Research Article

SIGNATURE VERIFICATION USING SIAMESE NETWORK BASED ON ONE-SHOT LEARNING

Authors: Merve VAROL ARISOY

To cite to this article: Varol Arısoy, M. (2021). SIGNATURE VERIFICATION USING SIAMESE NEURAL NETWORK ONE-SHOT LEARNING. International Journal of Engineering and Innovative Research ,3(3), p: 248-260. DOI: 10.47933/ijeir.972796

DOI: 10.47933/ijeir.972796

To link to this artice: https://dergipark.org.tr/tr/pub/ijeir/archive

International Journal of Engineering and Innovative Research

http://dergipark.gov.tr/ijeir

SIGNATURE VERIFICATION USING SIAMESE NETWORK BASED ON ONE-SHOT LEARNING

Merve VAROL ARISOY[1*]

1Mehmet Akif Ersoy University, Department of Informatics, Burdur, Turkey.

[*]Corresponding Author: mvarisoy@mehmetakif.edu.tr

https://doi.org/10.47933/ijeir.972796

(**Received:** 30.05.2021; **Accepted:** 04.07.2021)

ABSTRACT: With the acceleration of digitalization in all areas of our lives, the need for biometric verification methods is increasing. The fact that biometric data is unique and biometric verification is stronger against phishing attacks compared to password-based authentication methods, has increased its preference rate. Signature verification, which is one of the biometric verification types, plays an important role in many areas such as banking systems, administrative and judicial applications. There are 2 types of signature verification, online and offline, for identifying the identity of the person and detecting signature forgery. Online signature verification is carried out during signing and temporal dynamic data are available regarding the person's signature. Offline verification is applied by scanning the image after signing, and this verification is limited to spatial data. Therefore, the offline signature verification process is considered a more challenging task.

In this study, offline signature verification, independent of the writer, based on One-Shot Learning, was performed using Siamese Neural Network. Due to the fact that the Deep Convolution Neural Network requires a large amount of labeled data for image classification, real and fake signature distinction has been achieved by using the One-Shot Learning method, which can perform a successful classification by using less numbers of signature images. As a result of the experiments conducted on signature datasets, using the Siamese architecture, the proposed approach achieved percentage accuracy of 93.23, 90.11, 89.99, 92.35 verification in 4NSigComp2012, SigComp2011, 4NSigComp2010 and BHsig260 respectively.

Keywords: Offline Signature Verification, Siamese Neural Network, One-Shot Learning, Machine Learning, Deep Learning.

1. INTRODUCTION

Depending on the rapid development of technology, many transactions have become realizable through the use of the internet. These transactions include personal transactions such as banking and e-state transactions. During the execution of such transactions, it is absolutely necessary to make sure that the transactions are carried out with the right person. And this verification can be carried out by using biometric and behavioral verification techniques.

Biometric and behavioral features are used especially in cases where authentication and security are required to be in a high level. Biological features such as face, fingerprint, palm, iris, retina and behavioral features such as signature and voice can be given as examples for them. Especially with the development of GPUs and accordingly the developments in artificial intelligence algorithms, the use of biometric and behavioral features for authentication purposes in every field has become widespread. In the upcoming period, the application and usage areas of these verification techniques will expand further with the developments in quantum programming and, accordingly, in quantum machine learning topics.

At this point, signature, which is a type of behavioral biometric verification, is used at many points in daily life for authentication and confirming that the related person does the relevant job. For this reason, being able to distinguish between real and fake signature is highly important in terms of both verifying the identity of the related person and confirming that the related person does the relevant work. Signature verification is divided into online and offline signature verification. In offline signature verification, verification is performed by comparing an existing signature with reference signatures previously obtained from the relevant person. At this point, the document, on which the person has put the signature at that moment, is first scanned and converted into image format, then the signature is defined and verified from within this document. Two approaches are used for offline signing. These are writer-dependent and writer-independent approaches. In the writer-dependent approach, a separate model is created for each author, whereas in the writer-independent approach, it is used by creating a single model for all authors. In online signature verification, the signature is put on a tablet or monitor; therefore, features such as pen pressure and pen slope angle can also be analyzed. Therefore, in online signature verification, first of all, individuals' signatures are recorded in the system at the registration stage, with data preprocessing and feature extraction methods. Afterwards, when the user puts the signature again, the same attributes are extracted and compared with the reference signature features. If the difference is below a specified threshold value, it is accepted, otherwise it is rejected [7].

With the development of technology and the increase in security needs, the authentication methods have also differentiated. One of the authentication methods to be used is offline and online signature verification methods. Identifying these signatures, with high accuracy, in all transactions that people will make by using their signatures will be of great importance in terms of the correct progress of the process in all areas of life. Therefore, One-Shot Learning based Siamese Neural Network is proposed in this study for offline signature verification, and the performance of this method has been tested on four different datasets and the results have been shared.

In the following sections of the article, literature review, smart city applications, machine learning, Siamese network and One-Shot Learning-based signature verification mechanism and conclusion section, respectively, are included.

2. RELATED WORKS

Signature verification, which is one of the types of biometric verification, plays an important role in many areas such as banking systems, administrative and judicial applications, where users are required to have their authentication made. Signatures of individuals are unique to them, as in the example of fingerprints, and only by means of the signature, it can be determined who owns an official document or by whom it has been approved. However, although the way of signing is unique to the individual, a person's signature can be imitated as a result of a sufficient number of attempts. Machine learning and deep learning methods were used so as to prevent this threat and also to distinguish between real and fake signatures.

Signature verification can be carried out online and offline. There are studies related to the both methods in the literature. In study [1], they examined the spatial-temporal adaptation of the Siamese neural network. According to this, they extracted spatial features using 1-dimensional CNN (Convolutional Neural Network) and also included the input in the temporal field by using LSTM (Long Short-Term Memory) networks. Similarly, in [2], they also used this method in the process of signature verification because the Siamese network provides effective classification results with a small number of learning inputs.

In the work of [3], a time-based recurring neural network approach for the solution of the online signature verification problem is proposed. They combined Dynamic Time Warping with the RNN network to create powerful models that can better distinguish fake signatures. On the other hand in study [4], they created an architecture, independent from convolutional neural network-based language, for the signature verification process. Their architecture, named sCNN (Shallow Convolutional Neural Network), has three convolutional layers and one fully connected layer. The model, which they trained, is quite simple in terms of the number of base layers, unlike other advanced methods; therefore, they optimized fewer number of weight parameters. The model includes few numbers of layers and parameters that reduced the time to be spent on training and testing. They stated that the sCNN model gave better results in terms of accuracy and error rate compared to other methods.

In the work of [5], they developed an application on offline signature verification by establishing the Siamese Network, in which the Convolutional Neural Network used as a subnet. In the Siamese network, they aimed to make the real-fake signature distinction more accurately by adding some statistical features to the embedding vector, which is the mathematical expression of each signature image. In the study of [6], it is shown that the RNN network could be used for the solution the online signature verification problem. They used the model, which they established, in online signature verification by combining RNN LSTM and Siamse Network. By extracting the similarity metric between the two signature samples, they enabled the model to learn this. They were also able to classify a signature image which was previously unlearned by their system. Similarly, in [7] and in [8], the Siamese network is also applied in the field of offline signature verification.

In study [9], offline signature verification and signature identification by comparing 2 different models of RNN and CNN, is examined. The RNN models, were based on LSTM and BLSTM. These two models outperformed the model, which they created with CNN. In the work of [10], they proposed combining EEG signals and offline signature samples by using a multimoded Siamese Neural Network (mSNN) for enhanced user verification. mSNN networks learn distinctive temporal and spatial features from EEG signals by using an EEG encoder and from offline signatures by using a video encoder. These two encoders were combined in a common feature field for further procedures. They used a distance measure based on similarity and difference of input features to generate validation results in the Siamese network.

In [11], it is determined that the desired success rate could not be achieved on account of the insufficient dataset required for training in the signature verification process. Therefore, they proposed a new use of Cycle-GAN, which is a data augmentation method, in their study. They tested the data augmentation methods on CNN-based VGG16, VGG19, ResNet50 and DenseNet121 models, which are widely used in the literature. As a result of experiments, they observed that data augmentation methods increased the success of all CNN models in the offline signature database. In the work of [12], it is focused on offline signature verification by using the artificial neural network approach. They used geometric features for offline verification of signatures. Among these features, there are such functions as Baseline Slope Angle (BSA), Aspect Ratio (AR) and Normalized Area (NA) and Center of Gravity Extraction.

In the study of [13], it is aimed to learn difference metrics from signature image pairs by combining writer-independent online signature verification systems, RNN network with Siamse architecture. Furthermore, they tried Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) systems with Siamse architecture in order to measure the effectiveness of different network structures. As a result of their studies, they determined that the Siamese network outperformed state-of-the-art online signature verification systems using the same database.

In [14] they developed a deep learning-based online signature verification system. They used Legendre polynomial coefficients as a feature in order to model the signatures. They classified the signature images with a deep feedforward neural network and used the stochastic gradient descent algorithm with momentum as a deep learning algorithm. As a result of their studies during which they used the SigComp2011 dataset, they observed a decrease in the error rate and an increase in the accuracy rate.

In the study [15], they proposed a new single-template strategy that uses averaging templates and local stability weighted dynamic time warping (LS-DTW) to simultaneously improve the speed and accuracy of online signature verification in order to meet the latest demands for automated security systems. In this method, which is called Euclidean centroid-based DTW centroid average, it was adopted to obtain an effective average template set for each feature while maintaining intra-user variability among reference samples. Afterwards, the local stability of the average template set was estimated by using the matching points between the average template set and references. Later, they increased the discrimination ability at the verification stage by using the LS-DTW distance measure between the average template set and a query signature. According to the results they obtained, they reported that their method was effective in both random and fraud scenarios.

In the study [16], they proposed a system that uses a score-level combination of complementary classifiers using different local features (histogram of oriented gradients, local binary patterns, and scale-invariant feature transformation descriptors) for offline signature verification. They adopted two different approaches for the classification task; these were universal and user-dependent classifiers. While user-dependent classifiers are trained individually for each user to learn to distinguish a user's real signature from other signatures, the universal classifiers are trained with the difference vectors of the query and reference signatures of all users in the training set to learn the differences. With the fusion of all classifiers, they achieved an equal error rate of 6.97% in qualified forgery tests. In [17], it is pointed out that there were not enough studies on providing model training using small-scale sampling in offline signature recognition. Therefore, in their studies, they presented a new convolutional neural network (CNN) structure called Large-Scale Signature Network (LS2Net) with collective normalization to overcome the large-scale training problem. They also proposed the Class Center Based Classifier (C3) algorithm based on KNN. They stated that they got better results when special designs were made for datasets in their networks, where they used the Leaky ReLU structure.

In [18], a new grid-based template matching scheme for offline signature analysis and verification is proposed. Their method is based on efficient encoding of the geometric structure of signatures with grid templates that are properly partitioned into subsets. In [19], they developed an online signature verification approach based on writer-specific features, and an again on writer-specific classifier. Which features would best suit the author and which classifier would be used to verify the author were taken according to the error rate obtained with the training samples. Experimental results indicated the effectiveness of the features they had used for online signature verification, depending on the author. Moreover, they also noted that the error rate was lower, when compared to many existing contemporary studies, on online signature verification, especially when the number of existing training examples for each author was sufficient.

Machine learning methods are also used in signature verification systems. In machine learning-based signature verification processes, first of all, the model is trained with real and fake signature samples. Then, the similarity ratio between the fake signature being questioned and any signature sample in the training set is tried to be determined. In the continuation of the article, studies carried out using machine learning algorithms are given.

In the study of [20], a method which based on learning and encoding of rare words as a tool in providing feature field for offline signature verification is propsed. They used the K-SVD dictionary learning algorithm to create a writer-oriented dictionary. When they tested their sparse representation-based methods with the SVM classifier, they obtained successful results for the validation problem.

In [21] they created a writer-independent signature verification system by using single-class SVM. Upon noticing that SVM-based classification could make accurate classification in the presence of a large sample and that that success decreased when they reduced the sample size, they carefully adjusted the optimum threshold by combining the different distances between the signature samples, thus, they tried to achieve correct classification success with less samples.

In [22] they conducted an application to identify attacks developed against offline signature verification systems. In their applications, they aimed to determine the threats to offline handwriting signature verification with Contradictory Machine Learning method and to find the effect of conflicting samples on biometric systems. In study of [23], an online and offline signature verification model based on pixel density levels were proposed. For the signature verification process, a comparative analysis was performed using classifiers such as decision tree, Naive Bayes and KNN. As a result of their studies in which they used the DWT method for feature extraction, they achieved a classification success of 99.90% with decision trees, 99.82% with Naive Bayes and 98.11% with KNN.

In [24] they proposed a system that is made of combination of signature verification, machine learning, IoT and blockchain technologies so as to cope with the risk of identity theft that may occur during online trading. In their system, the signals of roll, slope and deviation values received from the MPU6050 sensor (Inertial Measurement Unit) are analyzed by using Digital Time Wrapping in order to obtain the DTW minimum distance in authentication of the user. When it comes to cryptocurrencies, they mention about a system design in which the private key is not stored, but the same unique private key assigned to the user by the Blockchain is generated each time by using a method involving biometrics and machine learning.

In [25] they applied the AlexNet, which is a convolutional neural network algorithm, so as to recognize the offline Chinese signature. Depending on the writer, they managed to distinguish between real and fake signatures. They concluded that classification success of AlexNet's was higher than that of SVM.

In study [26], they mentioned a small 3-layer deep convolutional neural network, trainable parameters of which are several times less than those of previously reported in the literature, so as to verify the offline signature. They used these networks with 2 different configurations. In the first one, they used it for a feature extractor function in a hybrid classifier. And in the second one, they used it as an end-to-end classifier in a Siamese network. In the hybrid classifier scheme, they used the support vector machine in order to verify the authenticity of the signature.

In [27], a new approach for online signature verification based on machine learning method is presented. In the method they proposed, they considered the average values of the attributes for validation. They enabled that features such as x and y coordinates, timestamp, pen ups and downs, azimuth, elevation and pressure, which they used, were learned by different classifiers (Naive bayes, J48, MLP, PART, Bayes Net, random forest and random tree).

3. Methods

In this section, CNN and Siamese Network, One-Shot Learning, pre-processing steps carried out on signature images, architecture formed for offline signature verification problem, respectively, are mentioned.

3.1. CNN (Convolutional Neural Networks, CNN) and Siamese Network

CNN is among the most successful and widely used architectures in the deep learning community, especially for computer vision tasks. CNN architecture usually consists of 3 layers. The first one is the convolutional layer, in which a kernel (or filter) of the weights is convoluted so as to extract the features. The second one is the nonlinear layer, which applies an enable function to the feature maps, thereby enabling the network to model nonlinear functions. And the third one is the pooling layer, which reduces spatial resolution by replacing neighborhoods in a feature map with some statistical information about these neighborhoods (average, max, etc.). The neural units in the layers are locally interconnected. Each layer of the CNN carries the input to an output of neuron activation, thus creating fully connected layers. After all these things, the input data is matched to a 1-dimensional feature vector [30-31].

The Siamese neural network is a network architecture that includes 2 identical subnets. Twin CNN's have an equal configuration, where the same parameters and shared weights are combined with a distance metric. In the event of a parameter update, this case is reflected in both subnets. In this architecture type, one of the twin networks takes a real signature image as input and the other one takes a signature image that is requested to be verified by the model as input. Afterwards, each twin network does a feature extraction based on the given input. Finally, the difference (similarity-difference) of the features extracted by each of the twin networks is found by calculating the distance metric with the loss function applied in the last output layer. The contrastive loss, which is a loss function mostly used in Siamese networks, is defined in (1) [35]. Since the Siamese architecture yields successful results in the scenarios of comparing the similarities of the picture images, this architecture has been specially preferred.

$$L(s_1, s_2, y = \propto (1-y)D_w^2 + \beta y \max(0, m - D_w)^2) \tag{1}$$

The s1 and s2 values included here represent the signature images in the input and y is a binary indicator function that indicates whether two examples belong to the same class or not. α and β are two constants, and m is the numerator. $D_w = ||f\ (s_1; w_1) - f\ (s_2; w_2)||_2$ is the Euclidean distance. f is the embedding function that matches a signature image with a real vector space through CNN. w1, w2 are the learned weights for a particular layer of the network [35].

According to the Siamese network, it is expected that feature vectors of image pairs belonging to the same class are closer to each other, while feature vectors of image pairs belonging to different classes are far from each other. In the last stage of this architecture, a threshold value is determined in the distance metric calculated and it is decided whether the 2 images belong to the same class or not [35].

3.2. One-Shot Learning

The Siamese network supports the One-Shot way of learning. In one-shot learning, learning can be done from a single input image and a single target image [35]. While most machine learning-based object classification algorithms require making training by using a large number of sample images, in One-Shot learning, it is aimed to obtain information about classes with one or more images from each object category [36].

In order to create a model in one-shot assisted image classification, first of all, a neural network that can distinguish the class identities of image pairs must be learned. This step constitutes the image validation step. The validation model learns the probability that the input pairs belong to the same class or to different classes, in other words, the similarity-difference ratios. Later, it is subjected to one-shot classification by using the network that is successful in the verification process. In the one-shot phase, an image pair is created with the test image and the image belonging to the new class and evaluated by the previously learned model, and it is decided whether the image is a real-fake signature [37].

In the network architecture established in this study, first of all, image vectors were learned with a supervised metric-based approach, and then the features of this network were re-used with on-shot learning without the need for retraining. The method adopted for the solution of the signature verification problem is given in Figure 1.

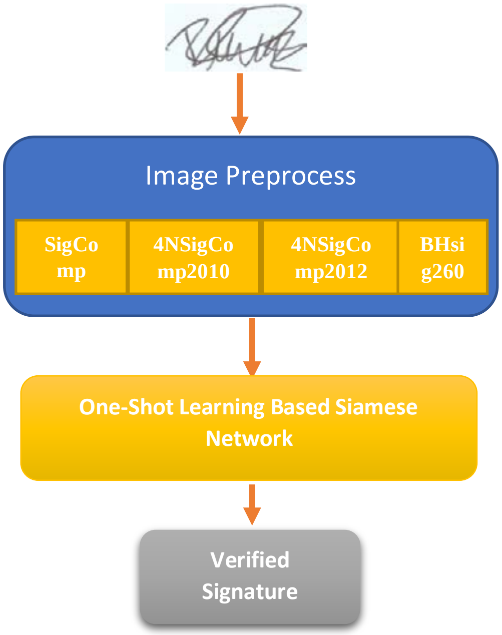

Figure 1. Solution Steps of the Signature Verification Problem

3.3. Pre-processing

Primarily, the "bounding box" method, known as the bounding box, and enabling the excess background images to be clipped, was applied on the used image set. Since in the generated neural network, training in the form of a stack is made, it is essential that the images to be used as input be standard in size. Therefore, sizing process was performed on the signature images. In order for the learning algorithm to better understand the features of the picture, the "binary thresholding" method, which converts the signature images into binary, was applied to each pixel in the signature image. Afterwards, the images were inverted so that the pixel values of the background could be 0. In the normalization process performed on the image, the standard deviation of the pixel values was achieved as a result of dividing these values. The pre-processing step was carried out on both the test and training set. Figure 2 shows the preprocessing steps.

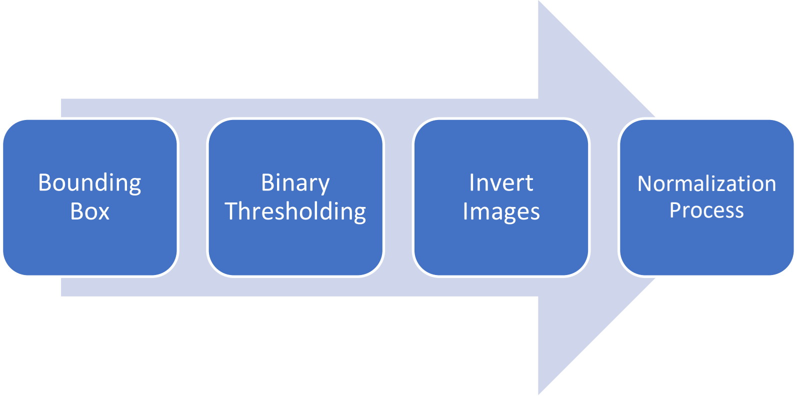

Figure 2. Preprocess Steps of Images

3.4. Network Architecture

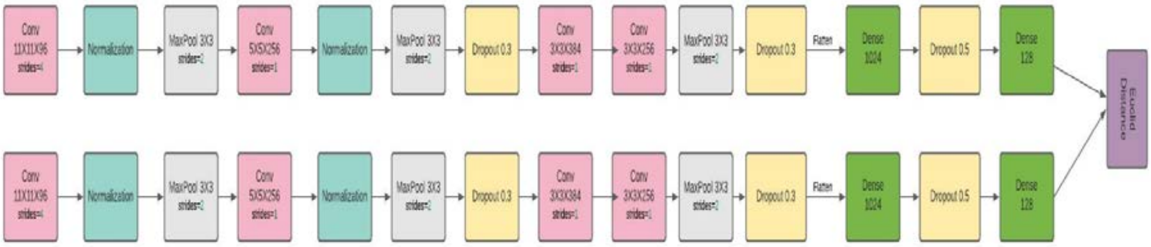

Figure 3. Siamese Network Architecture

In the established network architecture, a basic CNN was created with 4 convolution layers and then 2 fully-connected layers. Nuclei and neuron numbers are shown in Figure 3. Relu (Rectified Linear Units) is used as the activation function in all convolutional and fully-connected layers throughout the network. Each layer has a valid padding. Also, each block of convolutional layers is followed by a max-pooling layer with a filter size and stride of 2. The fully-connected layer in the last step represents the 128-neuron embedding vector of the input signature image. The 2 pairs of images given to the network are labelled with 1 if they are in the same class and labelled with 0 if they are in different classes. This situation is stated in the equation in (2).

$$f(x) = \begin{cases} 1 \ldots if\ (s1, s2)\ (Genuine, Genuine) \\ 0 \ldots if\ (s1, s2)\ (Genuine, Forged) \end{cases} \qquad (2)$$

4. Experiments

The developed signature verification algorithm has been tested on SigComp2011, BHSig260, 4NSigComp2010 and 4NSigComp2012 datasets.

4.1. SigComp2011

This dataset was published for the International Signature Verification Competition (SVC) at the ICDAR 2011 conference. The dataset includes online and offline signatures of Chinese and Dutch writers. In the study performed, the offline signatures of the SigComp2011 dataset belonging to the Chinese writers were used for both training and testing purposes. In the sub-dataset consisting of Chinese signatures, the training set contains 576 images for 10 identities, approximately 25 real signatures for each identity and 30 fake ones. The Chinese test set of the SigComp2011 dataset consists of 2 subsets as “reference” and “questioned”. Here, the reference set consists of real signatures and the questioned set consists of both real and fake signatures [32]. 576 signatures of this dataset, consisting of both real and fake signatures, 80% were used for training and 20% for verification. The signatures reserved for testing, 10% of those in both the "reference" and "questioned" folders were used for testing purposes.

4.2. BHsig260

The BHSig260 signature dataset contains the signatures of 260 persons, among them 100 subsets of the set consist of Bengali signatures and 160 subsets consists of Hindi signatures. There are 6240 real signatures and 7800 qualified fake signatures in the whole set. Each identity has 24 real and 30 qualified fake signatures. Also, for each of the signers, 24 genuine and 30 forged signatures are available. This results in 100x24 = 2400 genuine and 100x30 = 3000 forged signatures in Bengali, and 160x24 = 3840 genuine and 160x30 = 4800 forged signatures in Hindi [38]. In the conducted study, both Hindi and Bengali signatures were used separately for training and testing. Real and fake signatures of all authors in both the Bengali dataset and the Hindi dataset were used for training and testing purposes. In other words, some of the authors were not allocated for training and the rest for testing. Accordingly, 70% of the 2400 real signatures in the Bengali dataset were used for training, 20% for verification and the rest for testing. This separation format is also adopted for the Hindi dataset.

4.3. 4NSigComp2010

This dataset consists of offline signature images. The signature collection for education includes 209 images. Signatures consist of 9 reference (real) signatures and 200 queried signatures belonging to the same writer. In 200 query signatures, there are 76 real signatures written by the reference writer and 104 simulated/fake signatures (written by 27 fraudsters freely copying the reference writer’s signature features). The remaining 20 signatures are masked signatures written by the reference writer. Masking process involves an attempt to deliberately alter the signature of the reference writer so as to avoid being identified. The simulation/forgery process involves an attempt by a person to imitate the reference signature features of a genuine original writer.

This dataset contains 125 signature collections for testing. The signatures consist of 25 reference signatures and 100 queried signatures, this time belonging to another writer, apart from the writer for training. Of 100 query signatures, there are 3 real signatures written by the reference writer in normal signature style and 90 simulated signatures (freely typed by 34 fraudsters copying the reference writer's signature features). Moreover, there are 7 masked signatures written by the reference writer [33]. Of the part of this dataset reserved for training, 70% was used for training and 30% was used for validation. 20% of the part reserved for testing was used for testing purposes.

4.4. 4NSigComp2012

The training set of this dataset consists of the training and test set of 4NsigComp2010. In total, it includes the signatures of two examples writers. The first writer has 9 reference signatures and 200 queried signatures. Of these 200 queried signatures, 76 are real, 104 are forgery/fake and 20 are masked. And for the second writer, there are 25 reference signatures and 100 queried signatures. Of these 100 queried signatures, 3 are real, 90 are forgery/fake and 7 are masked.

The test set includes signature samples of belonging to 3 different writers. Query signatures consists of a mixture of real signatures, disguised signatures, and qualified frauds [34]. 90% of the part of this dataset reserved for training was used for training and 10% for validation. 20% of the part reserved for testing was used for testing purposes.

5. Results

In Table 1, the success results, which were obtained as a result of the One-Shot Learning-based Siamese Network method applied in solving the writer-independent offline signature verification problem, are given. Trials were applied separately for each dataset. Furthermore, real and fake signature pairs were used both when calculating accuracy and when comparing the similarity of 2 signature images. In the training conducted on each dataset, random signature pairs belonging to that dataset were selected. The performance evaluation of the offline signature verification task is not case having a standard. Because the way the training set given to the model is created, in other words, how much of it will be reserved for real and fake signatures, or how different datasets will be combined so as to obtain a new dataset is a completely personal application, the signature verification process is not a uniform task.

Table 1. Dataset values

Dataset	Accuracy	FAR	FRR
4NSigComp2010	89.99	10.22	8.33
SigComp2011	90.11	7.89	6.42
4NSigComp2012	93.23	6.77	7.02
BHsig260-Bengali	91.17	9.83	8.27
BHsig260-Hindi	92.35	8.92	7.65

Table 2 shows the accuracy of our proposed work together with other state-of-the-art methods on different datasets discussed in subheadings of Section 4.

Table 2. Comparison of the proposed work with the state-of-the-art methods on various signature databases

Databases	***State of art Methods***	***Accuracy***
SigComp2011	Ref [12]	82.5%
SigComp2011	Ref [39]	88%
SigComp2011	**Our proposed work**	**90.11%**
Bengali	Ref [7]	86.11%
Hindi		84.64%
Bengali	Ref [38]	66.18%
Hindi	Ref [38]	75.53%
Bengali	Ref [40]	84.90%
Hindi	Ref [40]	85.90%
Bengali	Ref [26]	75.06%
Hindi	Ref [26]	89.33%
Bengali	**Our proposed work**	**91.17%**
Hindi	**Our proposed work**	**92.35%**
4NSigComp2012	Ref [41]	88%
4NSigComp2012	**Our proposed work**	**93.23%**

5.1. Evaluation Protocol

A threshold value was used so as to detect whether signature pairs belong to the same class or not. Provided that the difference (dissimilarity ratio) between the two images is less than the threshold value (0.42), these two signatures are considered real-real, but provided that the difference is greater than the threshold value, these two signatures are considered real-fake. Performance assessment of the model was carried out by using accuracy (accuracy), FAR (False Acceptance Rate), FRR (False Rejection Rate) metrics. According to this, FAR and FRR calculations are as they are shown in (3) and (4), respectively.

$$FAR = \frac{Number\ of\ forged\ Pairs\ accepted\ as\ a\ geniune\ pairs}{T\ otal\ number\ of\ Forged\ Pairs\ submitted} \times 100 \qquad (3)$$

$$FRR = \frac{Number\ of\ Geniune\ Pairs\ rejected}{Total\ number\ of\ Geniune\ Pairs\ submitted} \times 100 \qquad (4)$$

6. Conclusion

In this study, an effective writer-independent offline signature verification task was performed by establishing a One-Shot Learning-based Siamese network. The aim of the study is to distinguish between real and fake signatures. Experiments were conducted on the 4NSigComp2010, SigComp2011, 4NSigComp2012, BHsig260 datasets. The model was also able to be distinguishing for new signatures without the need for any re-training. High accuracy rates were obtained on all datasets that were used. The largest of these ratios is the one on the 4NSigComp2012 dataset. As a new study in the future, through GAN (Generative Adversarial Neural Networks) architecture, which will be created by using the same datasets, it is planned to distinguish between real signatures and those signatures produced in a forged way.

REFERENCES

1. Ghosh, S., Ghosh, S., Kumar, P., Scheme, E., Roy, P.P. (2021). A novel spatio-temporal Siamese network for 3D signature recognition. Pattern Recognition Letters. 144, 13-20.
2. Jain, S., Khanna, M., Singh, A. (2021). Comparison among different CNN Architectures for Signature Forgery Detection using Siamese Neural Network. In: 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 481-486. IEEE Press, Greater Noida, India
3. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Ortega-Garcia, J. (2021). DeepSign: Deep On-Line Signature Verification. Ieee Transactions On Biometrics, Behavior, And Identity Science. 3, 229-239
4. Jain, A., Singh, S.K., Singh, K.P. (2020). Handwritten signature verification using shallow convolutional neural network. Multimed Tools Appl. 79, 19993-20018.
5. Jagtap A.B., Sawat D.D., Hegadi R.S., Hegadi R.S. (2019). Siamese Network for Learning Genuine and Forged Offline Signature Verification. In: Recent Trends in Image Processing and Pattern Recognition. RTIP2R 2018, pp. 131-139.
6. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Ortega-Garcia, J. (2017). Biometric Signature Verification Using Recurrent Neural Networks. In: 14th IAPR International Conference on Document Analysis and Recognition (ICDAR), pp. 652-657. Kyoto, Japan
7. Dey, S., Dutta, A., Toledo, J.I., Ghosh, S.K., Llados, J., Pal, U. (2017). SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification. Pattern Recognition Letters. 1-7.
8. Ruiz, V., Linares, I., Sanchez, A., Velez, J.F. (2020). Off-line handwritten signature verification using compositional synthetic generation of signatures and Siamese Neural Networks. Neurocomputing. 374, 30-41.
9. Ghosh, R. (2021). A Recurrent Neural Network based deep learning model for offline signature verification and recognition system. Expert Systems with Applications. 168.
10. Chakladar, D.D., Kumar, P., Roy, P.P., Dogra, D.P., Scheme, E., Chang, V. (2021). A multimodal-Siamese Neural Network (mSNN) for person verification using signatures and EEG. Information Fusion. 71, 17-27.
11. Yapıcı, M.M., Tekerek, A., Topaloğlu, N. (2021). Deep learning-based data augmentation method and signature verification system for offline handwritten signature. Pattern Anal Applic. 24, 165-179.
12. Tahir, N.M., Ausat, A.N., Bature, U.I., Abubakar, K.A., Gambo, I. (2021). Off-line Handwritten Signature Verification System: Artificial Neural Network Approach. 1, 45.57.
13. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Ortega-Garcia, J. (2018). Exploring Recurrent Neural Networks for On-Line Handwritten Signature Biometrics. in IEEE Access. 6, 5128-5138
14. Hefny, A., Moustafa, M. (2019). Online Signature Verification Using Deep Learning and Feature Representation Using Legendre Polynomial Coefficients. In: n book: The International Conference on Advanced Machine Learning Technologies and Applications AMLTA, pp. 689-697.

15. Okawa, M.: Time-series averaging and local stability-weighted dynamic time warping for online signature verification. Pattern Recognition. 112, (2021)
16. Yılmaz, M.B., Yanıkoğlu, B. (2016). Score level fusion of classifiers in off-line signature verification. Information Fusion. 32, 109-119.
17. Calik, N., Kurban, O.C., Yilmaz, A.R., Yıldırım, T., Durak, A.L. (2019). Large-scale offline signature recognition via deep neural networks and feature embedding. Neurocomputing, 359, 1-14.
18. Zois, E.N., Alewijnse, L., Economou, G. (2016). Offline signature verification and quality characterization using poset-oriented grid features. Pattern Recognition. 54, 162-177.
19. Manjunatha, K.S., Manjunath, S., Guru, D.S., Somashekara, M.T. (2016). Online signature verification based on writer dependent features and classifiers. Pattern Recognition Letters. 80, 129-136.
20. Zois, E.N., Theodorakopoulos, I., Tsourounis, D., Economou, G. (2017). Parsimonious Coding and Verification of Offline Handwritten Signatures. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 636—645. Honolulu, HI, USA.
21. Guerbai, Y., Chibani, Y., Hadjadji, B. (2015). The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters. Pattern Recognit., 48, 103-113.
22. Hafemann, L.G., Sabourin, R., Oliveira, L.S. (2019). Characterizing and Evaluating Adversarial Examples for Offline Handwritten Signature Verification. IEEE Transactions on Information Forensics and Security. 14, 2153-2166.
23. Shah, A.S., Khan, M.A., Subhan, F., Fayaz, M., Shah, A. (2016). An offline signature verification technique using pixels intensity levels. International Journal of Signal Processing, Image Processing and Pattern Recognition. 9, 205-222.
24. Jain, V., Chaudhary, G., Luthra, N., Rao, A., Walia, S. (2019). Dynamic handwritten signature and machine learning based identity verification for keyless cryptocurrency transactions. Journal of Discrete Mathematical Sciences and Cryptography. 22, 191-202.
25. Wencheng, C., Xiaopeng, G., Hong, S., Limin, Z. (2018). Offline Chinese Signature Verification Based on AlexNet. In: International Conference on Advanced Hybrid Information Processing ADHIP 2017: Advanced Hybrid Information Processing, pp. 33-37.
26. Rateria, A., Agarwal, S. (2018). Off-line Signature Verification through Machine Learning. In: 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gorakhpur, India.
27. Chandra, S. (2020). Verification of dynamic signature using machine learning approach. Neural Comput & Applic. 32, 11875-11895.
30. Minaee, S., Boykov, Y., Porikli, F., Plaza, A., Kehtarnavaz, N., Terzopoulos, D. (2020). Image Segmentation Using Deep Learning: A Survey. arXiv.
31. Voulodimos, A., Doulamis, N., Doulamis, A., Protopapadakis, E. (2018) Deep Learning for Computer Vision: A Brief Review. Comput Intell Neurosci.
32. Liwicki, M., Blumenstein, M., Heuvel, E., Berger, C.E.H, Stoel, R.D., Found, B., Chen, X., Malik, M.I. (2011). Sigcomp11: signature verification competition for on- and offline skilled forgeries, In: 11th Int. Conf. Document Anal Recognit.
33. Malik, M.I. (2010). ICFHR 2010 Signature Verification Competition (4NSigComp2010).
34. Liwicki, M., Malik, M.I., Alewijnse, L., Heuvel, E., Found, B. (2012). ICFHR 2012 Competition on Automatic Forensic Signature Verification (4NsigComp 2012). In: 2012 International Conference on Frontiers in Handwriting Recognition, pp. 823-828. Bari, Italy.
35. Jagtap, A.B., Sawat, D.D., Hegadi, R.S. et al. (2020). Verification of genuine and forged offline signatures using Siamese Neural Network (SNN). Multimed Tools Appl. 79, 35109-35123.
36. One-shot learning, https://en.wikipedia.org/wiki/One-shot_learning
37. Koch, G., Zemel, R., Salakhutdinov, R. (2015). Siamese neural networks for one-shot image recognition. In: ICML deep learning workshop.
38. Pal, S., Alaei, A., Pal, U., Blumenstein, M. (2016). Performance of an Off-Line Signature Verification Method Based on Texture Features on a Large Indic-Script Signature Dataset. In: 2016 12th IAPR Workshop on Document Analysis Systems (DAS), pp. 72-77.
39. Alvarez, G., Sheffer, B., Bryant, M. (2016). Offline Signature Verification with Convolutional Neural Networks. In: Technical Report. Stanford University, Stanford.
40. Dutta, A., Pal, U., Llad´os, J. (2016). Compact correlated features for writer independent signature verification, In: ICPR, pp. 3411–3416.
41. Butt, U.M., Masood, F., Unnisa, Z., Razzaq, S., Dar, Z., Azhar, S., Abbas, I., Ahmad, M. (2020). A Deep Insight into Signature Verification Using Deep Neural Network. IntelliSys.