2021 18th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE), Mexico City, Mexico November 10-12, 2021.

Supervised Neural Network for Offline Forgery Detection of Handwritten Signature

Saleem Summra, Ghani Usman, Aslam Muhammad, Martinez Enriques A. M
National Center for Artificial Intelligence, KICS, UET, $Lahore^{1,2}$
Computer Science Department UET, $Lahore^{2,3}$
Department of Computer Science, CINVESTAV-IPN, $Mexico^{4}$
summra.saleem@kics.edu.pk, *usman.ghani@uet.edu.pk*, *maslam@uet.edu.pk* & *ammartin@cinvestav.mx*

***Abstract*—Authorized high security systems for legal contracts is need of the hour for an automatic authentication system. This study investigates the off-line signature verification system to identify skilled forgery based on Writer-Independent system approach. This research advances our understanding of layer architecture in deep convolutional neural network (CNNs) to perform specific task using optimized learning parameters. Four layered architecture with Adam optimizer produces significant accuracy of 88.39% for self-generated off-line handwritten signatures. The proposed model efficiently classifies forged signatures from genuine ones.**

***Index Terms*—Off-line signatures, Multi-layered CNN, optimizer**

I. Introduction

For decades, authorization systems are very popular, which includes fingers prints, palm recognition and handwritten signature verification. As signature is the bio-metric identifier to authenticate an individual and so are required in legal and financial contracts such as credit card contract, bank account and cheque books. A person's signature can vary day-by-day with possibility that it is completely changed; referred as intra-class variability. Multiple signatures from the same user can have variations and these signatures should be considered genuine. Other comes is the difference between the original signature and the forged one, termed as inter-class variability. Problem arises in this domain is fake signature because every person has his own signature for identification at document level but a person can also sign forged. And so, a signature that is same as the actual sample is susceptible. The reason behind is the practice to replicate the style of true signer. Forgery can be introduced in many ways such as by practicing the same signature, known as simulation forgery.

Other one is blind forgery, which is very easy to handle because the person has signatures easily distinguishable. Next comes the tracing forgery, in which signature is traced on paper. Fourth type of forgery is that in which signature is scanned on the paper known as optical transfer. Moreover, signature authentication can be done both online and offline. Online system includes various other factors like speed of writing, pressure of pen and strokes etc. while in offline system, these factors are of no concern. In this paper, offline authenticity is inferred and simulation forgery is targeted using convolutional neural network.

Proposed verification system scans the signature image and then after some processing declares it as fake or genuine. Feature extraction for this purpose is questionable and can be concluded after looking previous research. Literature solves this problem by extracting various features of signatures using datasets of GPDS [17], MCYT [19] and CEDAR [26] such as Hafemann et al. [12] aimed to minimize the error rate and discussed writer independent approach. Different methods have been employed for extracting features, including global features [20], fuzzy logic algorithm [21], geometric characteristics [22] and convolutional neural networks [23]. Few gaps are found in the literature like work on helpful features as input to convolutional layer , better network to be employed for classification of forgery signatures along with details of convolutional neural network and its architecture. Our contribution aims to improve error and validity in results, and suggested model should be able to identify forged class in inclined signatures as well [24], [25]. This signature authentication system can be installed in banks to secure the transactions, has extensive use in written agreements and articles of incorporation.

Purpose of the research aims for optimized layered architecture of convolution neural network (CNN) to discriminate a genuine signature from skilled forged by encompassing textual features of signature. These features are extracted from neural network by passing signature images directly to the network and are then trained on CNN model. Proposed solution addresses minimal layered architecture characterizing different aspects and features of inclined style signature or straight one with most appropriate parameters. Vital goal is to improve accuracy and optimize the learning parameters of neural network for given data-set. For this cause, self-generated data-set is used in experiments and errors are computed for given scanned signature samples. This study tackles the forged signature issue by improving learning parameters of neural network architecture.

The remaining sections of this paper are organized as follow: section II briefly explains literature related to signature forgery while section III describes the proposed methodology. Section IV gives details about statistics of offline signature data and section V narrates training and implementation details of model. Section VI and VII illustrates results and conclusion

978-1-6654-0029-9/21/$31.00 ©2021 IEEE

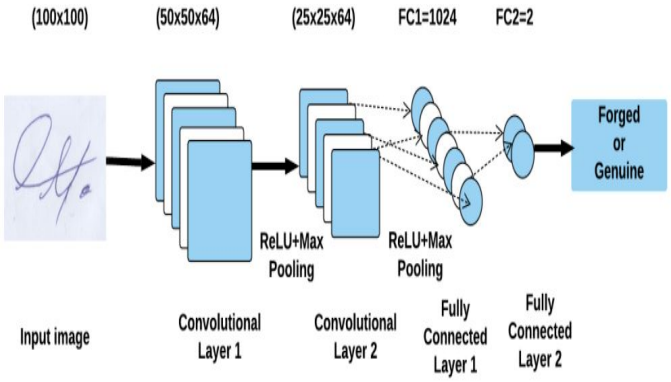

Fig. 1. Four layered System Architecture

of proposed study, respectively.

II. Related Work

4 The review of related previous work is structured in such a way that it includes their data sets, feature extraction techniques and learning algorithms. Giving general panorama of past-to-present literature, trained model can fall in category of either writer dependent or writer independent classification [12]. Previous studies have emphasized model trained on only one user and for verification another trained model for each user is needed. It increases complexity and is not that flexible as Writer-Independent classification is in which a single model is fitted on all users.
Images are pre-processed and are converted to gray scale image [1], [7]. These signature images are further skeletonized and noise is removed for further processing [8]. For further investigation of features, feature extraction plays significant role. Different features including Kolmogorov-Smirnov (KS), Kullback-Leibler (KL) divergence [6], K-Means, histogram frequencies, discrete cosine transform frequencies [10], aspect ratio, horizontal to diagonal length ratio and vertical and horizontal variance of signature [9], features were extracted and then selected one were used on the correlation filter (CFS) [14], baseline shift, pure width, projection, height, vertical and horizontal center [11].

Back propagation learning based model were also proposed in previous years. Kumar, D. A et al. [7] used CEDAR database [26] and feed forward back propagation neural network (FFBPN) in his work and determined accuracy and error. Vahid Malekian et al. [9] used Levenberg-Marquardt back propagation while Kumar et al. [7] extracted features using Concentric Circles Masking Method [4] and also with Nib lack algorithm [2] and then fed it to back propagation network (BPN). Barbantan et al. [14] fed CFS features to BPN and also tested Naive based model. Some authors have also suggested that CNNs can also be implemented but still offline signature verification needs more work to be done. Alvarez et al. [3] passed signatures through VGG-16 CNN model and the functions used at the output layer are Relu linearity and softmax nonlinearity. CNNs is also implemented on database GDPS-960 and Brazilia PUC-PR by Hafemann et al. [12] and SVM linear, SVM (rbf kernel) [13]. Soleimani et al. [15] also made comparison of models using UTSig[16], MCYT-75 [17], GPDSssynthetic [18] and GPDS960GraySignatures [19].

III. Proposed System and Methodology

The architecture of signature forgery detection system is based on deep convolution network described in detail in following sections.

A. CNN

A CNN consists of input layer, multiple hidden layers and an output layer. Usually CNN consists of convolutional layers with activation function (i.e. Relu, sigmoid and softmax etc.) fully connected layers and pooling layers. Convolution operation as shown in table I and figure 2 convolves the input image matrix with feature detector of size say K $\times$K and gives the mapped features where W is learn-able parameter. 2D Max Pool layer as stated in table I maps the maximum value in cluster of neurons to a single neuron. Function of fully

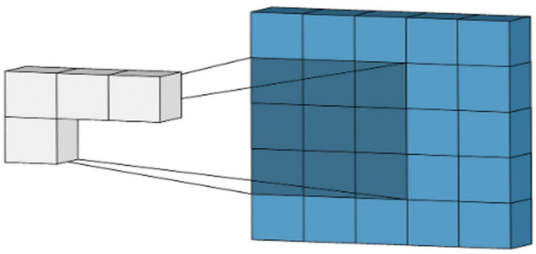

Fig. 2. Convolution Operation

connected layer is to connect neurons of one layer to other. In our case, $25\times25\times64$ (40,000) neurons were connected through fully connected layer to 1024 neurons. Relu activation function in I is used in convolutional layers.

B. Feature selection

The selection of set of features for signature verification is very important. Convolutional neural network is used for extracting features in this paper. Three suggested CNN architectures consisting of five convolutional layers, three convolutional layers and two convolutional layers with two fully connected layers at output are experimented in this research as shown in figure 3. Signature image of size 100 $\times$ 100 is fed to CNN. The proposed CNN is composed of two convolutional layers, two max pooling layers and two fully connected layers. Adam optimizer is used for this network along with Relu activation function at each layer.

• The first convolutional layer of proposed CNN has three channels with 64 filters.

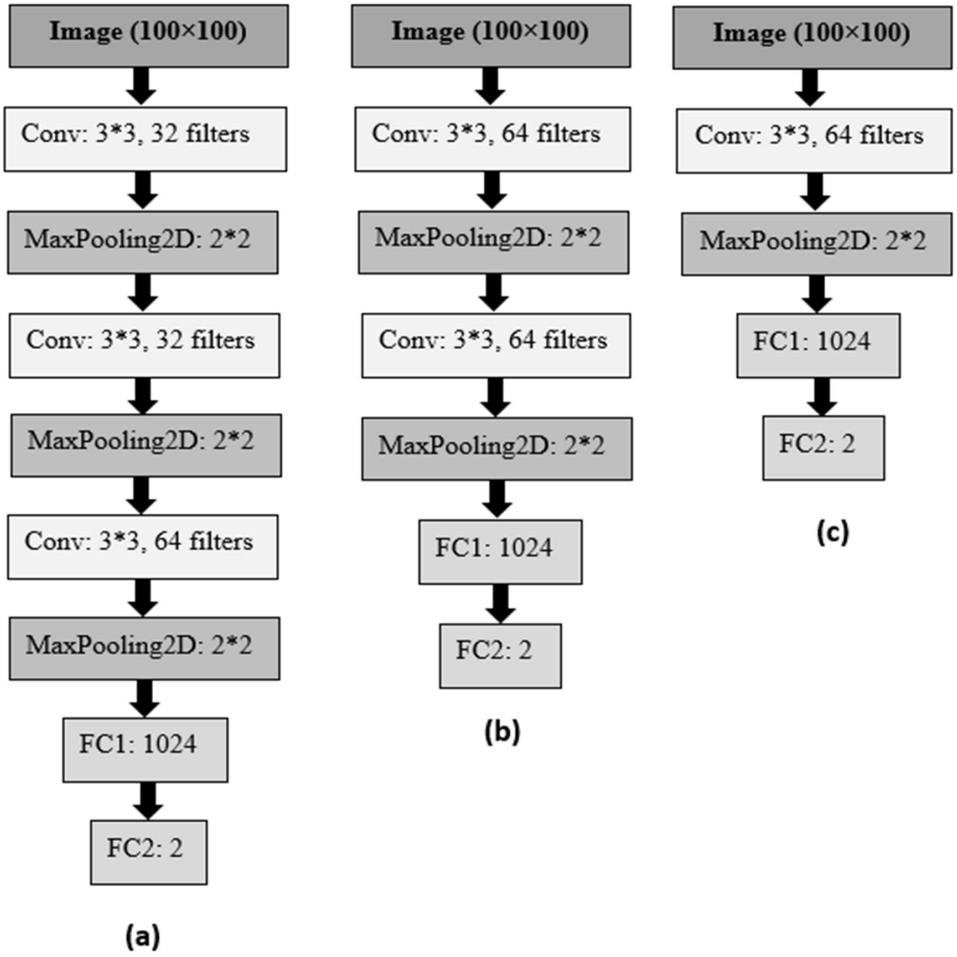

Fig. 3. Architecture of three CNN networks

• Next max pool layer of pool size two gives dimensions of 50×50×64.

•Second convolutional layer has 64 filters with three channels gives total of 50×50×64 pixels which is further max pooled with pooling size two. This gives total 25×25×64(40,000) pixels.

• Next layer is fully connected which has full connection to all activations in the previous layer, is used of size 1024 with softmax activation, selects 1024 pixels for further processing.

• Output layer comprises of fully connected layer with activation function Relu and maps output to class as forged or genuine. Loss function is applied to evaluate accuracy of model. Categorical cross entropy is used in our case and is defined in table I. Here p_i is actual probability. These layers as shown in figure 1 extract features for both types of signatures and are enough to identify even any complex signature.

Operation	Formula
Convolution	$y^t = h^{t-1} * W^t$
Maxpooling	$h^l_{xy} = max_{i=0,...,s,j=0,...,s} h^{(x+i)(y+j)}_{l-1}$
Relu	$Relu(y_i) = max(0, y_i)$
Fully connected Layer	$y^t = W^t h^{t-1}$

TABLE I: Mathematical formulas of operations used in network

C. Loss Function

Loss function is used to measure performance of architecture on dataset. If the predicted label is frequently wrong, output of loss function will be greater. On the other hand, if predicted label is mostly correct, output of loss function will be lower. For better results, loss function helps to analyze model behavior. In our experiments, categorical cross entropy loss function is used on different architectures. After that, softmax function is employed to measure probability for each class. Softmax equation as shown in eq. 1 computes probability for each possible outcome $z_1, z_2, z_3, ..., z_o$ where c is total number of possible outcomes. These softmax classification scores are further passed through exponential function and then division with sum of all exponential scores gives highest probability

for the class it belongs to.

$$softmax(z)_i = \frac{exp(z_i)}{\sum_j exp(z_j))} \text{for all i in} \{1, 2, ...c\} \quad (1)$$

IV. Dataset

For this purpose of off-line signature verification system, survey data were collected and maintained which contains 55 subjects each of which has 7 genuine signature samples and 7 forged ones. A sample form was prepared printed into multiples copies and distributes among subject for the purpose of data gathering, later it was scanned for experimentation. Both forged and genuine signatures are handled in our data set. Data is split in such a manner that model is trained on all subjects while evaluated on unseen signature images both forged and genuine. Dataset has been divided into three splits of ratio; 60-40, 70-30 and 80-20 for training purpose. Some of the samples of dataset are shown in figure 3. Data samples of four different subjects has been collected. Furthermore, first three column shows genuine signature of each subject and next three column shows forged signatures.

Fig. 4. Data samples from self collected dataset

V. Training and Implementation Details

Deep learning framework tensorflow has been used for training on different architectures. We have trained the networks using 2 GB GPU and having 8GB memory capacity. Hyper parameters of network are used as following: learning rate of $5e^5$, mini-batch size of 16 with Adam optimizer. Training set contains both genuine and forged signature samples of subjects. Three splits of data have been used for training of network. Relu activation function used at output of each convolution layer in network. Experiments are performed with three splits of data on 3 layered, 4 layered and 5 layered convolutional neural network. CNN network with two convolution and two fully connected layers performs best among all with a highest achieved training accuracy of 79.14 % and validation accuracy of 88.39% for 80-20 split ratio. While the sensitivity for training and validation set are 84.4% and 81.14%, respectively. Training time of network is about thirty five minutes for 17 epochs early stopping was employed to deal with over-fitting of network.

A. Updating Parameters

Purpose of the research was to investigate best optimizer and activation function for a better fit neural network architecture. For this purpose, various experiments were performed with different architectures as discussed above. With each architecture, various optimizers with activation function at each convolutional layer are employed. Experiments were made with 5 layered architecture and again, there were obtained poor accuracy with Adam optimizer and Relu function. Validation accuracy of 5 layered architecture with Nesterov, SGD and RMSprop and Relu activation were unable to classify test signature samples. So, further experiments were employed with 4 layered architecture and results were surprisingly better with Adam optimizer and relu activation. Other combinations of sigmoid and Relu function with SGD and RMSprop were failed for this architecture. When three layered architecture with single convolutional layer was structured and implemented with SGD and Relu function, it worked but results were better from 5 layers and Adam optimizer.

VI. Results and Discussions

For optimized and better results, accuracy is calculated after each iteration which helped in tuning parameters of model. We separated some forged and genuine images from the dataset for testing phase and some for validation phase. These signature images were tested after complete training and tuning of model. We proceeded with the model which reports better results on validation set and evaluate model on the basis of classification accuracy. Model with highest accuracy, is found better to use for distinguishing signatures. Mathematical expression for calculating accuracy has been shown in equation 2.

$$Accuracy = \frac{truePositives + trueNegatives}{totalSamples} \quad (2)$$

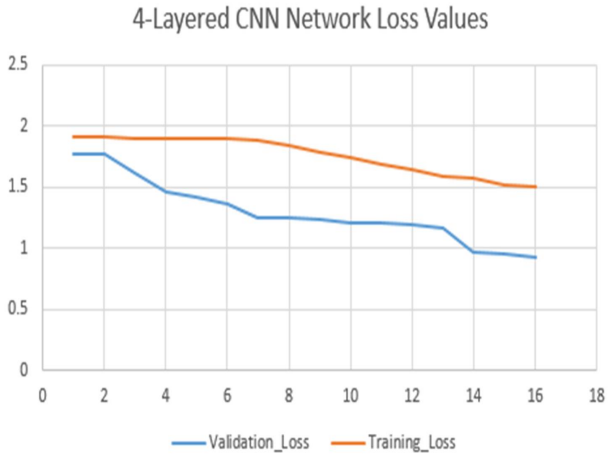

Fig. 5. Loss graph over successive epochs

	Network Architecture					
	5 Layered CNN		***4 Layered CNN***		***3 Layered CNN***	
Split Ratio	*Training Accuracy*	*Validation Accuracy*	*Training Accuracy*	*Validation Accuracy*	*Training Accuracy*	*Validation Accuracy*
60-40	59.73%	65.33%	71.23%	81.34%	57.44%	63.44%
70-30	64.72%	69.54%	76.87%	84.41%	59.44%	67.23%
80-20	69.33%	73.64%	79.14%	88.39%	61.33%	64.66%

TABLE II: Comparison of three CNN networks for training and validation accuracy on distinct splits of data

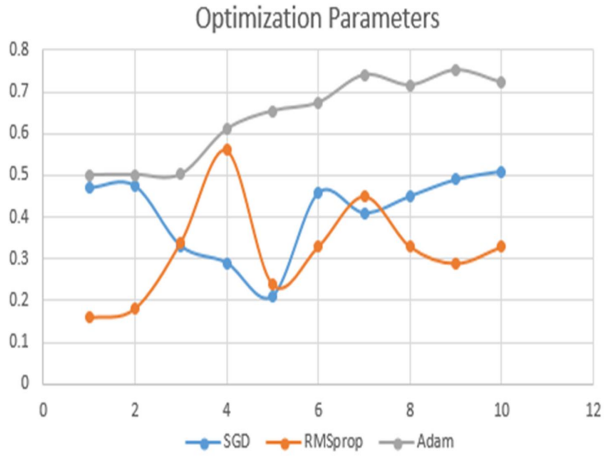

Fig. 6. Optimization graph of network accuracy using multiple optimizer

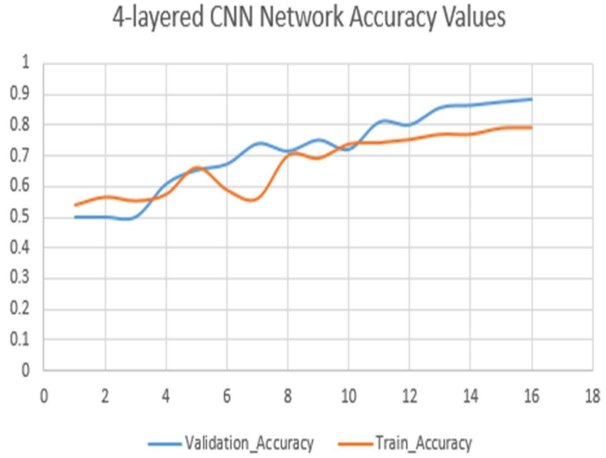

Fig. 7. Accuracy graph over successive epochs

Major aim of research study is to classify a signature as genuine or forged one. Data set is labeled into two classes for genuine or forged signature irrespective of subject identity. Dataset distributed into 60-40, 70-30 and 80-20 ratio has training and validation sets. Experiments with three splits of data were carried out for 3 proposed networks i.e. five layered, four layered and 3 layered architectures. The shallow networks are evaluated in this study due to less convoluted data features and optimized network. Furthermore, with limited number of subjects for signature data we can experiment with less deep network. The augmentation technique cannot be employed for data has global feature are crucial as compared to local features. 5-layered CNN network comprises of 3 convolution and two fully connected layers. In addition to this each block of convolution layer consist of one Relu and one max-pooling layer. Last fully connected layer outputs probability of signature to be forged or genuine. In 5-layered architecture maximum accuracy of 69.33% and 73.64% has been achieved on training and validation split for 80-20 ratio respectively as shown in table IV.

To preserve more features of signature at initial layers less deeper network was experimented with proposed three different splits of data. Four-layered CNN network comprises of two convolution and two fully connected layer with Relu and max-pooling supported in each block. Remarkable increase in accuracy of 79.14% and 88.39% is achieved for training and validation set as compared to deep network of five layers. Accuracy of training set starts from 54% and gradually increase to 79.14% with successive epochs. Furthermore, accuracy of validation set commences from 50% and reaches up to 88%. Similarly loss values for training and validation set has been shown in figure 4. Furthermore optimizer comparison and accuracy of proposed system has been shown in figure 5 and 6, respectively.

Experiment with further reduced layer leading to only one convolution layer was carried with dataset. But experimental results shows further reduction of layers reduce accuracy instead of generating improved results. Highest achieved accuracy of 59.44% and 67.23% for training and validation set is obtained.

VII. Conclusion

In this research work CNN network has been employed for signature verification task. Proposed research study shows that CNN network performs well for forgery detection when trained on feature of genuine and forged signatures of a subject. Self-collected Pakistani dataset for signature forgery detection is employed. Despite of lesser amount of data remarkable results have been achieved because CNN network is invariable to scaling, geometry, translation and rotation. Experiments with multiple CNN networks were carried out for signature forgery detection with conclusion that fewer numbers

of filters and layers give significant results. However, further improvements will be taken in future which will cover the more types of forged signatures and extracted features will be enough then to distinguish a forged signature from a genuine one.

ACKNOWLEDGMENT

We would like to thank National Center for Artificial Intelligence (NCAI) for funding research project. The research group would also like to thank full team and organization (KICS) for their technical support.

REFERENCES

[1] Gideon, S. Jerome, et al. "Handwritten Signature Forgery Detection using Convolutional Neural Networks." Procedia computer science 143 (2018): 978-987.

[2] Kumar, L. Ravi, and A. Sudhir Babu. "Genuine and Forged Offline Signature Verification Using Back Propagation Neural Networks." IJCSIT) International Journal of Computer Science and Information Technologies (2011).

[3] Alvarez, Gabe, Blue Sheffer, and Morgan Bryant. Offline Signature Verification with Convolutional Neural Networks. Tech. rep., Stanford University, Stanford, 2016.

[4] Kumar, D. Ashok, and S. Dhandapani. "A Novel Bank Check Signature Verification Model using Concentric Circle Masking Features and its Performance Analysis over Various Neural Network Training Functions." Indian Journal of Science and Technology 9.31 (2016).

[5] Jarad, Mujahed, Nijad Al-Najdawi, and Sara Tedmori. "Offline handwritten signature verification system using a supervised neural network approach." Computer Science and Information Technology (CSIT), 2014 6th International Conference on. IEEE, 2014.

[6] Srinivasan, Harish, Sargur N. Srihari, and Matthew J. Beal. "Machine learning for signature verification." Computer Vision, Graphics and Image Processing. Springer, Berlin, Heidelberg, 2006. 761-775.

[7] Kumar, D. A., and S. Dhandapani. "A Bank Cheque Signature Verification System using FFBP Neural Network Architecture and Feature Extraction based on GLCM." International Journal of Emerging Trends and Technology in Computer Science (IJETTCS) 3.3 (2014).

[8] RamachandraA, C., et al. "Robust Offline signature verification based on global features." Advance Computing Conference, 2009. IACC 2009. IEEE International. IEEE, 2009.

[9] Malekian, Vahid, et al. "Rapid off-line signature verification based on Signature Envelope and Adaptive Density Partitioning." Pattern Recognition and Image Analysis (PRIA), 2013 First Iranian Conference on. IEEE, 2013.

[10] Ribeiro, Bernardete, et al. "Deep learning networks for off-line handwritten signature recognition." Iberoamerican Congress on Pattern Recognition. Springer, Berlin, Heidelberg, 2011.

[11] Karki, Maya V., K. Indira, and S. Sethu Selvi. "Off-line signature recognition and verification using neural network." Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on. Vol. 1. IEEE, 2007.

[12] Hafemann, Luiz G., Robert Sabourin, and Luiz S. Oliveira. "Writer-independent feature learning for offline signature verification using deep convolutional neural networks." Neural networks (IJCNN), 2016 international joint conference on. IEEE, 2016.

[13] Hafemann, Luiz G., Robert Sabourin, and Luiz S. Oliveira. "Analyzing features learned for offline signature verification using Deep CNNs." Pattern Recognition (ICPR), 2016 23rd International Conference on. IEEE, 2016.

[14] Barbantan, Ioana, Camelia Vidrighin, and Raluca Borca. "An offline system for handwritten signature recognition." Intelligent Computer Communication and Processing, 2009. ICCP 2009. IEEE 5th International Conference on. IEEE, 2009.

[15] Soleimani, Amir, Babak N. Araabi, and Kazim Fouladi. "Deep multitask metric learning for offline signature verification." Pattern Recognition Letters 80 (2016): 84-90.

[16] A. Soleimani, K. Fouladi, B.N. Araabi, Utsig: A persian offline signature database, Submitted Manuscript, Submitted at IET Biometrics in Aug 2015.

[17] J. Fiérrez-Aguilar , N. Alonso-Hermira , G. Moreno-Marquez , J. Ortega-Garcia , An off-line signature verification system based on fusion of local and global infor- mation, in: Biometric Authentication, Springer, 2004, pp. 295–306 .

[18] M.A. Ferrer , M. Diaz-Cabrera , A. Morales , Static signature synthesis: A neuro- motor inspired approach for biometrics, Pattern Analysis and Machine Intelli- gence, IEEE Transactions on 37 (3) (2015) 667–680 .

[19] M.A. Ferrer , J. Vargas , A. Morales , A. Ordóñez , Robustness of offline signature verification based on gray level features, Information Forensics and Security, IEEE Transactions on 7 (3) (2012) 966–977 .

[20] Ramesh, V.E., Murty, M.N., "Off-line signature verification using genetically optimized weighted features", Pattern Recognition 32, (1999) 217–233.

[21] Ismail, M.A., Gad, S., "Off-line Arabic signature recognition and verification", Pattern Recognition 33 (2000), 1727–1740.

[22] Hobby, J.D., "Using shape and layout information to find signatures, text, and graphics", Computer Vision and Image Understanding, 80, (2000) 88– 110.

[23] Bajaj, R., Chaudhury, S., "Signature verification using multiple neural classifiers", Pattern Recognition (1997) 30, 1–7.

[24] Poddar, Jivesh, Vinanti Parikh, and Santosh Kumar Bharti. "Offline signature recognition and forgery detection using deep learning." Procedia Computer Science 170 (2020): 610-617.

[25] Jain, Soumya, Meha Khanna, and Ankita Singh. "Comparison among different CNN Architectures for Signature Forgery Detection using Siamese Neural Network." 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). IEEE, 2021.

[26] Larkins, Robert, and Michael Mayo. "Adaptive feature thresholding for off-line signature verification." 2008 23rd International Conference Image and Vision Computing New Zealand. IEEE, 2008.