2023 Third International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) | 978-1-6654-9400-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAECT57570.2023.10117669

An Offline Signature Verification Using Deep Convolutional Neural Networks

Shubhangi S.Rokade
Department of EDT
National institute of Electronics and Information Technology,
Aurangabad
shubhangirokade67@gmail.com

Shashank Kumar Singh
Scientist – 'B'
National institute of Electronics and Information Technology,
Aurangabad
shashank@nielit.gov.in

Saurabh Bansod
Scientist – 'C'
National institute of Electronics and Information Technology,
Aurangabad
saurabhbansod@nielit.gov.in

Prashant Pal
Scientist – 'B'
National institute of Electronics and Information Technology,
Aurangabad
prashantpal@nielit.gov.in

Abstract— **When a biometric authentication technology verifies a handwritten offline signature. Due to the time-variant character of signatures, signature verification is a difficult process. There are two primary forms of signatures, such as the dynamic signature used online. A static signature is one that is not currently active. The phrase intra-personal variability is used when an offline signature cannot be made in the same way even by a skilled signer. To prevent fraudulent signatures in this instance, we use a highly deep learning (DL) offline signature verification algorithm. The Convolution Neural Network (CNN) is a component of deep learning (DL). CNN was created and educated for two distinct. For two distinct models, such WI and WD, the writer-independent (WI) and writer-dependent (WD) approaches are the most crucial elements in the signature verification process.**

Keywords—Convolution Neural Network, Offline Signature, Deep learning, Signature verification.

I. Introduction

Since those early days, signatures have been the most popular biometric identification method and have always been written in pen on paper. Electronic devices like tablets and desktops can now be signed thanks to technological advancements. As a result, there are two sorts of signatures used today: offline (static) and online (dynamic). Because they have more identifiable qualities, online signatures are significantly simpler to authenticate. On the other hand, even though offline signatures are more prevalent, they are more challenging to authenticate since they lack the same distinguishing characteristics as online signatures [1][3].

In offline signatures, only the shape of the signature is present. They present a difficult research challenge because of this. Offline signatures are still a common verification method in use today, especially in legal documents, banking, and business transactions, even though they carry legal, ethical, and financial risks. Because of this, offline signatures are regularly abused by bad actors and utilized in fraud. Signature verification is used to stop fraud and bad intentions. As machine learning technology advances, new algorithms offer interesting options for signature verification. Due to these factors, signature verification is currently one of the most crucial issues in machine learning approaches that must be resolved [1] [3]. The inability to replicate offline signatures in the same way is their main flaw. The signatures may differ based on the writing materials used (pencil, paper, etc.), the writer's current state of mind, one's hand. Even the most skilled signers can never consistently use the same signature. The term for this is intra-personal. Fluctuation [2], [3]. Consequently, one of the primary obstacles for the highest intra-personal level of verification is offline signature. Variability between the different specimens originating from the same author. This makes the offline possible.

An NP-hard (non-deterministic) problem of signature verification polynomial-time challenging) issue. What's important about these Various studies have been conducted to understand the situation. Since 2004, signature verification. To solve this issue, competitions for digital signatures such as SigComp2011[2], SigWiComp2013 and 4NSigComp2012 were organized. Researchers have attempted to address this issue by utilizing support vector machine algorithms Dynamic Time Wrap (DTW) [3], [4], (SVM)[2] [3], Fuzzy Systems, Principle Component Analysis (PCA) Instruments[4], Probabilistic Neural Network (PNN)[5], Deep Multitask Metric Learning (DMML) [3].

Numerous fields, including autonomous cars, object recognition, motion recognition, and voice recognition, have seen substantial advancements because of deep learning. Each year, deep learning receives billions of dollars from companies like Google, NVidia, Facebook, and Microsoft that significantly advance this field. The deep learning approach has been shown to offer successful solutions in various domains with the help of academic and industry contributions [5] [4]. Although it appears that using the deep learning approach, a credible solution to the offline signature verification problem has not yet been discovered.

In the literature, DL and hybrid approaches produced the best results for offline signature verification. A two-step hybrid classifier method that involves identifying the owners of the signatures and establishing the authenticity of the signatures was proposed by Ribeiro et al. A fresh Deep Convolutional Generative Adversarial Network (DCGANs) model was put forth by Zhang et al. [5] for offline signature verification, and they reported that the approach is promising even though it falls short of the state-of-the-art for GPDS in terms of performance.

Hafemann et al. [2] employed a CNN model with two methods: WD for the classification stage and WI for feature extraction. For boosting the success of signature verification, they [2] compared two distinct CNN architectures that include AlexNet and VGG in a different study. Hafemann et al. [3] reported in 2017 The CNN model had an EER of 1.72% success in the GPDS-160 dataset. Using the SIGCOMP 2011 dataset, Tayeb et al. released a CNN-based signature verification application [4] and claimed an overall success rate of roughly 83 percent.

It has been noted in the literature that, despite some research utilizing the DL approach for offline signature verification, it has not yet had sufficient success [2] - [3]. With this work, we hope to advance the field of signature verification. We emphasize the study's finding that the CNN model can perform well in the offline signature and has been proven successful in many other domains. Determine whether it is supported by further feature extraction techniques.

In this study, we place more emphasis on CNN's accomplishments than on signature verification. Even though the results we got fall short of the state-of-the-art in the field of signature verification, we still think CNN has demonstrated its success in this area. We point out that if CNN is backed by additional feature-extraction techniques, high success will be attained.

There are 5 sections in this document. The methodologies employed in this study are outlined in the second section. The third section describes the proposed application. Results of the experiment are described in the fourth section, and the study's conclusion is delivered in the fifth section.

II. METHODOLOGIES

In this work, offline signature verification is done using the deep learning method. As a deep learning technique consist of convolutional neural network (CNN) and Artificial Neural Network(ANN) and hoc models were employed as the samples. The Convolutional Neural Networks utilized were trained separately utilizing Writer Dependent (WD) and Writer Independent (WI) formats (WI).

LeCun et al. made the initial CNN proposal for image processing, and it included two fundamental elements, such as spatially shared weights and spatial pooling. They enhanced the CNNs in 1998 and created LeNet-5, a ground-breaking 7-level convolutional network for digit categorization. The most popular DL architecture for feature learning nowadays is CNNs, which have successful applications in a variety of fields like driverless vehicles. character recognition, video processing, and medical image processing and object recognition.

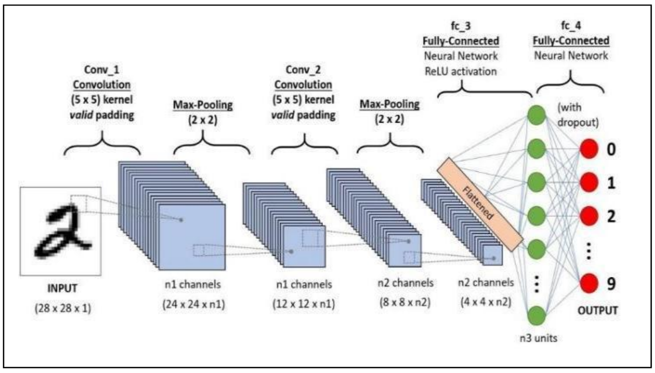


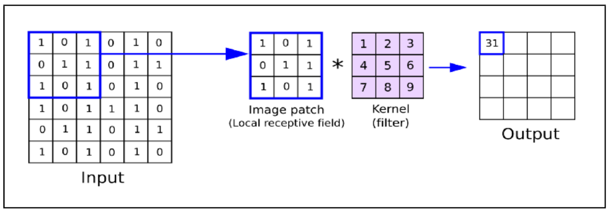
Fig. 1. Basic structure of CNN

As shown in Fig. 1, which was taken from a research by LeCunetal. [2], a CNN comprised of triple layers: a convolutional layer, a subsampling layer and a fully-connected layer. Using these convolutional operations and pooling operations, CNN seeks to learn the extract the characteristics of images. While the last layers of sampling explain pieces of forms and objects, the first layers of sampling define edges, color or data [2]. Convolution is accomplished in the convolution layer by multiplying these matrices with a bias and by shifting the sample to data matrix by input data matrix using the basic formulation of the convolution process as given in equation (1) and is represented by the basic convolution process in Figure 2. Pixels from the output image, input image, filter (kernel), and bias term were represented in the equation by y, x, w, and b, respectively.

$$Y_n = \sum_{n=1}^{9} (W_n x_n + b_n) \qquad (1)$$

Pooling is one of the effective strategy employed by CNNs. By propagating of the greatest activation, the pooling is utilized to spatially down-sample the previous layer's activation of the prior neuronal populations. The pooling's primary objective the model's computational complexity is being decreased through layers. by progressively reducing the dimension of the illustration.

Fig. 2. Basic convolution process



Every layer's end can be normalized using an activation function called a rectified linear unit (ReLU), if that is chosen. Equation describes the ReLU's fundamental process in eq (2).

$$ReLU(x) = \begin{cases} 0, if\ x < 0 \\ x, if\ x \geq 0 \end{cases} \qquad (2)$$

Fully connected layers (FC), the fundamental building blocks of conventional neural networks, make up the final layer in CNN. Neurons in the next layer are connected to one another to create FC. After that, a Soft Max layer is used to normalize it to a probability distribution. The goal of FC is to convert the high-level filtered images into votes. These votes are represented as weights, or the degree to which a value is connected to a certain category.

Another technique we employ in this study is to divide the training data into Writer Dependent (WD) and Writer Independent (WI) data sets, and then train the CNN model independently for each of these two data sets. In the literature, it can be noted that offline signature verification systems use two different methodologies, such as WD and WI [5] In WD, the classifier is trained separately for each person using only their unique signatures.

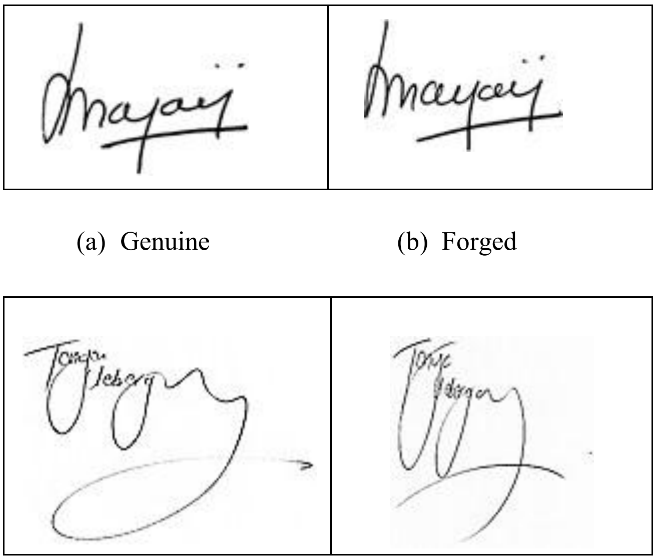
In WI, however, it is trained using the signatures of every person. Although WI aims to address the issue of a small number of training samples, it's possible that many of the features unique to signature authors will be lost. The issue of a tiny training sample is something that WI seeks to address, however it's probable that many features can disappear [1], [2,]

III. PROPOSED METHOD

In this paper, we suggested a CNN-based signature verification approach to stop hostile individuals from forging signatures. By highlighting the effectiveness of the suggested method in the field of signature verification, we hope to make a contribution to this subject. Our approach uses CNN architects that have received specialized training for WI and WD. The GPD Synthetic Signature data set, which has been extensively used in the field of signature verification, was employed in the model.

The "Institute Universitario para el Desarrollo Tecnológico and la Innovación in Comunicaciones (IDeTIC)" provided the signature dataset. The 4000 unique signatures in the GPDS synthetic Signature dataset are collected. Each person has 30 samples of fraudulent signatures in addition to 24 real signatures. All of the signatures were produced using various pen models. The signatures have a resolution of 600 dpi and are in the "jpg" format. Figure 3 displays instances of real and fake signatures from this database.

Using the Keras Framework, the Python-based application was created. Theano and Tensorflow are the two backends for the Keras Framework. Tensorflow backend was utilised in this investigation. The reported results are encouraging even though the models were not backed by any further feature extraction techniques.



(a) Genuine (b) Forged

(a) Genuine (b) Forged

Fig. 3. Forged and Genuine signature examples from GPDS synthetic signature

In the initial this model the signature is sampled under WD signatures. Single person fabricated 54 signatures which includes 24 as genuine and 30 as forgeries. By selecting 30 signatures from the samples of signatures used for training. The sampled signature consists of 15 samples as genuine and 15 samples as forgeries. Other collectives of 24 samples are intimated for test. Hence this model is composed of five Conv2D layers, two MaxPooling2D layers, three Dense layers and two Dropout layers collectively. In the model, every Conv2D layers are fabricated by ZeroPadding2D layer. The signature images used for samples are gray scale images sized as 300px width and 210px height. Here the shape of the model is "shape (210,300,1)", which is the same with the size of the images. Rectified Linear Units (Re LU) is implemented as the activation function in the Conv2D layers. Respectively, the structure of the layers used in this model consist of First Conv2D layer which has 32 dimensions that is 3px width and 3px height. Second Conv2D layer has 64 dimensions has the same 3px width and 3px height. After the sampling the signature in second Conv2D layer, first MaxPooling2D layer get increased with the size of 3px width and 3px height with stride size of 2px width and 2px height. Then the images were sampled in Third Conv2D layer which has 128 dimensions that are 3px width and 3px height. In the final sampling process, the Fifth Conv2D layer is again consist of 128 dimensions that are 3px width and 3px height. After the fifth Conv2D layer, second MaxPooling2D layer is composed of the same properties as the first MaxPooling2D layer was used. First and second Dense layers (Fully connected convolution layers) are composed of two hundred fifty-six dimensions and Re LU activation function of the samples. After the two dense layers, a fabricated layer with a 0.4 parameter was applied. Finally, classification was performed using the dense layer of which the features of Soft Max activation function is used. The consecutive model used as WI signatures to train CNN. It consists of 540 samples of signatures in total, which collectively include 240 samples as real ones and 300 samples as fake one, all these samples are collected by ten separate people. Random selections of signatures were made for training. Among that 300 signatures are used, out of which 150 were forgeries and 150 were real. For testing, another 240 signatures are again sampled

TABLE. 1 OBTAINED RESULT FOR WI AND WD APPROACHES

DL Architecture	*Signature Method*	*Test Data*	*Training Data*	*Accuracy*
CNN	*WI*	*240*	*300*	*68%*
	WD	*24*	*30*	*82%*

According to the findings, WD has a 82% success rate compared to WI's 65% success rate. If the CNN method is used, it is anticipated that the success of the outcomes would rise by including more feature extraction techniques.

IV. CONCLUSION

One of the crucial steps after confirming handwritten signatures, which are the target of many forgeries, the subjects of recent research. This study used DL applications. Based on the successful CNN architecture results from numerous fields were used to verify signatures. CNN architecture was trained independently as WD for the study.as two distinct models, and WI. Among the main issues the issue with insufficient training data for the CNN application for signature verification. To resolve this We used two distinct CNN models to the issue. We sought to Utilize WI to address the issue of a poor signature example. while WD improves categorization accuracy. The acquired outcomes demonstrated how promising CNN architecture is to confirm a signature. In this research, database for GPD Synthetic Signature. In subsequent efforts, we want to improve the findings by utilising various DL algorithms supplemented by additional feature extraction techniques.

REFERENCES

[1] G. Alvarez, B. Sheffer, and M. Bryant, “Offline Signature Verification with Convolutional Neural Networks,” 2016.

[2] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Analyzing features learned for Offline SignatureVerification using Deep CNNs,” in 2016 23rd International Conference on Pattern Recognition (ICPR),2016, pp. 2989–2994.

[3] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Offline handwritten signature verification #x2014; Literature review,” in 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA), 2017, pp. 1–8.

[4] M. I. Malik, M. Liwicki, L. Alewijnse, W. Ohyama, M. Blumenstein, and B. Found, “ICDAR 2013 Competitions on Signature Verification and Writer Identification for On- and Offline Skilled Forgeries (SigWiComp2013),” in 2013 12th International Conference on Document Analysis and Recognition,2013, pp. 1477–1483.

[5] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, “A survey ondeep learning for big data,” Inf. Fusion, vol. 42, pp. 146–157, 2018.