International Journal of Innovative Computing, Information and Control
Volume **17**, Number **5**, October **2021**

ICIC International ©2021 ISSN 1349-4198
pp. 1691–1703

MULTIMODAL BIOMETRIC FUSION ONLINE HANDWRITTEN SIGNATURE VERIFICATION USING NEURAL NETWORK AND SUPPORT VECTOR MACHINE

Orieb AbuAlghanam[1], Layla Albdour[2] and Omar Adwan[3,4]

[1]Department of Networks and Information Security
[3]Department of Computer Science
Al-Ahliyya Amman University
Amman 19328, Jordan
{ O.AbuAlghanam; adwanoy }@ammanu.edu.jo

[2]Department of Computer Science
[4]Department of Computer Information System
University of Jordan
Aljubeiha, Amman 11942, Jordan
Bdourlaila@gmail.com; adwanoy@ju.edu.jo

Received March 2021; revised July 2021

Abstract. *The handwritten signature is the most widely accepted biometric scheme used to verify an individual's identity. Recently, smart devices, such as tablets, PCs and smartphones, have become widespread around the world, thus making it easier to verify anyone's identity using a handwritten signature and to differentiate whether the signature is real or not. In this paper, we propose two models for an online handwritten signature verification system to enhance the accuracy of prediction and decrease the equal error rate. The first model is based on the neural network classifier used to verify online handwritten signatures. The second model is based on a multimodal called a fusion model. In conducting the experiments, an MCYT-100 benchmark dataset was used to test and evaluate the proposed methods. The results indicate that the first proposed model achieves 3.8% EER compared to other related proposals. Moreover, the multimodal achieved 1.3% EER compared to other multimodal alternatives and outperformed the first model. Also, the second model shows an enhancement and better performance by decreasing the EER approximately 2.5% compared to the first model.*

Keywords: Biometrics-based security, SVM, Online handwritten signature verification, Neural network

1. **Introduction.**

Nowadays, security demands are increasing worldwide by individuals and organizations. Several researchers have attempted to improve and develop the security schemes such as key distribution techniques [1] and several proposals for enhancing intrusion detection systems have been put forth [2].

Cybersecurity has become one of the most important issues these days for digital data [3,4]. One of the most important techniques used to provide security for digital applications is biometric security. Biometric security is defined by human characteristics that help to distinguish one person from another; this type of security can be classified either physiologically or behaviorally as shown in Figure 1. The human face, retinal, fingerprint, and iris are considered as the physiological characteristics that cannot change while the voice, keystroke dynamics and handwritten signature as well as others are considered as examples of the behavioral class [5,6]. The handwritten signature verification has been

DOI: 10.24507/ijicic.17.05.1691

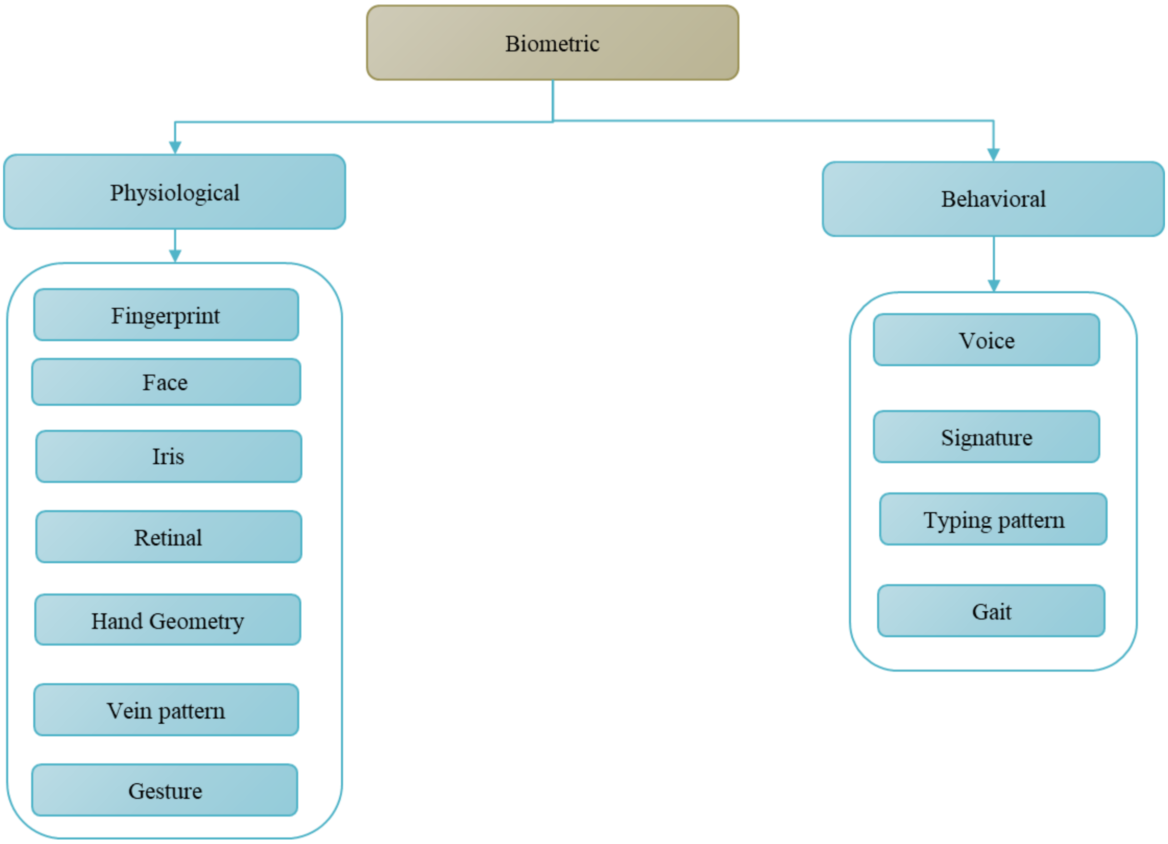

Figure 1. General biometric classification [11]

widely applied in biometrics and forensics fields. Moreover, an important issue, which can be solved using biometric security, is distinguishing genuine and forged signatures, since the handwritten signature is used widely for numerous applications including bank transactions [7,8].

Handwritten signature verification (HSV) systems tend to verify the identity of an individual based on signature analysis. The online handwritten signature is used in many applications and is considered a personal authentication [9,10]. Moreover, handwritten verification is one of the most widely used biometric security systems.

Several studies have been proposed for both offline and online handwritten signature verification systems. They differ from each other primarily based on the data acquisition method, the data preprocessing, or the model that is used. Nowadays, due to the increased use of E-services, E-commerce, and E-government, and due to the spread use of smart devices [12], the online signature is used over offline environments. There are two approaches for signature verification, which are as follows.

- Online approach: In this approach, the signer uses an optical pen for writing. At this time many physical characteristics should be taken into consideration such as the velocity of movement of the hand, acceleration between hand strokes, and pressure exerted at various positions.
- Offline approach: This approach is for signatures written on paper. It uses an optical scanner to obtain the signature. In offline signature verification, a set of geometrical, spatial and moment features is used for the comparison processes [13].

This paper focuses on the online handwritten signature verification, which is widely used in many applications for authentication purposes. The MCYT-100 signature dataset is used to compare the results with state-of-the-art works.

1) Propose a classifier model to improve the accuracy for classifying the genuine and the foreign handwritten signature for online handwritten signature based on neural network models and Hu seven values.
2) Propose a MultiModal that is based on the first model by adding support vector machine to neural network to be a fusion (MultiModal). In addition, we apply feature selection techniques. The main object from the MultiModal is to reduce EER at the first model.

The rest of this paper is organized as follows. Section 2 introduces related literature. Section 3 proposes the architecture design and settings. Section 4 presents the results and analysis. Finally, we conclude the paper in Section 5.

2. **Literature Review.** Nowadays, smartphones enable to access a large variety of services like voice communication, data storage, and wireless connectivity. However, an increasing number of services leads to an increased risk of vulnerabilities and attacks, which leads to a corresponding rise of security solutions proposed by researchers for authentication in smartphones, like passwords, secret paths, and signature verification. Online biometric signature verification is considered as one of the most popular authentication mechanisms. People adopt this mechanism due to its nature, which is most secure, fashionable, trustable and difficult for unauthorized persons to breach privacy with.

In [14], an online handwritten signature verification scheme was presented to solve the problem as a two-class pattern recognition problem. A test signature's authenticity uses dynamic time warping and determines the distance between the reference signature and the test signature's nearest and farthest one. In [15] an online Arabic handwritten signature recognition system was proposed. It aims to improve the method for detecting desired critical points from vertical and horizontal direction-length of handwriting stroke features of online Arabic script recognition, as is proposed in this study.

In [16], two methods were proposed for selecting discriminative features to improve the robustness and to reduce the fluctuation of the internal and external environments when the signature is written. In [16] the MCYT-100 dataset is used to show the algorithm's efficiency; a modified DTW with SCC is presented. On the other hand, different studies in the literature have used the MCYT-100 dataset to evaluate the performance of their model and to classify the real or forger signatures.

Several studies in the literature have presented an enhancement for the accuracy of the classifier or for the model by selecting the most important feature in the dataset. In [17], a Kd-tree indexing mechanism was proposed to index the prior features for a faster identification method. Moreover, in [18], the empirical mode decomposition (EMD) method was devised to verify handwritten signatures and used two datasets, one of which was the MCYT-100. Also, for preprocessing in the experiment datasets, many kinds of normalizations were performed before applying EMD. In [19], the authors proposed a signature verification model based on image-based handwritten signatures that are considered important when a hard copy of the signature is needed. Due to less dynamicity in static image-based signatures, they proposed a hybrid method probabilistic neural network (PNN), principal component analysis (PCA), and discrete Radon transform (DRT). They aimed to distinguish forgery signatures from genuine ones by working on the image level. The proposed method of evaluation was conducted on the authors' independent database as well as the MCYT-100 database.

In recent years, the effectiveness of multimodal systems has been noted due to their advantages in providing greater security in comparison to unimodal systems, and due to the fact that they showed better accuracy and less EER [20]. The multimodal approach combines two or more factors/biometrics, such as the iris and fingerprint, or uses two different classifiers, such as NN and SVM. Experimental studies have found that the identities established by systems that use more multi-biometrics have much better results and much better performance than the systems that use single biometrics, especially when applied to large target populations. In [21], the authors used Levenshtein distance string matching algorithm, Damerau-Levenshtein distance, and Sift3.

Several fusion models or multimodal handwritten signatures have been proposed in literature. In [22], a secure multimodal biometric system by fusing an electrocardiogram (ECG) and fingerprint based on a convolution neural network (CNN) was proposed. Moreover, in [23], a novel multimodal biometric user authentication system was proposed to limit unauthorized access by combining the behavioral dynamic signature with the physiological electroencephalograph (EEG). The offline handwritten signature was suggested to use geometric features in [24,25]. Twenty-two GLCM and eight geometric elements are used in total. Each feature's four metrics are calculated: mean, range, variance, and entropy. As a result, 1 × 88 features were developed, which were later combined with geometric features.

The neural network model is highly desired for classification or for predicting purposes [23,26]. It has been noticed that many proposals use neural network to enhance the accuracy of the model. Moreover, in [26] an NN is used on the semantic and syntactic aspects of the language to introduce an extension of the NMT model that effectively incorporates additional part-of-speech (POS) tags into the attention system to produce even better results.

In this paper, we differ with other related previous studies, we exploit the benefits of the neural network model and use Hu seven values to enhance the accuracy of the model by presenting less value for EER%. Also, we develop a multimodal that reaps the benefits of the first model and add another SVM model. We select the important features which show how it outperforms the second model, which has not been done before. Also, we used two separate algorithms to take advantage of the benefits of both, in addition to improving the way of selecting the most important feature in the online handwritten signature, and that sets us apart from other fusion proposals.

3. Proposed Architecture Design and Settings.

Artificial neural networks (ANNs) were created in the 1940s, and were known as neural networks (NN). The artificial neural network is a mathematical model inspired by the observation of neural network processing in biological neural networks and the human nervous system. ANN aims to create a way to process the data rapidly just like the human brain. An ANN consists of simple computational elements (called neurons) and connections between them with weights [27].

Proposed by McCulloch and Pitts [44], the threshold logic unit (TLU) was the first artificial neuron model. It mainly depends on a binary system where the inputs and outputs are binary values, and use a fixed activation function. The basic components of a neural network are inputs with weights on input connections, input functions that calculate an input signal entering to the neuron, an activation function that calculates the activation level in order to stimulate neuron production, and finally, an output function that calculates the output signal after threshold reaches a specific level. As shown in Table 1, 134 features are used for the signature verification system, Min, Max, Mean, and Standard Deviation are called image moment invariants. The features are used as input for the backpropagation NN.

Global features of the image are recognized by moment and functions moment. They are used for object recognition despite the signature image orientation, size, and position. A non-linear moment invariant function is used to compute the feature vector of the signature. The signature shape is described by a set of features using algebraic invariants.

Table 1. Signature features

Feature	Description	Feature	Description
f1: Pressure	Min (p)	f17: Euclidian distance	$d(x, y) = \sqrt{\sum_{i=1}^{n} (xi - yi)^2}$
f2: Pressure	Max (p)	f18: Duration	Time spent during signing
f3: Pressure	Mean (p)	f19: Pen up	when $p = 0$
f4: Pressure	Standard deviation (p)	f20: X	Min (x)
f5: Azimuth	Min (az)	f21: X	Max (x)
f6: Azimuth	Max (az)	f22: X	Mean (x)
f7: Azimuth	Mean (az)	f23: X	Standard deviation (x)
f8: Azimuth	Standard deviation (az)	f24: Y	Min (y)
f9: Altitude	Min (a)	f25: Y	Max (y)
f10: Altitude	Max (a)	f26: Y	Mean (y)
f11: Altitude	Mean (a)	f27: Y	Standard deviation (y)
f12: Altitude	Standard deviation (a)	50 features: X	50 points after normalization
f13: X start	$x0$	50 features: Y	50 points after normalization
f14: X end	xn	7 features Hu moment invariant	Shape descriptors Equation (5) (Hu equations values [28])
f15: Y start	$y0$		
f16: Y end	yn		

In this section, we discuss the two proposed models that are used to verify the handwritten signature. Moreover, the description of each model is detailed in the subsections that follow, in addition to presenting a brief description about the phases in each model.

3.1. **First proposed model.** The first model, as shown in Figure 2, is a combination of general authentication (i.e., user name and password) and the handwritten signature biometric. The main basic phases are data acquisition, data preprocessing, feature extraction, and the verification process. Based on the advantage of neural networks (NN) backpropagation paradigm, we mainly used NN classification algorithms to build the verification model.

Moreover, global features of the image are recognized by moment and functions moment, which are used for object recognition despite the signature image orientation, size, and position. A non-linear moment invariant function is used to compute the feature vector of the signature. The signature shape is described by a set of features using algebraic invariants.

In two-dimensional moments of a digitally sampled $M \times M$ image that has gray function $f(x, y)$, $(x, y = 0, \ldots, M-1)$, the two-dimensional moment is given by Equations (1) and (2) to convert the input signature from image to matrix and select the most important pixels.

$$m_{pq} = \sum_{x=0}^{x=M-1} \sum_{y=0}^{y=M-1} (x)^p \cdot (y)^q f(x, y) \tag{1}$$

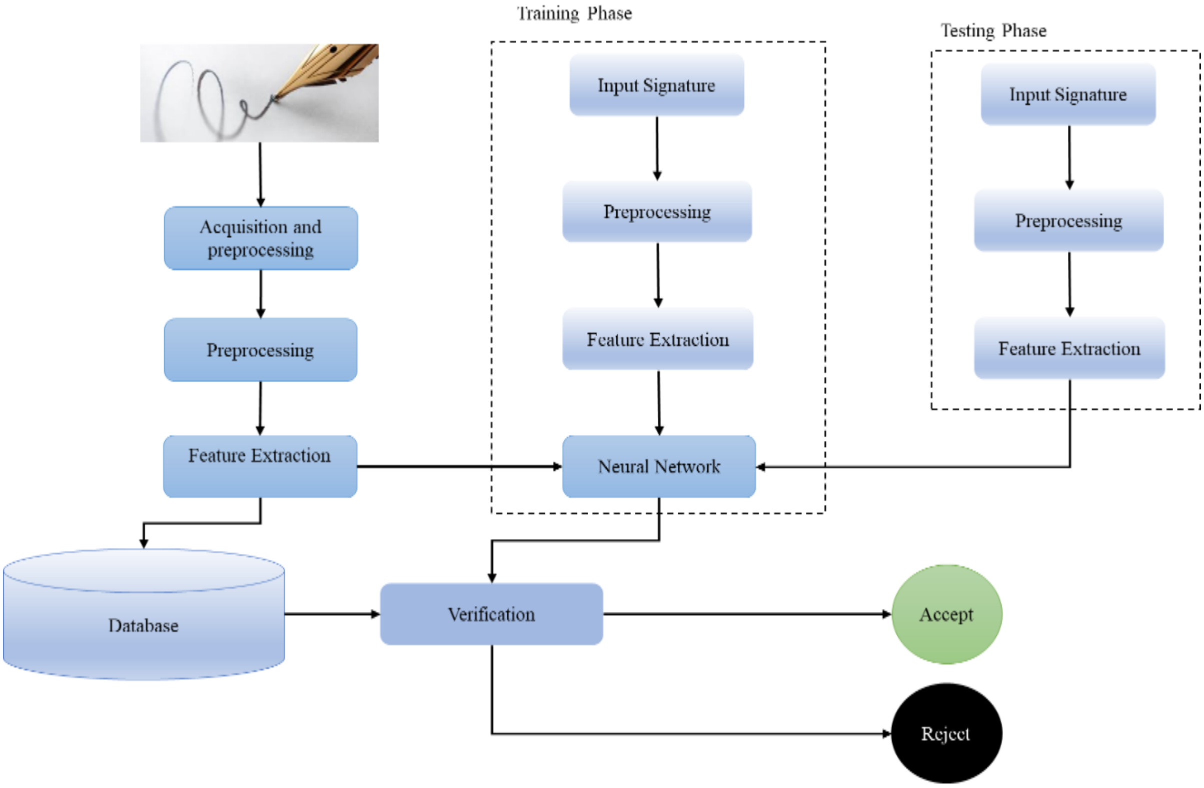

FIGURE 2. Neural network model for online handwritten verification

The moments $f(x,y)$ translated by an amount (a,b), are defined as:

$$\mu_{pq} = \sum_x \sum_y (x+a)^p \cdot (y+b)^q f(x,y) \tag{2}$$

The central moments m'_{pq} or μ_{pq} are computed from (2) by substituting $a = -\bar{x}$ and $b = -\bar{y}$ as, $\bar{x} = \frac{m_{10}}{m_{00}}$ and $\bar{y} = \frac{m_{01}}{m_{00}}$,

$$\mu_{pq} = \sum_x \sum_y (x-\bar{x})^p \cdot (y-\bar{y})^q f(x,y) \tag{3}$$

After applying scaling and normalization, the central moment will be defined as:

$$\eta_{pq} = \mu_{pq}/\mu_{00}^{\gamma}, \quad \gamma = [(p+q)/2]+1 \tag{4}$$

Hu and Peng [28] defined seven values, as illustrated in Figure 3. These values are computed by order three for the normalized central values, which are invariant to signature position, orientation or scale. Regardless of the orientation, height, or scale, these seven shape descriptors are used to define the shape of the signature. Since the Min, Max, Start, End, and Euclidean distance are all affected by the signature scale, we normalize it. The normalization process tends to reduce all signature sizes to 52 points.

Preprocessing step. The following is a brief summary of the input dataset, the preprocessing steps using Hu seven values, and the image of handwritten signature changes that occur as a result of these steps.

- The signatures are reconstructed as input and after that, each input which is an image signature is converted to image and it is a set of x, y coordinates.
- The dataset is not imaged, and it is a set of x, y coordinates. Those coordinates are guidelines for the signature image.

- Then the image of the signature is drawn depending on x, y and we fill the gaps between them.
- We load the image and calculate the Hu moment invariant, which are 7 features that describe the shape of the signature image regardless of the orientation.
- We extract the rest of the features by using row values of x, y, pressure, altitude, and azimuth that are described in the dataset.
- The 134 features are used as input for NN for training and testing dataset.

$$M_1 = (\mu_{20} + \mu_{02}).$$

$$M_2 = (\mu_{20} + \mu_{02})^2 + 4\mu_{11}{}^2.$$

$$M_3 = (\mu_{30} - 3\mu_{12})^2 + (3\mu_{21} - \mu_{03})^2.$$

$$M_4 = (\mu_{30} + \mu_{12})^2 + (\mu_{21} + \mu_{03})^2.$$

$$M_5 = (\mu_{30} - 3\mu_{12})^2(\mu_{30} + \mu_{12})[(\mu_{30} - \mu_{12})^2 - 3(\mu_{21} + \mu_{03})^2] + (3\mu_{21} - \mu_{03})\ (\mu_{21} + \mu_{03})[\ 3(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2].$$

$$M_6 = (\mu_{20} + \mu_{02})[(\mu_{30} - \mu_{12})^2 - (\mu_{21} - \mu_{03})^2] + 4\mu_{11}\ (\mu_{30} - \mu_{12})\ (\mu_{21} - \mu_{03}).$$

$$M_7 = (3\mu_{21} - \mu_{03})(\mu_{30} + \mu_{12})[(\mu_{30} - \mu_{12})^2 - 3(\mu_{21} + \mu_{03})^2] - (\mu_{30} - 3\mu_{12})\ (\mu_{21} + \mu_{03})[3(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2].$$

FIGURE 3. Hu equations values [28]

3.2. **Second proposed model.** In the second multimodal, as shown in Figure 4, we applied some modifications on the first modal that included adding a support vector machine algorithm, and applied a feature selection to selecting the important features and to enhancing the accuracy for classification in online handwritten signatures.

The basic concept of segmentation is focused on the distribution of points on both sides of a local-maximum value pixel; this aids in providing an intrinsic information structure to handwriting patterns and reduces the impact of abrupt changes in direction and/or extremely short breaks. In machine learning or pattern recognition applications, feature selection methods enable us to reduce computation time, improve prediction accuracy, and gain a better understanding of the data. In this paper, the MTCY-100 dataset is used, which is imaged for handwritten signatures, and thus contains a huge number of features that are needed to cope with. In the multimodal, feature selection techniques have been used to enhance the classification results. Correlation criteria are used for filtering the features that have related dependency with the label class.

4. **Experimental Results and Analysis.**

4.1. **The MCYT-100 database.** Several studies use the open access online signature database MCYT-100 [29], which contains signatures for 100 different individuals, each one having 25 genuine signatures and 25 skilled forgery signatures. Figure 5 shows a sample of the MCYT-100 database which contains 100 global features; some studies use all these features while others select some of these features by, for example, ranking these features from the most prior one or by selecting the first 20 features. Many proposed algorithms used the MCYT-100 signature database in their experiments to evaluate the performance of the proposed methods. In our approach we used all features, and some of them were modified in order to enhance the accuracy.

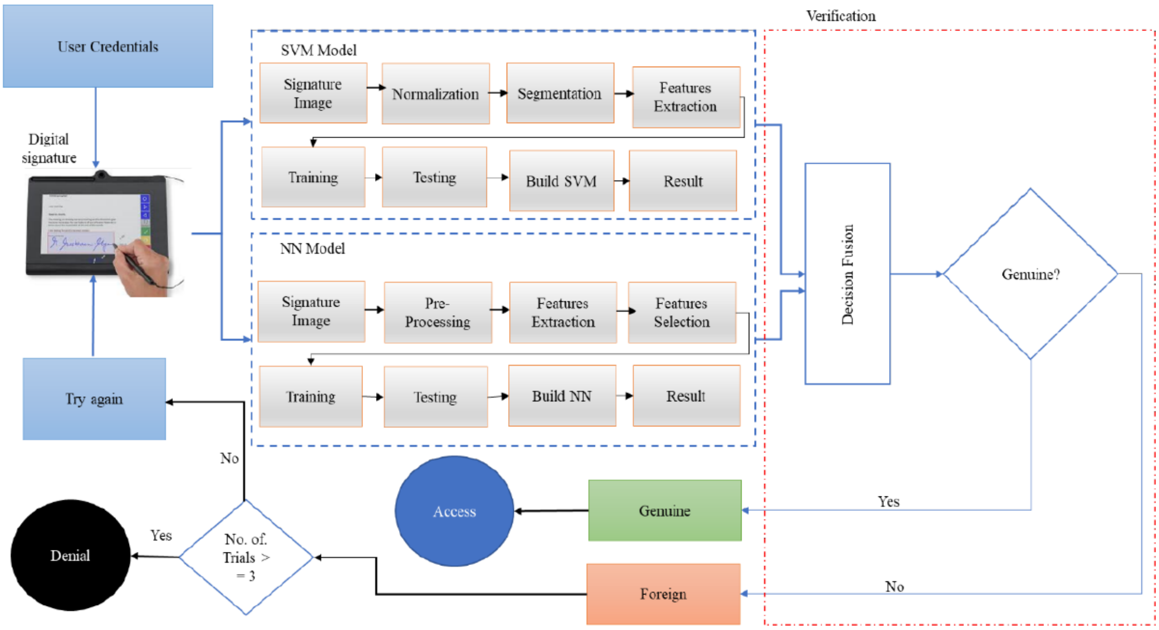

FIGURE 4. Fusion multimodal for online handwritten verification

FIGURE 5. Sample of MCYT-100 handwritten signature

4.2. **Performance metrics.** In any handwritten signature verification model, there are different performance metrics that are used. Equal error rate (EER) is one of the most popular biometric security system performance metrics used to predetermine the threshold values, given its false acceptance rate and its false rejection rate. The performance of signature verification systems is measured in two ways. The false rejection rate (FRR) shows the percentage of genuine signatures that the system considers as forgeries. On the other hand, the false acceptance rate (FAR) measures the percentage of forged signatures that the system accepts as genuine ones. The performance of any classification algorithm is measured using these metrics. The acceptance and the rejection rates depend on a threshold predefined in the classification algorithm [15]. For instance, when we accept every input signature, the FRR is 0% and the FAR is 100%. On the other hand, if the opposite happens and we reject every signature, the FRR is 100% and the FAR is 0%. The error trade-off curve is the FAR as a function of FRR [30].

4.3. **Comparative studies.** A standard online signature database MCYT-100 is used in our work. The experiments for the first model, which is a neural network, were done multiple times and the average was taken for them; the EER was 3.8%. In order to show the effectiveness of our proposed method, we used a backpropagation paradigm. The first time, the number of hidden layers was 60, and the second time it was 90. Our experiments were characterized by using Hu equations, which were added to the features of the original dataset.

Table 2 shows a comparison between different related signal models for handwritten signature verification systems using the MCYT-100 dataset. It can be noticed that the proposals differ from one another based on the number of features that are selected and the method of classification that is used. The number of features that are selected in some previous experiments used some of these features because the used classifier for them could not use a large number of features. Therefore, a specific group of features were selected and used instead. In our proposed model the result of experiments showed better results and outperformed other related works.

Table 2. Different signature features for MCYT-100 dataset

Reference	Number of features	Method	EER%
[31]	14 local features	HMM	8.20
[32]	x, y, p, r, θ	Manhattan distance	4.02
[33]	6 features	DTW	13.56
[34]	All features	Linear programming descriptor classifier (LPD)	5.2
[35]	All features	User-specific global-parameter fusion model	4
[36]	All features	Feature warping + Gaussian mixture models	10.86
[37]	All features	Polynomial	4.22
[38]	All features	Fourier	10.89
[39]	x, y, azimuth	Discrete cosine transf. + Wavelet transf.	9.80
Our first model	All features	NN	3.8

Figure 6 shows the percentage of EER for all related previous studies that were illustrated in Table 2. As can be noticed, the error rate was different from one study to another, such as the fact that the number of features may be the same while the error rate is different depending on the verification approach from one study to another, but in general increasing the number of features decreases the error rate taking consideration of feature extraction and feature selection. For example, when using the highest number or selecting a significant feature, the error rate was at its lowest.

In the second proposed model, which is a fusion model, the results show less EER%, which was 1.3% compared with the first proposed model that reached 3.8% EER. Table 3 shows the comparisons between each multimodal used for online handwritten signature verification for the same datasets. It can be noticed that in [41,43], when the feature selection is used, the EER% is reduced compared with others that use all features. Moreover, in [40,42], all features were used in the classifier model and it can be noticed that the results gave a higher EER% compared with others. On the other hand, using a fusion model for classification gave better results than using a single model.

In Figure 7, the proposed fusion model outperforms other related fusion models that also used the MCYT-100 dataset. In our fusion model we achieved 1.3%, which is considered a less EER% compared with the others.

5. **Conclusion.**

In a big data era, the demand for verification and authentication models that achieve high performance and accuracy are essential. This paper presented two

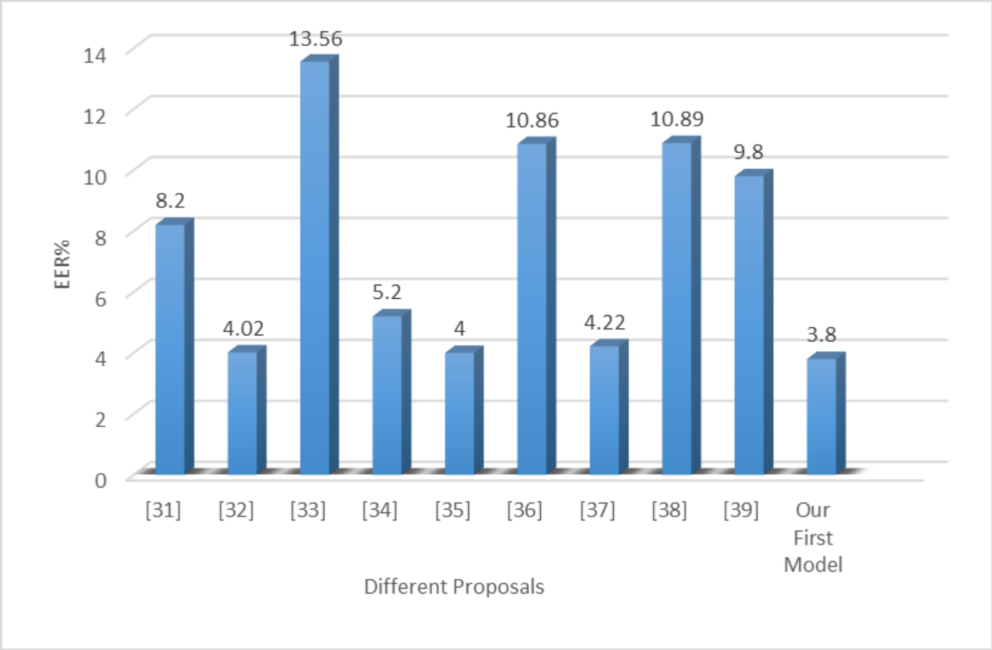

Figure 6. Comparison results for related proposals in the literature in terms of EER% for single model

Table 3. Comparison in terms of EER% of the proposed fusion model against the recent models on MCYT-100 database

Reference	Number of features	Method	EER%
[40]	All features	DTW and GMM	2.12
[41]	Feature selection	Deep learning + DTW	2.40
[42]	All features	Representation learning + DTW	3.16
[43]	Feature selection	Curvature feature + Torsion feature	1.81
Our fusion model	Feature selection	NN + SVM	1.3

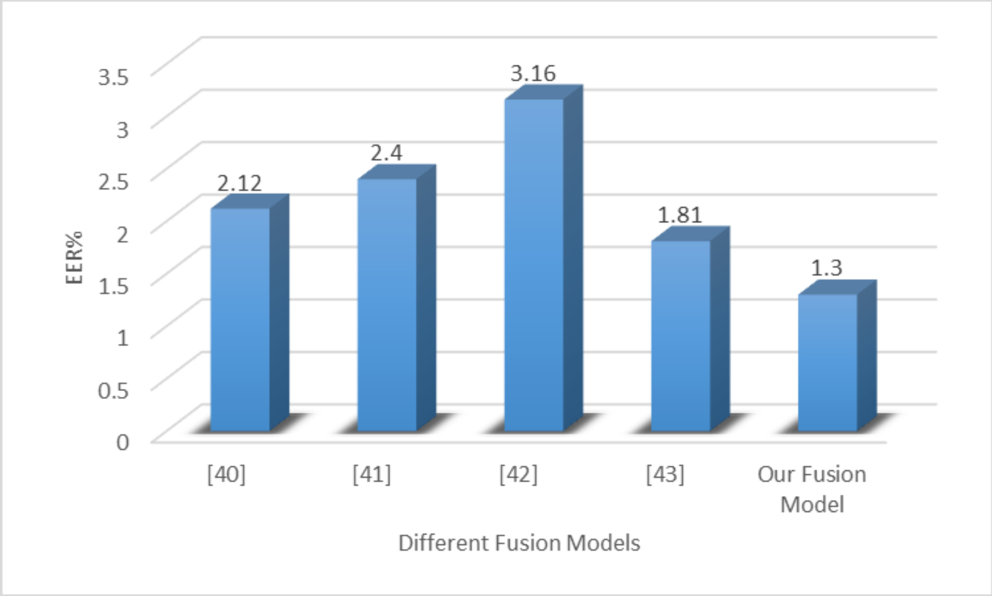

Figure 7. Comparison results for related proposals in the literature in terms of EER% for multimodal

handwritten signature verification models. The first model was based on a neural network backpropagation classifier method for online handwritten signature verification using Hu seven values that are used for the preprocessing step to reduce EER%. Hu moment invariants, which are seven features, in addition to the original features, were used to distinguish genuine from forged signatures. Moreover, a special purpose normalization was used to equalize the sizes of used signatures. The used features can differentiate the signatures regardless of the size, orientation, scale or rotation of the signatures. The second model was a fusion model that contains two different classifiers, which are SVM and NN, in addition to a feature selection technique. The experiments were done on the MCYT-100 dataset. The accuracy of our first online handwritten signature verification system is 3.8%, which is a very good result compared to previous studies. Also, the proposed fusion multimodal outperformed by achieving 1.3% EER compared to the other related fusion models in literature. To the best of our knowledge, this is the first paper that is used these methods and techniques to verify a handwritten signature. In the future, instead of neural network backpropagation, a deep learning framework will be utilized to extract features. Moreover, an appropriate feature selection technique will be used to reduce the EER%.

REFERENCES

[1] O. AbuAlghanam, M. Qatawneh and W. Almobaideen, A survey of key distribution in the context of Internet of Things, *Journal of Theoretical and Applied Information Technology*, vol.97, no.22, 2019.

[2] H. Alazzam, A. Sharieh and K. E. Sabri, A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer, *Expert Systems with Applications*, vol.148, 113249, 2020.

[3] Z. El Mrabet, N. Kaabouch, H. El Ghazi and H. El Ghazi, Cyber-security in smart grid: Survey and challenges, *Computers & Electrical Engineering*, vol.67, pp.469-482, 2018.

[4] M. Qatawneh, W. Almobaideen and O. AbuAlghanam, Challenges of blockchain technology in context Internet of Things: A survey, *International Journal of Computer Applications*, vol.175, no.16, pp.13-20, 2020.

[5] A. K. Jain, A. Ross, S. Prabhakar et al., An introduction to biometric recognition, *IEEE Transactions on Circuits and Systems for Video Technology*, vol.14, no.1, 2004.

[6] S. Dargan and M. Kumar, A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities, *Expert Systems with Applications*, vol.143, 113114, 2020.

[7] B. Ribeiro, N. Lopes and C. Silva, Learning the hash code with generalised regression neural networks for handwritten signature biometric data retrieval, *2015 International Joint Conference on Neural Networks (IJCNN)*, pp.1-6, 2015.

[8] M. Okawa, Template matching using time-series averaging and DTW with dependent warping for online signature verification, *IEEE Access*, vol.7, pp.81010-81019, 2019.

[9] F. Leclerc and R. Plamondon, Automatic signature verification: The state of the art – 1989-1993, *International Journal of Pattern Recognition and Artificial Intelligence*, vol.8, no.3, pp.643-660, 1994.

[10] S. Shariatmadari, S. Emadi and Y. Akbari, Patch-based offline signature verification using one-class hierarchical deep learning, *International Journal on Document Analysis and Recognition (IJDAR)*, vol.22, no.4, pp.375-385, 2019.

[11] M. Obaidat and N. Boudriga, *Security of E-Systems and Computer Networks*, Cambridge University Press, 2007.

[12] M. Saleemi, M. Anjum and M. Rehman, eServices classification, trends, and analysis: A systematic mapping study, *IEEE Access*, vol.5, pp.26104-26123, 2017.

[13] A. Kumar and K. Bhatia, A survey on offline handwritten signature verification system using writer dependent and independent approaches, *2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall)*, pp.1-6, 2016.

[14] A. Kholmatov and B. Yanikoglu, Identity authentication using improved online signature verification method, *Pattern Recognition Letters*, vol.26, no.15, pp.2400-2408, 2005.

[15] A. Rehman, Neural computing for online Arabic handwriting character recognition using hard stroke features mining, *arXiv Preprint*, arXiv: 2005.02171, 2020.

[16] X. Xia, X. Song, F. Luan, J. Zheng, Z. Chen and X. Ma, Discriminative feature selection for on-line signature verification, *Pattern Recognition*, vol.74, pp.422-433, 2018.

[17] K. Nagasundara, S. Manjunath and D. Guru, Indexing of online signatures, *International Journal of Machine Intelligence*, vol.3, no.4, pp.289-294, 2011.

[18] T. Hafs, L. Bennacer, M. Boughazi and A. Nait-Ali, Empirical mode decomposition for online handwritten signature verification, *IET Biometrics*, vol.5, no.3, pp.190-199, 2016.

[19] S. Y. Ooi, A. B. J. Teoh, Y. H. Pang and B. Y. Hiew, Image-based handwritten signature verification using hybrid methods of discrete Radon transform, principal component analysis and probabilistic neural network, *Applied Soft Computing*, vol.40, pp.274-282, 2016.

[20] G. S. Walia, T. Singh, K. Singh and N. Verma, Robust multimodal biometric system based on optimal score level fusion model, *Expert Systems with Applications*, vol.116, pp.364-376, 2019.

[21] N. Forhad, B. Poon, M. A. Amin and H. Yan, Online signature verification for multi-modal authentication using smart phone, *Proc. of the International Multiconference of Engineers and Computer Scientists*, vol.1, 2015.

[22] M. Hammad and K. Wang, Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network, *Computers & Security*, vol.81, pp.107-122, 2019.

[23] P. Kumar, R. Saini, B. Kaur, P. P. Roy and E. Scheme, Fusion of neuro-signals and dynamic signatures for person authentication, *Sensors*, vol.19, no.21, 4641, 2019.

[24] F. E. Batool, M. Attique, M. Sharif, K. Javed, M. Nazir, A. A. Abbasi, Z. Iqbal and N. Riaz, Offline signature verification system: A novel technique of fusion of GLCM and geometric features using SVM, *Multimedia Tools and Applications*, pp.1-20, 2020.

[25] F. Albregtsen, *Statistical Texture Measures Computed from Gray Level Coocurrence Matrices*, Image Processing Laboratory, Department of Informatics, University of Oslo, https://www.uio.no/studier/emner/matnat/ifi/INF4300/h08/undervisningsmateriale/glcm.pdf, pp.1-14, 2008.

[26] L. H. B. Nguyen, H. D. Minh, D. Dinh and T. L. Manh, Improving neural machine translation with POS tags, *ICIC Express Letters, Part B: Applications*, vol.12, no.1, pp.91-98, 2021.

[27] J. J. Hopfield, Neural networks and physical systems with emergent collective computational abilities, *Proceedings of the National Academy of Sciences*, vol.79, no.8, pp.2554-2558, 1982.

[28] Y. Hu and S. Peng, Adapted solution of a backward semilinear stochastic evolution equation, *Stochastic Analysis and Applications*, vol.9, no.4, pp.445-459, 1991.

[29] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho et al., MCYT baseline corpus: A bimodal biometric database, *IEE Proceedings – Vision, Image and Signal Processing*, vol.150, no.6, pp.395-401, 2003.

[30] A. K. Jain, K. Nandakumar and A. Nagar, Biometric template security, *EURASIP Journal on Advances in Signal Processing*, vol.2008, p.113, 2008.

[31] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia and A. Neri, Cancelable templates for sequence-based biometrics with application to on-line signature recognition, *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, vol.40, no.3, pp.525-538, 2010.

[32] N. Sae-Bae and N. Memon, Online signature verification on mobile devices, *IEEE Transactions on Information Forensics and Security*, vol.9, no.6, pp.933-947, 2014.

[33] M. Diaz, A. Fischer, M. A. Ferrer and R. Plamondon, Dynamic signature verification system based on one real signature, *IEEE Transactions on Cybernetics*, vol.48, no.1, pp.228-239, 2016.

[34] D. Muramatsu and T. Matsumoto, Online signature verification algorithm with a user specific global-parameter fusion model, *2009 IEEE International Conference on Systems, Man and Cybernetics*, pp.486-491, 2009.

[35] A. Nautsch, C. Rathgeb and C. Busch, Bridging gaps: An application of feature warping to online signature verification, *2014 International Carnahan Conference on Security Technology (ICCST)*, pp.1-6, 2014.

[36] E. Maiorana, P. Campisi, D. La Rocca and G. Scarano, Use of polynomial classifiers for on-line signature recognition, *2012 IEEE 5th International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pp.265-270, 2012.

[37] B. Yanikoglu and A. Kholmatov, Online signature verification using fourier descriptors, *EURASIP Journal on Advances in Signal Processing*, vol.2009, no.1, 260516, 2009.

[38] L. Nanni and A. Lumini, A novel local on-line signature verification system, *Pattern Recognition Letters*, vol.29, no.5, pp.559-568, 2008.

[39] A. K. Bhunia, A. Alaei and P. P. Roy, Signature verification approach using fusion of hybrid texture features, *Neural Computing and Applications*, vol.31, no.12, pp.8737-8748, 2019.

[40] S. Lai, L. Jin and W. Yang, Online signature verification using recurrent neural network and length-normalized path signature descriptor, *2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR)*, vol.1, pp.400-405, 2017.

[41] X. Wu, A. Kimura, B. K. Iwana, S. Uchida and K. Kashino, Deep dynamic time warping: End-to-end local representation learning for online signature verification, *2019 International Conference on Document Analysis and Recognition (ICDAR)*, pp.1103-1110, 2019.

[42] S. Lai and L. Jin, Recurrent adaptation networks for online signature verification, *IEEE Transactions on Information Forensics and Security*, vol.14, no.6, pp.1624-1637, 2019.

[43] L. He, H. Tan and Z. Huang, Online handwritten signature verification based on association of curvature and torsion feature with Hausdorff distance, *Multimedia Tools and Applications*, pp.1-26, 2019.

[44] W. S. McCulloch and W. Pitts, A logical calculus of the ideas immanent in nervous activity, *The Bulletin of Mathematical Biophysics*, vol.5, no.4, pp.115-133, 1943.