.13	84%
Fuzzy-based classifier (Fuzzy classifier)	0.08	0.11	92%
Two- levels classifier (Neutrosophic classifier)	0.01	0.04	98%

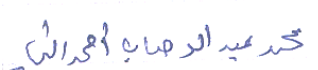
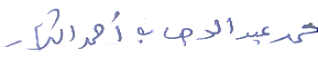
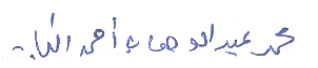
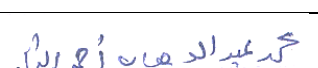
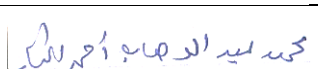

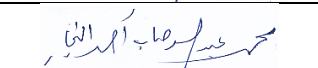
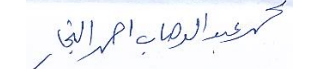
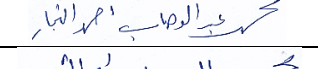
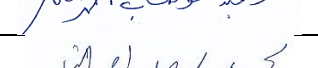
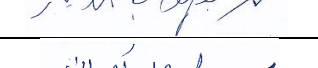
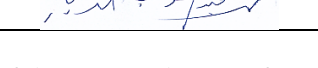
In order to draw conclusions about the new system's capacity to validate signature data from various scripts, a second set of experiments was performed. Unlike many other systems that use linked component analysis to extract all graphical features, the suggested approach does not need language-specific geometrical analysis (i.e., is text-independent). The verification rate for English signatures is approaching 100%. Still, it seems that the Arabic script yields much inferior results compared to the Western script. One probable explanation for the difference might be

that English signatures seem to exhibit greater individual style variation as compared to Arabic ones. It would seem that automatic signature verification is more challenging when dealing with Arabic script.

To see how well the proposed method works when dealing with signatures that exhibit low style variation (small change), we run additional tests. The results for the tested genuine and forged signatures are shown in Table 3. Evidently, the suggested approach is very capable of reducing FAR and FRR. The system's signature verification capabilities are somewhat degraded in some instances, especially when dealing with genuine signatures. One possible reason for this result is that, in contrast to forged signatures, which exhibit high style variations with trained genuine signatures, extracted features from some genuine signatures differ from training features, leading to a discrepancy.

Because it cannot determine all of the distinctions between the retrieved characteristics in both skilled forgery and genuine signatures, the system's ability to detect skilled forgery signatures is often diminished. To get around this issue, researchers may extract more features from the signatures (using something like a scale-invariant feature transform, for example) and use them to make the signatures more different from one another. However, processing time will be sacrificed for this. As can be seen in Table 3, the proposed approach has a commendable ability to identify non-skilled signatures. Because of this, plus the fact that we rely on geometric features to characterize the topology and geometry of a signature—preserving both its global and local properties—and because we employ two tiers of classifiers. Some degree of translation and rotation variation is also tolerable, and these features have a high tolerance for changes and style variations.

Table 3: Accuracy for style variations across tested genuine and forgery signatures

Type of style variations	Signature	Value generated by distance classifier	Value generated by Neutrosophic classifier	Final decision
Genuine signature style variations		0.187	1.431	Accepted
		0.188	1.596	Accepted
		0.158	1.291	Accepted
		0.334	1.476	Accepted
		0.412	1.546	Rejected
Forgery signature style variations		0.579	0.729	Rejected
		0.703	0.693	Rejected
		0.311	0.711	Accepted
		0.310	0.732	Accepted
		0.638	0.897	Rejected
		0.579	0.730	Rejected
		0.703	0.693	Rejected

The effectiveness of the suggested system for managing rotated signatures was tested via trials, even though the system based on the circular grid approach to extract rotation-invariant local features had already been adopted.

Fig. 7 demonstrates that the system's efficiency is unaffected and the verification accuracy remains within 98% when the signature is rotated up to 10 degrees. When the angle of rotation approaches around 42° , the verification accuracy reaches 70%, but it drops sharply thereafter. In order to determine whether circular grid segmentation of the signature or rectangular grid segmentation is better for extracting local features, the suggested system was tested with various signatures using both configurations (8 sectors with 45° in the circular grid and 25 (5×5) equal boxes), and the results were analysed in terms of FAR, FRR, and accuracy. Table 4 shows the results and reveals that circular grid segmentation produces superior results, increasing verification accuracy by at least 2%. The capacity of the circular grid segmentation to encircle stylistic variances in the signatures is, of course, the reason for this.

To demonstrate that the proposed system's verification rate depends on the number of signatures per signer, a final series of experiments was conducted. With more samples reported by each signer, the likelihood of a successful hit rises. Performance decreases as the number of samples increases (up to 40 per signer) because of increased intra-class signer variability. Due to the expected reduction in inter-class authors' variability, the verification rate drops with increasing signature counts. After 40 samples, the accuracy rate decreases by around 2-4 percent for every doubling of the signatures in the dataset .

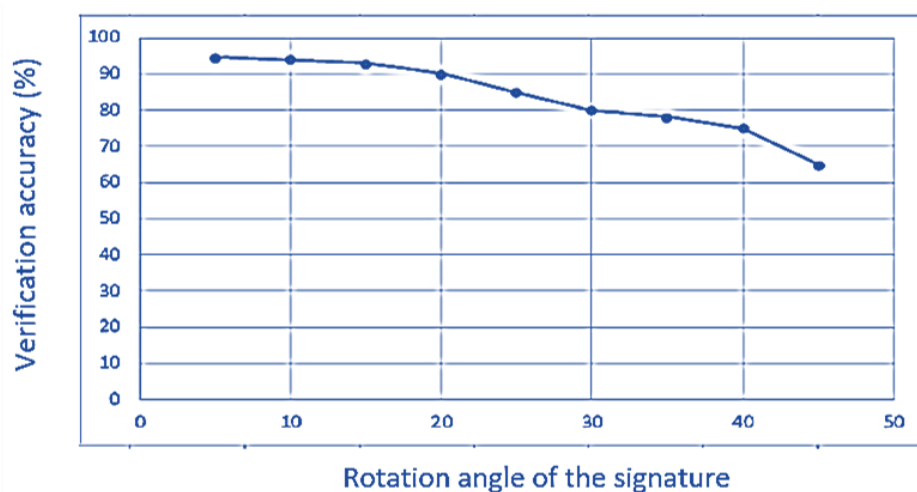


Figure 7: System accuracy under different angle rotations of signature

Table 4: System Accuracy under different type of grid segmentation.

Grid type	FRR	FAR	Accuracy
Circular grid	0.02	0.04	98 %
Rectangular grid	0.04	0.06	96 %

5. Conclusions

Two layers of verification based on similarity distance and neutrosophic notions are proposed in this study as an adaptable solution for offline signature verification. Before the verification procedure begins, the signature database is tagged. Then, the pre-processing operations and feature extraction are examined. By merging the benefits of both global and local features, a suitable mixture of both is used to produce more distinctive and effective features. A multi-classifier-based verification method is created. One of them is determined by the similarity distance between feature vectors, which compares the input signature's feature vector to the average signature in the database. In order to reach a decision with a degree of certainty, the other classifier uses neutrosophic concepts and a set of fuzzy rules. Neutrosophic logic is an extended and general framework to measure truth, indeterminacy, and falsehood that closely resembles human psychological behaviour. We achieved a verification rate of 98% in our experiments. Additionally, they proved the system's effectiveness and resilience. The proposed method outperformed competing systems in terms of success rate, implementation ease, and optimized run time because of the correctly chosen unique signature features used in conjunction with two stages of verification. Different features to improve the system's performance will be looked at in future development.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest”.

Data Availability Statement: Not applicable

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

References

- [1] Dhieb, T., Boubaker, H., Njah, S., Ben Ayed, M., Alimi, A. A novel biometric system for signature verification based on score level fusion approach. *Multimedia Tools and Applications*, 81(6):7817-7845. 2022.
- [2] Huang, J., Xue, Y., Liu, L. Dynamic signature verification technique for the online and offline representation of electronic signatures in biometric systems. *Processes*, 11(1):1-18, 190, 2023.
- [3] Jagtap, A., Sawat, D., Hegadi, R. Review on offline signature verification: datasets, methods and challenges. In *Proceedings of Third International Conference of the Recent Trends in Image Processing and Pattern Recognition, India, Revised Selected Papers, Part I 3*, pp. 458-468, Springer Singapore, 2021.
- [4] Paul, J., Dutta, K., Sarkar, A., Das, N., Roy, K. A survey on different feature extraction methods for writer identification and verification. *International Journal of Applied Pattern Recognition*, 7(2):122-144, 2023.
- [5] Alobaidi, A., Dhieb, T., Hamdani, T., Wali, A., Ouahada, K., Alimi, A. In-air signature verification system based on beta-elliptical approach and fuzzy perceptual detector, *IEEE Access*, 11(12):134058-134073, 2023.
- [6] El-Douh, A., Lu, S., Abdelhafeez, A., Ali, A., Aziz, A. Neutrosophic model for evaluation healthcare security criteria for powerful and lightweight secure storage system in cloud-based e-healthcare services. *Neutrosophic Sets and System*, 58(1): 367- 378, 22, 2023.
- [7] Hefny, A., Hassanien, A., Basha, S. Neutrosophic rule-based identity verification system based on handwritten dynamic signature analysis. *Computers, Materials & Continua*, 69(2): 2367-2385, 2021.
- [8] Alqarni, M., Samak, A., Ismail, S., Abd El-Aziz, R., Taloba, A. Utilizing a neutrosophic fuzzy logic system with ANN for short-term estimation of solar energy. *International Journal of Neutrosophic Science*, 20(4):240-240, 2023.
- [9] Zhang, K., Xie, Y., Noorkhah, S., Imeni, M., Das, S. Neutrosophic management evaluation of insurance companies by a hybrid TODIM-BSC method: a case study in private insurance companies. *Management decision*, 61(2):363-381, 2023.
- [10] Aytekin, A., Okoth, B., Korucuk, S., Karamaşa, Ç. Tirkolae, E. A neutrosophic approach to evaluate the factors affecting performance and theory of sustainable supply chain management: application to textile industry. *Management Decision*, 61(2):506-529, 2023.
- [11] Mohamed, S., Abdel-Monem, A., Tantawy, A. Neutrosophic MCDM methodology for risk assessment of autonomous underwater vehicles. *Neutrosophic Systems with Applications*, 5(1):44-52, 2023.
- [12] Rehman, A., Naz, S., Razzak, M. Writer identification using machine learning approaches: a comprehensive review. *Multimedia Tools and Applications*. 78(4):10889-10931, 2019.
- [13] Abdulhussien, A., Nasrudin, M., Darwish, S., Alyasseri, ZA. Feature selection method based on quantum inspired genetic algorithm for Arabic signature verification. *Journal of King Saud University-Computer and Information Sciences*, 35(3):141-156, 2023.
- [14] Alharbi, I. Efficient handwritten signatures identification using machine learning. *International Journal of Advanced Computer Science and Applications*, 14(3):141-148, 2023.
- [15] Zhou, Y., Zheng, J., Hu, H., Wang, Y. Handwritten signature verification method based on improved combined features. *Applied Sciences*. 11(13):1-14, 5867, 2021.
- [16] Longjam, T., Kisku, D., Gupta, P. Multi-scripted writer independent off-line signature verification using convolutional neural network. *Multimedia Tools and Applications*, 82(4):5839-5856, 2023.
- [17] Chang, S., Wu, T. Development of a signature verification model based on a small number of samples. *Signal, Image and Video Processing*, vol.2023, pp-1-10, 2023.
- [18] Alsuhimat, F., Mohamad, F. A Hybrid method of feature extraction for signatures verification using CNN and HOG a multi-classification approach. *IEEE Access*, 11(1):21873-21882, 2023.
- [19] Keykhosravi, D., Razavi, S., Majidzadeh, K., Sangar, A. Offline writer identification using a developed deep neural network based on a novel signature dataset. *Journal of Ambient Intelligence and Humanized Computing*, 4(9):12425-12441, 2023.

- [20] Djoudjai, M., Chibani, Y. Open writer identification from offline handwritten signatures by jointing the one-class symbolic data analysis classifier and feature-dissimilarities. *International Journal on Document Analysis and Recognition*, 26(1):15-31, 2023.
- [21] Batool, F., Attique, M., Sharif, M., Javed, K., Nazir, M., Abbasi, A., Iqbal, Z., Riaz, N. Offline signature verification system: a novel technique of fusion of GLCM and geometric features using SVM. *Multimedia Tools and Applications*. 79(3): 1-20, 2020.
- [22] Banerjee, D., Chatterjee, B., Bhowal, P., Bhattacharyya, T., Malakar, S., Sarkar, R. A new wrapper feature selection method for language-invariant offline signature verification. *Expert Systems with Applications*. 186(1):1-20, 115756, 2021.
- [23] Anisimova, E., Anikin, I. Finding a rational set of features for handwritten signature recognition. In *Proceedings of the International Conference on Dynamics of Systems, Mechanisms and Machines (Dynamics)*, pp. 1-6, 2020.
- [24] Liu, J., Fung, G. Signature verification based on a fuzzy genetic algorithm. In *Knowledge-Based Intelligent Techniques in Character Recognition*, pp. 121-148, CRC Press, 2020.
- [25] Anisimova, E., Anikin, I. Fuzzy sets theory approach for recognition handwritten signatures. In *Proceedings of the International Russian Automation Conference, Sochi, Russia*, pp. 969-982, Springer International Publishing, 2021.
- [26] Meshram, C., Alsanad, A., Tembhurne, J., Shende, S., Kalare, K., Meshram, S., Akbar, M., Gumaee, A. A provably secure lightweight subtree-based short signature scheme with fuzzy user data sharing for human-centered IoT. *IEEE Access*, 9(3):3649-3659, 2020.
- [27] Adeyemi, B., Olaoye, O., Uchehara, C., Akinola, O., Sunmola, F. Adoption of off-line signature verification and forgery detection system using additive fuzzy and TS modelling technique in financial auditing and forensics investigation. *International Journal of Computer Science and Mobile Computing*, 10(6): 38-59, 2021.
- [28] Bibi K, Naz S, Rehman A. Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. *Multimedia Tools and Applications*, 79(1-2):289-340. 2020.
- [29] Houtinezhad, M., Ghaffary, H. Writer-independent signature verification based on feature extraction fusion. *Multimedia Tools and Applications*, 79(9-10):6759-6779, 2020.
- [30] Makkar, G., Goyal, P. Combined static and dynamic features extraction from handwritten signature. *Scandinavian Journal of Information Systems*, 35(1):468-4675, 2023.
- [31] Chompookham, T., Gonwirat, S., Lata, S., Phiphatphaisit, S., Surinta, O. Plant leaf image recognition using multiple-grid based local descriptor and dimensionality reduction approach. In *Proceedings of the International Conference on Information Science and Systems*, pp. 72-77, 2020.
- [32] Priya, I., Chaurasia, N. Estimating the Effectiveness of CNN and Fuzzy Logic for Signature Verification. In *Proceedings of the Third International Conference on Secure Cyber Computing and Communication*, pp: 1-6, 2023.
- [33] Yue, W., Wan, X., Li, S., Ren, H., He, H. Simplified neutrosophic petri nets used for identification of superheat degree. *International Journal of Fuzzy Systems*, vol. 24, no. 8, pp. 3431-3455, 2022.
- [34] S. Pai, and R. Gaonkar. Safety modelling of marine systems using neutrosophic logic. *Journal of Engineering for the Maritime Environment*, vol. 235, pp. 225-235, 2021.
- [35] Rajarao, B., Renuka, M., Sowjanya, K., Krupa, K., Babbitha, M. Offline signature verification using convolution neural network. *Industrial Engineering Journal*, 52(4): 1087- 1101, 2023.