Open Access | **Baghdad Science Journal** | **P-ISSN: 2078-8665**
Published Online First: March 2022 | **2022, 19(5): 1100-1110** | **E-ISSN: 2411-7986**

DOI: http://dx.doi.org/10.21123/bsj.2022.6117

Offline Signature Biometric Verification with Length Normalization using Convolution Neural Network

Zahraa Mazin Alkattan ***Ghada Mohammad Tahir Aldabagh***

Department of Software, College of Computer Sciences and Mathematics, University of Mosul, Mosul, Iraq
*Corresponding author: zahraa.alkattan@uomosul.edu.iq
E-mails address: ghadaaldabagh@uomosul.edu.iq

Received 3/4/2021, Accepted 15/9/2021, Published Online First 20/3/2022, Published 1/10/2022

Abstract:

Offline handwritten signature is a type of behavioral biometric-based on an image. Its problem is the accuracy of the verification because once an individual signs, he/she seldom signs the same signature. This is referred to as intra-user variability. This research aims to improve the recognition accuracy of the offline signature. The proposed method is presented by using both signature length normalization and histogram orientation gradient (HOG) for the reason of accuracy improving. In terms of verification, a deep-learning technique using a convolution neural network (CNN) is exploited for building the reference model for a future prediction. Experiments are conducted by utilizing 4,000 genuine as well as 2,000 skilled forged signature samples collected from 200 individuals. This database is publicly distributed under the name of SIGMA for Malaysian individuals. The experimental results are reported as both error forms, namely False Accept Rate (FAR) and False Reject Rate (FRR), which achieved up to 4.15% and 1.65% respectively. The overall successful accuracy is up to 97.1%. A comparison is also made that the proposed methodology outperforms the state-of-the-art works that are using the same SIGMA database.

Keywords: Biometrics, Deep-learning, Handwritten signature, Histogram Oriented Gradient (HOG), Image Processing, Length-normalization, Signature verification.

Introduction:

In general, the biometric system has been defined as an individual that is based on a characteristic vector extracted from the physiological or behavioral characteristics of the individual[1]. Normally, two modes of biometric operations are as follows: identification and verification[2]. First, Identification Mode is a comparison of the biometric target data with all of the other data available in the system, and can be represented in the following question: "Who are you?.". In other words, it performs a (*1:n*) match as it is a one-to-many comparison. This method of biometric authentication is widely used for forensic and surveillance purposes. Although the second mode of the biometric process is called the Verification Mode. This model is based on the following question: "Are you the one you claim to be?". Here, the target biometric data is compared to the original reference stored in the system to authenticate its identity. It can also be specified to fit one-to-one (1:1) data[3].

Handwritten Signature Verification Systems are used to automatically recognize whether the signature given by the author belongs to the individual in question. The genuine signatures are those produced by the claimed individual (original writer) and the forgeries are those made by the impostor (forger). Some of the problems related to offline hand-written signatures are a high number of users (classes)[4]. Also, the high-dimensional vector length, the limited number of training samples per writer with high intra-class variability.

The handwritten signature usually comprises the first with the last names of an individual, and it is often the case that the signature does not contain a full name, but rather a part of it. This type of signature is referred to as a *paraph*. The motivation is that the signature can be defined as a behavioral type of biometrics that acts as a non-intrusive as well as non-invasive authentication for the users[5]. Also, its implementation involves both company transactions and government agencies[6]. Besides, the biometric signature is deemed as one of the most accepted biometrics because most people have their signatures, which can be used as codes for them[7]. However, the main problem is the high intra-user variability properties, which decreases the total accuracy of the signature verification. That is because the individuals may not produce the same signature as one of the signed previously[7]. The method of signature authentication is either static or dynamic data format[8]. The static is also known as offline signature verification, which conducts signature verification using scanned images signed on a paper-based document as shown in Fig.1.

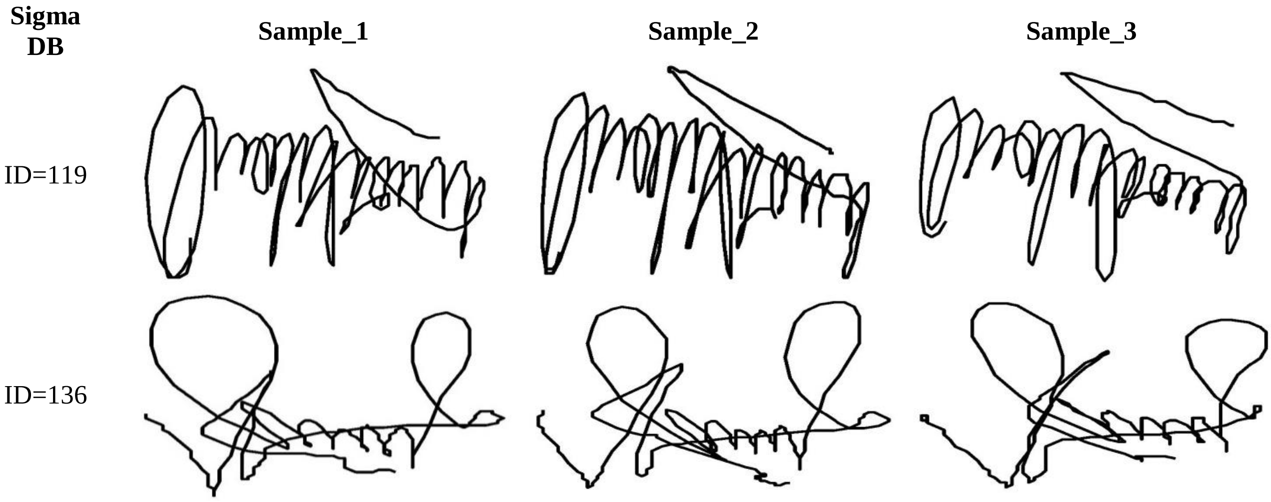


Figure 1. Three samples of two users' offline signatures taken from SIGMA Database: user ID=119 and ID=136.

While the dynamic one is referred to as an online signature verification process, signature samples are collected one point by one digitally, usually using computerized pens and visual tablets [8].

It should be noted that the high correct matching (accuracy) of the signature authentication is difficult to be attained due to the issue named "high intra-user variability", in which the False Reject Rate (FRR) increases. Therefore, the objective of this research is to propose a verification system that increases the accuracy, which outperforms the existing works, by exploiting the deep-learning based on the convolutional neural network (CNN). The contribution of this paper is to improve the accuracy achieved until now with the SIGMA database by using both histogram orientation gradient (HOG) passed to deep-learning as a hybrid technique. Finally, to validate the proposed work, a comparison is made between the proposed method and the state-of-the-art works using the database called SIGMA databases.

The paper is structured as follows: Section 2 is devoted to related work for the authentication of signatures; Section 3 explains the system architecture by using a signature length normalization with a (HOG) and a convolutional neural network. The experiment and implementation are then defined in Section 4. The consequence and discussion of the proposed method are explained in Section 5. Then, the conclusion is provided in Section 6.

Related Work

In this section, the latest work of handwritten signature verification is reviewed regarding the method description of the work, a database used in that work with its characteristics, and the resulted accuracy of the method with any other comment that is required to be mentioned.

For instance, in the work in reference [8], online signature verification is presented by using length normalization as Up-Sampling and Down-Sampling techniques. This is accomplished by the PCA (Principal Component Analysis) for feature extraction to build the feature vector that represents the signature sample. Then, passing this vector to ANN (Artificial Neural Network) for classification is performed by exploiting the Database of SIGMA (the same database will be used in this research paper). The result was obtained with a False Accept Rate (FAR) of up to 5.5 % and a False Reject Rate (FRR) of up to 8.75 %. Another online signature verification has been presented for online handwritten signature recognition by using the same database SIGMA as in reference [9]. This approach to online signature verification through the use of multilayer perceptron (MLP) on a subset of principal component analysis (PCA) features. The result is as follows: a false acceptance rate (FAR) of 7.4% and a false rejection rate (FRR) of 6.4%.

Baghdad Science Journal
2022, 19(5): 1100-1110
P-ISSN: 2078-8665
E-ISSN: 2411-7986

Another work is presented in reference [10] for an offline handwritten signature. In this method a feature vector of an offline handwritten signature by using Histogram Orientation Gradient (HOG) for the feature extraction and also used Support Vector Machine (SVM) for the classification. An experiment has been conducted to estimate the accuracy by using SIGMA database. The result achieved up to 96.8% as detailed: False Accept Rate (FAR) is 3% and False Reject Rate (FRR) is 3.35%.

Another work used scale-invariant feature transform (SIFT) and speeded-up robust features (SURF) features to build codebooks of the feature histograms as in reference [11]. This work used and support vector machines (SVMs) for the verification. Here, the Database used 1600 samples and a recognition rate is up to 95% by involving the ten-fold cross-validations.

Another idea of the signature verification in case there are few samples of trailing, samples generator is used based on the genuine signer to duplicates and generate the same image space as in reference [12]. The classifier is the SVM, as claimed the equal error rate (EER) has been decreased from 5.71% to 1.08%. The evaluation has been performed using many database signatures such as GPDS, MCYT-75, and CEDAR.

Also, convolutional neural network (CNN) methods as deep-learning-based on four models VGG16, VGG19, ResNet50, and DenseNet121 have been used for offline handwritten signature verification as in reference [13]. Here, the best model achieved an accuracy of up to 98.06% in DenseNet121 by using the MCYT database.

Methodology

Operations are divided into two main phases: training (enrollment) and testing (verification) as shown in Figure 2. In the first place, the training operation begins by gathering a database of signature samples as images from individuals. These signatures are certainly are signed with different lengths. For this reason, the signature length normalization is then exploited based on the algorithm provided in reference [8] that is

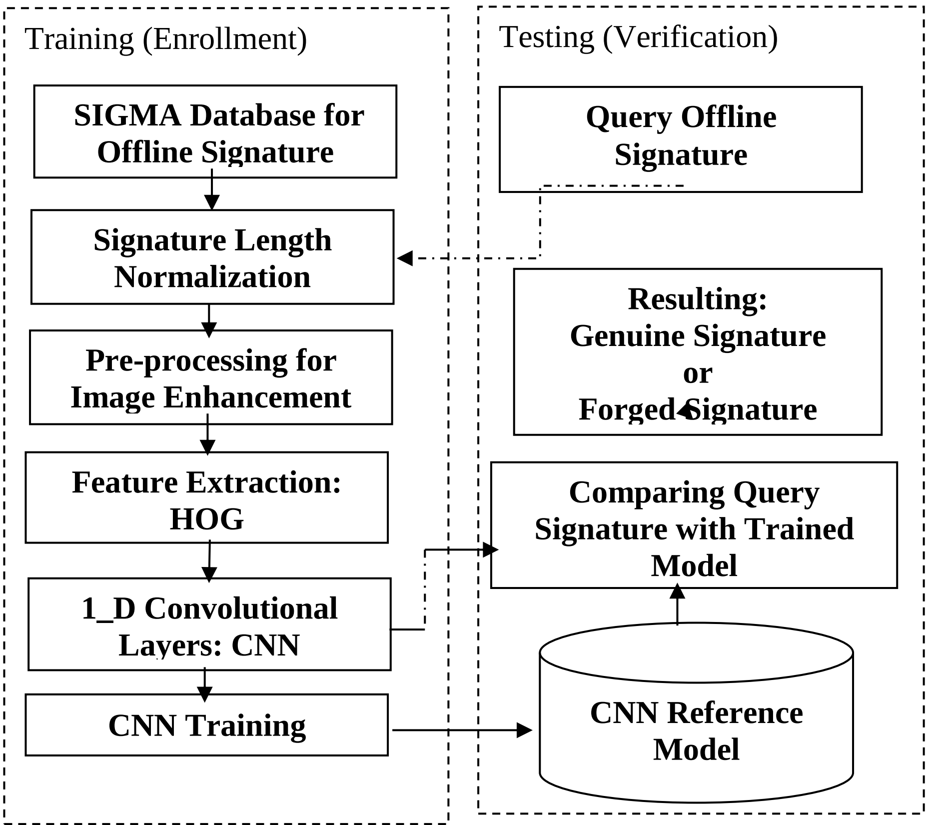


Figure 2. Framework design of the proposed offline Signature verification system.

Approved to increase the verification rate if signature lengths are normalized with the same length (the idea of the normalization will be discussed in subsection A). Several processing techniques are then used to improve the signature images in terms of contrast and noise reduction. In this process, contrast enhancement is used based on the intensity improvement, Furthermore, a non-linear filter (median filtering) [14] with kernel size [*3x3*] is also used to eliminate noise. After that,

Baghdad Science Journal
2022, 19(5): 1100-1110
P-ISSN: 2078-8665
E-ISSN: 2411-7986

feature extraction called histogram orientation gradient (HOG) is used to increase the recognition rate for signature verification.

Thus, the feature vector after the HOG phase is a one-dimensional vector (1-D) that will be fed to the convolutional neural network (CNN) for the classification procedure. CNN then generates a reference model that can be used for future verification (prediction). The second step, which is the authentication process, is carried out if there is a need to verify the signature whether it is genuine or forged. The operation is done by taking the signature from the entity and then converting it to an image. After that, the same steps that have been taken in the training operation will be implemented during the verification phase, except for the training as shown in Fig. 2. CNN is used to compare the registered and the queried signature attributes that need to be verified in the testing phase. Finally, a decision is made based on a threshold to determine if an offline signature must be approved or rejected.

A- Signature length normalization

To cope with the intra-user variability of handwritten signatures, which decreases the verification rate, the method of normalization is extended to the online handwritten signature as described in the reference [8]. After normalization in this study, the signature type format is converted from online (time series signature format $X[t]$) to offline (image signature format). Signature length normalization shall be accomplished concerning time, as a result, all signature samples in the SIGMA database shall consist of a defined period of signature length.

Accordingly, the normalization for the signature length is agreed to be 256 pixels (dotted) in this research. The reason for selecting this factor for all individuals of the database is because most of the signature samples in this database are close to the average length of the 261 pixels signal sampling.

The normalization method is accomplished by mapping the unknown length to the proper length (256) of the signature provided that the original signature sample will not be confused or distorted. The normalization method is focused on two main operations: Down-Sampling with Up-Sampling [15]. In terms of the Down-Sampling is explained as if a signature signal $X[t]$, and it is required to run a 2-pixels down-sampling data, then the output is selecting only one from every two pixels as $Y[t]=X[2t]$. In terms of the up-sampling operation, which is explained that the output $Y[t]$ is generated by interlacing between two old values a new value, which is derived by performing an interpolation process as in (1):

$$value_{new} = \frac{A[t]+A[t+1])}{2} \qquad (1)$$

Down-Sampling is applied to those signatures when the length of the signature exceeds the length of the desired signature. While Up-Sampling is applied to those signatures when the duration of the signature is less than the length of the desired signature.

B- HOG features for signature

Histogram Orientation Gradient (HOG) is used for the representation of the shape features introduced by Dalal and Triggs at the 2005 CVPR conference [16]. In this research, HOG was adopted as a feature extraction technique for authenticating signature images. HOG is implemented by selecting masks for edge detections to compute derivatives and gradients, then, splitting an image into cells and grouping cells into a block, block overlapping, and normalization parameters [16]. In the current work, HOG was implemented by setting the Cell-Size to [*110x110*] pixels. Then the size of the block is [*2x2*]. Block-Overlap between adjacent lines is selected 1 for better accuracy. Also, the number of bins selected in the orientation histograms is 9 bins as default. HOG depends on the gradient (∂) that can be computed by Eq.(2), while the orientation (θ) can be claculated using Eq.(3).

$$\partial = \sqrt{S_1^2 + S_2^2} \qquad (2)$$

$$\theta = Tan^{-1}(\frac{S_2}{S_1}) \qquad (3)$$

Accordingly, the overall feature vector length for is 432 the aforementioned configuration, which is used to represent each signature image sample. Figure 3 depicts two offline handwritten signatures from SIGMA database (having ID=119, ID=136) with a three kinds of cell size as [*100x100*], [*110x110*] and [*120x120*]. It is worth mentioning that the output of the HOG is a 1-dimensional vector that contains the histogram of the ordination gradient for the image.

Baghdad Science Journal
2022, 19(5): 1100-1110
P-ISSN: 2078-8665
E-ISSN: 2411-7986

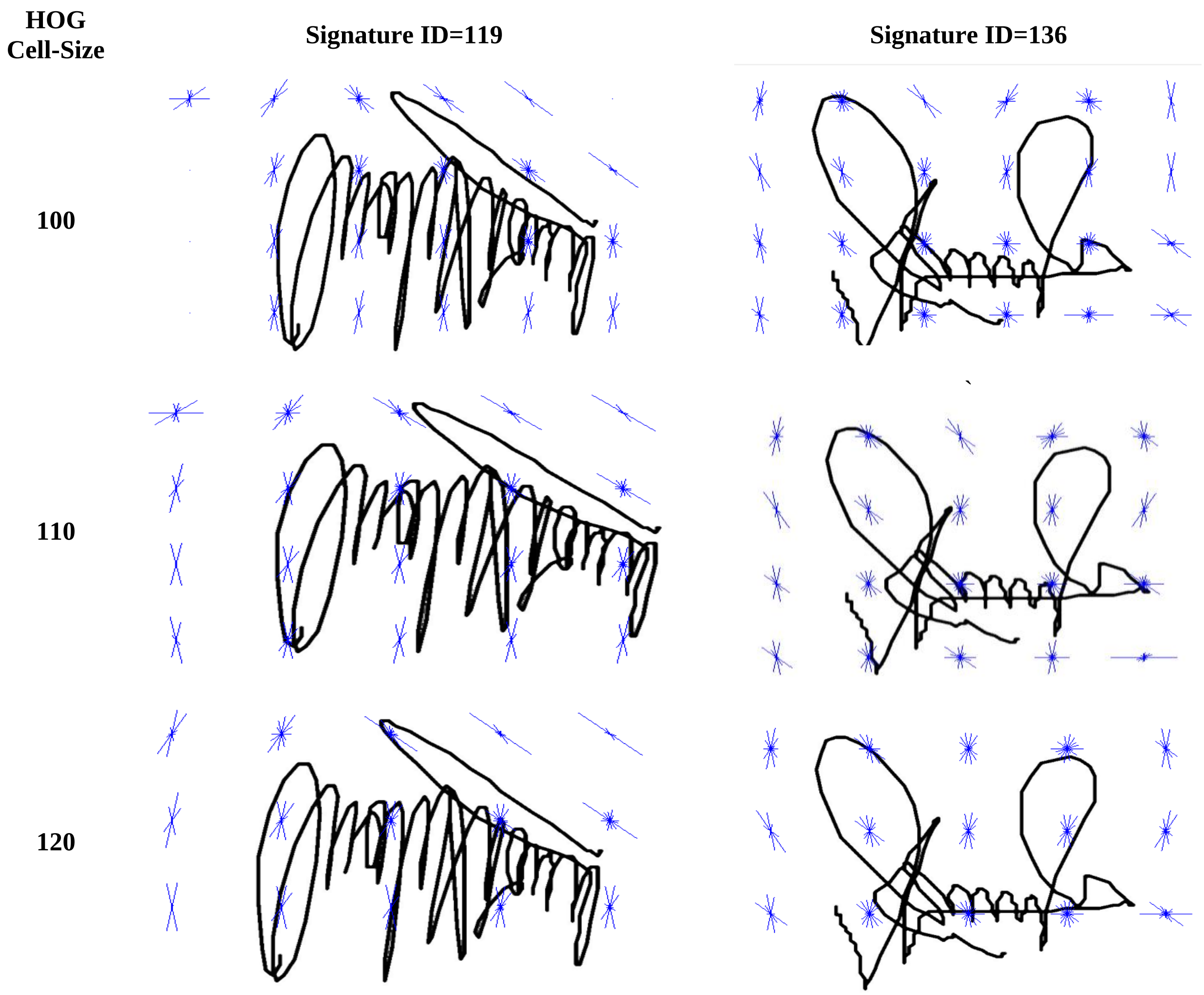


Figure 3. Offline handwritten signature visualization based on the HOG features effects.

C- Signature verification by CNN

One of the most popular deep-learning algorithms is called convolutional neural network (CNN) explained in[17-19] that is used for classification and prediction. CNN contains different processing layers. the basic three layers are convolution, rectified linear unit (ReLU), and pooling layers. the procedure starts by inserting the input images and apply convolution operations with convolutional filters. several filters will be included that are used to highlight the edges of the input image. As far as the Rectified Linear Unit (ReLU) is concerned, it facilitates quicker and more efficient training by mapping negative values to zero and retaining positive values. This is often referred to as activation since only the active features are forwarded to the next layer[17]. Next, the Pooling operation, which is performing nonlinear down-sampling by selecting the value of a block size [*2x2*] throughout the image. These operations are repeated over tens or hundreds of layers, with each layer learning to identify different features.

After the extensive running of the experiment to choose a suitable number of layers, the proposed CNN design in this research paper has several layers as illustrated in Fig. 4. This design consists of three primary layers called rounds. Each round layer contains four processing operations, which are the convolution layer, normalization, activation function (Relu), and finally the max-pooling layer. The configuration of all rounds is the same except for the convolution operation, where the number of filters is different in each round. The number of the filter masks are as follows: 21, 42, and 84 for the Conv1, Conv2, and Conv3 respectively. The convolutions stride is [1x1] and the padding type is the same. it is worth mentioning that the input to the CNN is a 1-D feature vector having a length of either 288, 432, or 540.

1) Conv_1 21 filters[1x13x1] stride [1 3]	**5)** Conv_2 42 filters [1x13x21] stride [1 3]	**9)** Conv_3 84 filters [1x13x42] stride [1 3]			**Class 1:** COVID
2) Batch normalization_1 21 channels	**6)** Batch normalization_2 42 channels	**10)**Batch normalization_3 84 channels			
3) ReLU_1 **4)** Max_Pooling_1 from block 1x2 stride [1 2] padding [0 0 0 0]	**7)** ReLU_2 **8)** Max_Pooling_2 from block 1x2 stride [1 2] padding [0 0 0 0]	**11)** ReLU_3 **12)** Max_Pooling_3 from block 1x2, stride [1 2] padding [0 0 0 0]			**Class 2:** non-COVID
Round 1	Round 2	Round 3	Flatten	2-Fully Connected	Softmax
Feature Extraction			Verification		

Figure 4. Depicts the configuration of the proposed CNN layers.

Experiment Setup

Several experiments have been conducted on offline signatures to test the accuracy of the verification of the proposed process. The experiments are carried out using the signature samples in the SIGMA database related to Malaysian people [20]. Now, each individual will have a unique training matrix used to train a model specific for that individual. The training matrix is designed to have 20 samples, divided as following each individual has 10 genuine samples as well as 10 forged samples, which are combined in one matrix to form a training matrix. In which the 10 forged samples are further divided into two-part as five for skilled forged samples and the other five for randomly forged samples (taken from a different individual). Finally, the training matrix includes 20 signature samples. Each signature sample is represented by 432 features. these 432 features came from the HOG feature extraction.

The training is run by CNN for each individual's signatures. In other words, there will be 200 times training and testing operations in each experiment. Then, the evaluation of the signature verification system is stated by extracting the following two errors: FAR (False Accept Rate) and FRR (False Reject Rate) [21] for each person separately. Regarding the test matrix, which is designed similarly to the training matrix, must be built with the same number of features and classes. Once the training type of the proposed system is supervised learning, target scores for each class must be presented [22]. Accordingly, the *+1* target has been assigned to the genuine signatures, while the *-1* target has been assigned to the forged signature samples. Here, the target matrix has a size of *[20x1]*, because the first 10 targets are for those genuine signature samples, and the remaining targets are for those the 10 forged signature samples as illustrated in Table 1:

Table 1. Shows the training and testing matrix distribution for the SIGMA database for one user out of 200 users.

Matrix Type	Genuine Samples No.	Forged Samples No.	Total Number
Training Matrix	10	10	20
Testing Matrix	10	10	20
Total Sample / User	20	20	40
Target (Label)	+1	-1	

Now to calculate the FRR error, a result of the prediction of the CNN output will be evaluated. The size of the predicted matrix is the same as the sample numbers in the testing matrix, which is *[20x432]* (20 signature samples each one with a length of 432 features). To calculate the FRR, the first 10 output scores have to be as +1 target. If any of these 10 outputs are not +1, that means a counter named FR (False Rejection) will be added by one (increment) such as $(FR = FR + 1)$. Then, the rate of this error is calculated as in (4):

$$FRR = \frac{FR}{10} \times 100\% \qquad (4)$$

Conversely, the predicted output vector indexed from 11~20 must be *-1* target. If any one of these 10 predicted output is not -1, then a counter named (FA) will be increased by one such as $(FA = FA + 1)$. This means that the error FAR is appeared and computed as in (5):

$$FAR = \frac{FA}{10} \times 100\% \qquad (5)$$

After extracting the FAR and FRR errors, the total accuracy related to that users is calculated as (6) :

$$User_{Accuracy}\% = 100 - \frac{FAR+FAR}{2} \qquad (6)$$

Ultimately, to calculate the overall verification accuracy of the SIGMA database, the average operation is applied to the 200 individuals' accuracy as in (7):

$$AVR_{Accuracy} = \frac{1}{200}\sum_{i=1}^{200} User_{Accuracy}[i] \qquad (7)$$

To reproduce the work and experiments the following parameters are configured as follows: for the CNN training, optimization type is either the *adam* (adaptive moment estimation) [23], or the *sgdm* (Stochastic Gradient Descent with Momentum) [24] in the experiment. However, adam is better than sgdm in terms of the recognition rate. Also, Learn Rate Schedule is configured as piecewise, Max Epochs (1 iteration / Epochs) is configured as 80, Learn Rate Drop Factor is selected to be 0.9, and Learn Rate Drop Period is 5. These hyper-parameters have been selected by using the try and error method to adjust the reference trained model.

Results and Discussions:

The experimental results of this research are reported in two forms. Firstly, tables illustrate the verification rates, and the second form is the graphical representation to show the successful accuracies for each user in the SIGMA database containing 200 users.

Accordingly, Table 2, illustrates the results achieved by the proposed verification methodologies by using ADAM training CNN type. In Table 2, the most important thing is the accuracy obtained from the two types of error FAR and FRR. Six experiments have been conducted with a different setting in terms of the HOG feature extraction by altering the Cell-size three times, as follows, *[100x100]*, *[110x110]*, and *[120x120]* that resulted in feature vector as *540*, *432*, and *288* respectively. Also, the signature image size for all of them is unified having size [*460x613*] gray-scale image type.

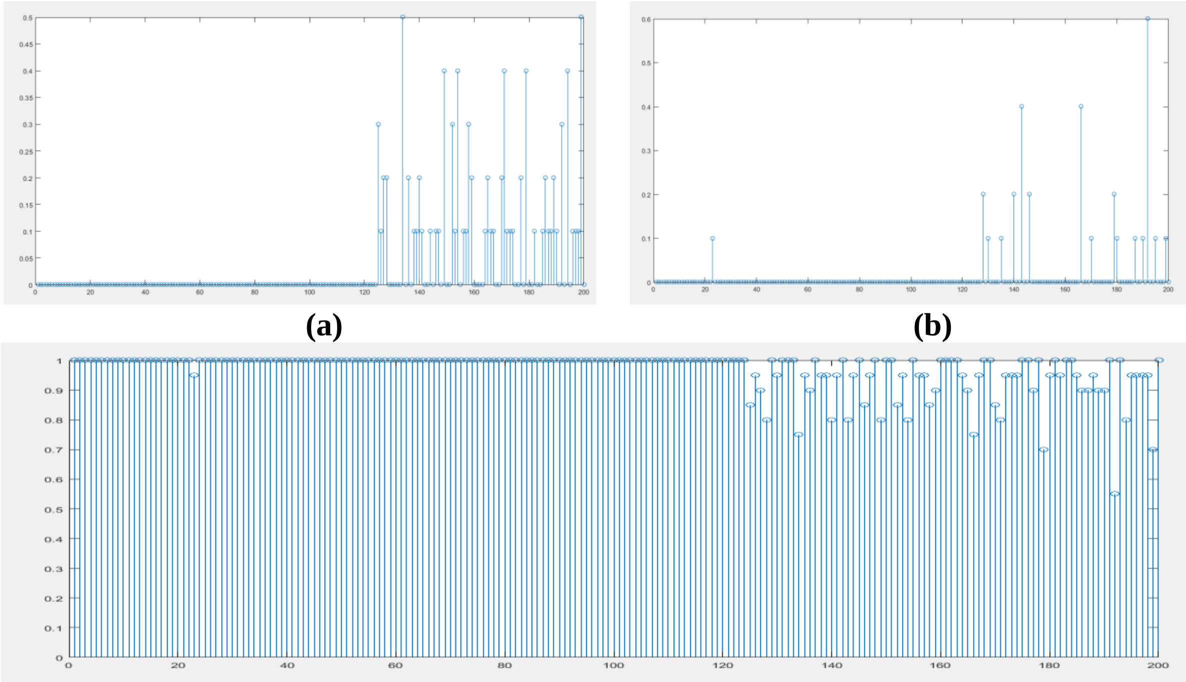
Table 2. Accuracy results based on adam optimizer for Training.

Exp. No.	Signature Image Size	HOG Cell Size	HOG Feature Vector Length	FAR%	FRR%	Accuracy%
1	460x613	100x100	540	4.55	2.10	96.67
2				4.10	2.05	96.92
3	460x613	110x110	432	4.30	1.55	97.07
4				4.15	1.650	**97.10**
5	460x613	120x120	288	4.40	2.05	96.77
6				3.95	1.90	9707

For each feature vector length, the experiment was repeated 2 times to achieve the reliability and validity of the experiment execution. As it is obvious that the best-achieved accuracy is 97.1% because FAR is up to 4.15% and FRR is up to 1.65%. when the vector length is 432 coming from the cell-size [*110x110*] pixels. other experimental results as in Table 2 are near to the best-achieved accuracies.

Next, to show the accuracies for all 200 users in the SIGMA database, Fig. 5 depicts the accuracies, FAR, and FRR for each user. As shown in Fig. 5(a), FAR rate error for 200 users, as it is clear that the errors start increasing from the user after 120. Also, Fig. 5 (b) is the FRR error type for all 200 users, for instance, that sample 140 has FRR is 0.4 (40%).

In terms of Fig. 5(c), all 200 users' accuracies have been depicted. For example, most of the users have accuracies up to 1, which means 100%. the average of them is calculated based on Eq. (7), which is reported in Table 2 for FAR, FRR, and accuracy 4.3%, 1.55%, and 97.07% respectively.



(a) (b) (c)

Figure 5. Verification results based on adam training solver: (a) error 1 type: FAR, (b) error2 type: FAR, (c):accuracies for SIGMA database 200 user for the case 97.07%.

Similarly, Table 3, illustrates the results achieved by the proposed verification methodologies, in which the optimizer is based on sgdm training CNN type. In Table 3, the most important thing is the accuracy obtained from the two types of error FAR and FRR. Also. six experiments have been conducted with a different setting in terms of the HOG feature extraction by altering the Cell-size three times such as *[100x100]*, *[110x110]*, and *[120x120]* that resulted in feature vector as *540*, *432*, and *288* respectively. Also, the signature image size for all of them is unified having size [*460x613*] gray-scale image type. For each feature vector length, two times of experiments have been conducted to achieve the reliability and validity of the experiment execution. As it is clear, the best accuracy that has been achieved is 97.05% when FAR is up to 3.6% and FRR is up to 2.3%, for the vector length is 288 coming from the cell-size [*120x120*] pixels. Other experimental results as in Table 3 are near to the best-achieved accuracy.

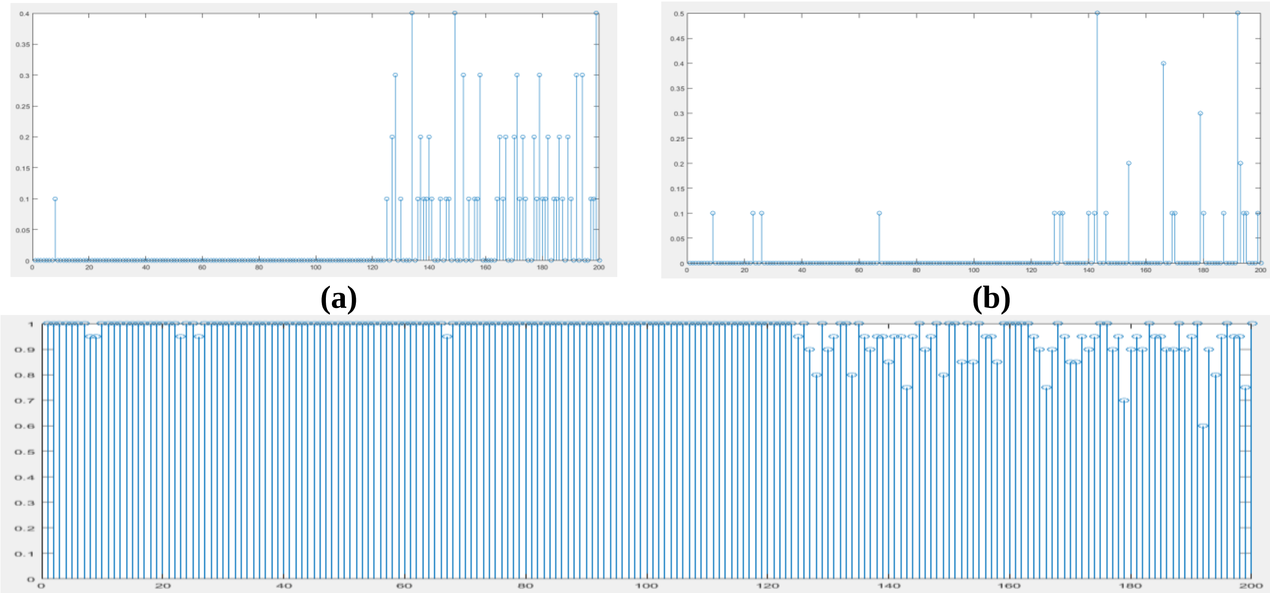
Table 3. Accuracy results based on sgdm optimizer for Training.

Exp. No.	Signature Image Size	HOG Cell Size	HOG Feature Vector Length	FAR%	FRR%	Accuracy%
1	460x613	100x100	540 [21 42 84]	3.90	2.50	96.80
2				4.10	2.45	96.72
3	460x613	110x110	432 [21 42 84]	4.05	1.90	97.02
4				4.10	2.25	96.82
5	460x613	120x120	288 [21 42 84]	3.60	2.30	**97.05**
6				4.40	2.40	96.60

The accuracies based on sgdm training for all 200 users in the SIGMA database, Fig. 5 depicts these accuracies as well as FAR and FRR for each user. Fig. 6(a), FAR rate error for 200 users. Also, Fig. 6 (b) is the FRR error type for all 200 users, for instance, that sample 199 has FRR is 0. 1 (10%). In terms of Fig.6(c), all 200 users' accuracies have been depicted as it is shown that most of the users have accuracies up to 1. Thus, the average of them is calculated based on Eq. (7), which is reported in Table 3 for FAR, FRR, and accuracy are 3.6%, 2.3%, and 97.05% respectively.

Baghdad Science Journal
2022, 19(5): 1100-1110

P-ISSN: 2078-8665
E-ISSN: 2411-7986



(a) (b)

(c)

Figure 6.Verification results based on sgdm training solver: (a) error 1 type: FAR, (b) error2 type: FAR, (c): accuracies for SIGMA database 200 users for the case 97.05%.

It is worth mentioning that each training and testing time for one user by using the proposed method is taking around 3-5 seconds. As a result, the training time for all users of the SIGMA database (200 users) database consumes approximately 1000 seconds (16.7 minutes). The experiments have been conducted on workstation hardware as characterized on a single CPU having hardware specification up to 6G-RAM, Core-i3, 2.4GHz.

In terms of the benchmarking and comparison for the proposed work with the state-of-the-art works, Table 4 lists the accuracies of the handwritten signature verification existing in the literature used in the same SIGMA database. As it is clear that the proposed methodology of using the following steps: contrast enhancement preprocessing, signature length normalization, HOG, and CNN has outperformed the existing works used the same SIGMA signature database, in which this database is publically published online[20].

Table 4. Comparing the proposed accuracies with state-of-the-art accuracies dedicated for SIGMA handwritten signature database.

No.	Method	Ref.	Accuracy %
1	Normalized, PCA and ANN	8	92.87
3	PCA and ANN	9	93.1
4	HOG and SVM	10	96.8
5	**Proposed method**	-	**97.10**

It is worth mentioning that the limitation of this work needs a high CPU ability to be able to run the convolution operations and other CNN layers. For instance, if the proposed algorithm needs to be uploaded to an embedded system that system needs to be included with a suitable processing speed to avoid any delay happened in the real-time execution.

Conclusion:

Offline handwritten signature verification has a high rate of intra-user variability, which decreases the general recognition rate. In this paper, the verification rate has been improved by using the proposed methodology as compared with the state-of-the-art works. This method is specified by the following steps: contrast enhancement and image noise filtering, signature length normalization, feature extraction by exploiting HOG, and finally the classifier using one-dimensional convolution CNN. The database used for the evaluation is named SIGMA handwritten signature database, which contains 6000 signature samples with the skilled forgeries samples and published online. The best successful accuracy achieved is up to 97.1% when the FAR and FRR are 4.15% and 1.65% respectively in which this accuracy outperforms all the existing works that are using this SIGMA database. These accuracies have been obtained when the training optimizer is ADAM, which is better than the SGDM optimizer, Also, the length of the feature vector is 432 features extracted by using the HOG method. In future work, trying to decrease the error rate as possible as could from 2.9% to zero by using different possible deep-learning algorithms.

Acknowledgements:
The authors would like to thank the University of Mosul / College of Computer Science and Mathematics for their facilities, which have helped to enhance the quality of this work.

Authors' declaration:
- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in University of Mosul.

Authors' contributions statement:
Z. M. A. has around 65% contribution of the article paper as follows: Idea Conception, framework design, acquisition of database, and proofreading, while the second author G. M. T. A. has around 35% contribution of the total work, as follows: analysis of the research, drafting the MS, revision, and proofreading.

References:
1. Singh M, Singh R, Ross A. A comprehensive overview of biometric fusion. Inf. Fusion. 2019;52:187-205.
2. Elhoseny M, Elkhateb A, Sahlol A, Hassanien AE. Multimodal biometric personal identification and verification. Adv. in Soft Comput. Machine Learning in Image Processing: Springer; 2018. p. 249-76.
3. Jain AK, Kumar A. Biometrics of next generation: An overview. Second generation biometrics. 2010;12(1):2-3.
4. Vaijayanthimala J, Padma T. Multi-modal biometric authentication system based on face and signature using legion feature estimation technique. Multimed Tools Appl. . 2020;79(5):4149-68.
5. Bibi K, Naz S, Rehman A. Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. Multimed Tools Appl. . 2020;79(1):289-340.
6. Faris Khlebus S. OFFLINE SIGNATURE VERIFICATION BASED ON USING NEURAL NETWORK CLASSIFICATION. J. kerbala Univ. . 2017;13(4):234-46.
7. Faundez-Zanuy M, Fierrez J, Ferrer MA, Diaz M, Tolosana R, Plamondon R. Handwriting biometrics: Applications and future trends in e-security and e-health. Cognit. Comput. . 2020;12(5):940-53.
8. Malallah FL, Ahmad SMS, Adnan WAW, Arigbabu OA, Iranmanesh V, Yussof S. Online handwritten signature recognition by length normalization using up-sampling and down-sampling. International Journal of Cyber-Security and Digital Forensics (IJCSDF). 2015;4(1):302-13.
9. Iranmanesh V, Ahmad SMS, Adnan WAW, Yussof S, Arigbabu OA, Malallah FL. Online handwritten signature verification using neural network classifier based on principal component analysis. Sci. World J. . 2014;2014.
10. Abbas NH, Yasen KN, Faraj K, Razak LFA, Malallah FL. Offline handwritten signature recognition using histogram orientation gradient and support vector machine. J. Theor. Appl. Inf. Technol. . 2018;96(8):2075-84.
11. Sriwathsan W, Ramanan M, Weerasinghe A. Offline handwritten signature recognition based on SIFT and SURF features using SVMs. Asian Res. J. of Mathematics. 2020:84-91.
12. Maruyama TM, Oliveira LS, Britto AS, Sabourin R. Intrapersonal parameter optimization for offline handwritten signature augmentation. IEEE Transactions on Information Forensics and Security. 2020;16:1335-50.
13. Yapıcı MM, Tekerek A, Topaloğlu N. Deep learning-based data augmentation method and signature verification system for offline handwritten signature. Pattern Anal. Appl. . 2020:1-15.
14. Yin L, Yang R, Gabbouj M, Neuvo Y. Weighted median filters: a tutorial. IEEE Trans. circuits syst II.: analog and digital signal processing. 1996;43(3):157-92.
15. Frajka T, Zeger K. Downsampling dependent upsampling of images. Signal Processing: Image Commun. . 2004;19(3):257-65.
16. Dalal N, Triggs B, editors. Histograms of oriented gradients for human detection. 2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05); 2005: Ieee.
17. O'Shea K, Nash R. An introduction to convolutional neural networks. arXiv preprint arXiv:151108458. 2015 Nov 26.
18. Hassan NF, Abdulrazzaq HI. Pose invariant palm vein identification system using convolutional neural network. Baghdad Sci. J.. 2018;15(4).
19. Asroni A, Ku-Mahamud KR, Damarjati C, Slamat HB. Arabic Speech Classification Method Based on Padding and Deep Learning Neural Network. Baghdad Sci. J.. 2021;18(2 (Suppl.)):0925-.
20. Ahmad SMS, Shakil A, Ahmad AR, Agil M, Balbed M, Anwar RM, editors. SIGMA-A Malaysian signatures' database. 2008 IEEE/ACS International Conference on Computer Systems and Applications; 2008: IEEE.
21. Jain AK, Griess FD, Connell SD. On-line signature verification. Pattern recognition. 2002;35(12):2963-72.
22. Fabris F, De Magalhães JP, Freitas AA. A review of supervised machine learning applied to ageing research. Biogerontology. 2017;18(2):171-88.
23. Kingma DP, Ba J. Adam: A method for stochastic optimization. arXiv preprint arXiv:14126980. 2014.
24. Murphy KP. Machine learning: a probabilistic perspective: MIT press; 2012.

التحقق من تواقيع الافراد الصورية باستخدام عمليات مساوات الاطوال والشبكات العصبية الالتفافية

زهراء مازن القطان **غادة محمد طاهر الدباغ**

قسم البرمجيات، كلية علوم الحاسوب والرياضيات، جامعة الموصل، موصل، العراق

الخلاصة:

تواقيع اليدوية الصورية هي نوع من انواع البايومتري التصرفي الذي يعتمد على الصور. المشكلة هي في دقة تمييز التواقيع وتأكيديها وسبب انه عندما نادرا ما يوقع الشخص نفس التوقيع مرة ثانية بالضبط. وهذه المشكلة تسمى التقلب داخل المستخدم.هذا البحث يهدف لتحسين دقة التمييز التواقيع الورقية. في هذه الورقة العلمية، الطريقة المقترحة تتم بواسطة عملية مساواة اطوال التواقيع و الرسم البياني للمشتقات الموجه لكي يتم تحسين دقة التمييز. بالنسبة لعمليات التاكيد، تقنية التعلم العميق باستخدام شبكات العصبية الألتفافية تم استغلالها لعمليات التعليم والفحص. حيث تم اجراء تجارب باستخدام 4000 توقيع حقيقي و 2000 توقيع مزور بصورة احترافية حيث تم تجميع هذه التواقيع من 200 شخص ماليزي ووضعها في قاعدة بيانات اسمها "سكما" والتي هي متوفرة على المنصات الالكترونية للاستخدام العام. تم استخراج نتائج التجارب من خلال الخطئين وهما نسبة القبول الخاطئ وكان 4.15% والخطئ المسمى نسبة الرفض الخاطئ ونسبته مختبريا 1.65%. والنسبة الدقة النهائية لقاعدة البيانات سكما هي 97.1%. وايضا في هذه الورقة العلمية تم مقارنة الطريقة المقترحة مع الطرق المتوفرة موخرا و التي تم اعتماد نفس قاعدة البيانات سكما لغرض المقارنة وتبين أن نسبة تميز التواقيع بالطريقة المقترحة تتفوق على الذي متوفر حاليا باستخدام نفس قاعدة البيانات سكما.

الكلمات المفتاحية: البايومتري، التعليم العميق، التواقيع اليدوية، الرسم البياني للمشتقات الموجهة، معالجة صور، مساواة الاطوال، التأكد من التواقيع.