IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ENHANCING SIGNATURE VERIFICATION USING CONVOLUTIONAL NEURAL NETWORKS FOR FORGERY DETECTION

Dr. Reshma Banu
reshma127banu@gmail.com
Professor, Computer Science and Engineering Vidya Vikas Institute of Engineering and Technology, Mysore

Monika H M
Student of Computer Science and Engineering Vidya Vikas Institute of Engineering and Technology, Mysore

Saniya Sultana
Student of Computer Science and Engineering Vidya Vikas Institute of Engineering and Technology, Mysore

Nisarga M
Student of Computer Science and Engineering Vidya Vikas Institute of Engineering and Technology, Mysore

Kumar H
Student of Computer Science and Engineering Vidya Vikas Institute of Engineering and Technology, Mysore

Abstract:

The issue of handwritten signature verification hasn't been fully solved despite new research in the area. In our social and legal lives, handwritten signatures are crucial for authentication and proof. Only if a signature comes from the intended recipient can it be approved. It is extremely unlikely that two signatures created by the same individual will be identical [7]. Even though two signatures are made by the same individual, many signature characteristics can change. Determining the forgery thus becomes a difficult job. Systems for checking signatures are made to identify whether a specific signature is real or fake. In this research, a signature verification method based on convolutional neural networks (CNNs) is suggested. Using a CNN neural network model, we can extract a more accurate representation of the image information. Raw pictures of signatures are used to train the CNN model for feature extraction and data augmentation, and judgments are made about whether a given signature is genuine or forged. This software can be used to verify signatures on a variety of platforms, including signing loans and applications as well as legal documents.

Words to Know: CNN, feature extraction, pre-processing, machine learning, RELU, and deep learning.

1. Introduction:

A legal mark of a person, performed by hand for authentication, can be described as a handwritten signature. There are two major categories of techniques and systems used to address signature verification. The other is based on the online signature verification method, where more hardware devices are used and are immediately connected to the computer. The offline signature verification method relies on fewer hardware devices and relies on images taken with a camera. For offline verification, fewer characteristics are used. Since ancient times, the use of signer signatures to identify people has been a major innovation. Biometric devices are typically split into two categories:

- Verification
- Identification

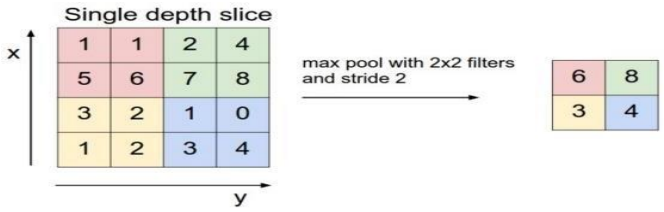
Verification and identity of people are two distinct processes. Verification determines whether a person's biometric truly belongs to them, whereas identification recognizes the person's biometric from a batch of candidates [1]. This essay examines the use of fingerprints to validate an individual. Two marks for signatures are used in the verification process: genuine and fake.

Due to the widespread use of signatures, many malicious actors attempt to forge them to obtain an advantage; as a result, very effective signature forgery detection techniques are required. Data acquisition, pre-processing, feature extraction, the comparison process, and performance evaluation are the five sub-problems that must typically be solved to create a signature verification and detection system. In this paper, we suggest an offline convolutional neural network technique for verifying handwritten signatures. With a CNN-based approach and Python and its libraries, we were able to effectively detect forged signatures [3]. With the help of a dataset of signatures, the CNN model is trained, and predictions are then made based on information indicating whether a signature is real or fake. Security systems in public locations like ATMs, official government buildings, colleges, legal organizations, etc., can be developed into apps or websites.

2. Convolutional Neural Network:

A multi-layer convolutional neural network with deep supervised learning design may have the proverbial capacity to extract features for classification by itself. They can be used in picture classification, segmentation, and image analysis for

medical purposes. An automated feature extractor and a trainable classifier are the two components of CNN [4]. The feature extractor uses convolutional filtering and down sampling to extract the feature from the incoming data.



A CNN is used in the suggested technique as both a feature extractor and a classifier. We presume that a CNN trained for classifying fake and real signatures can extract useful features for differentiating forgery-related behavioral traits, such as hesitation and delay before drawing the signature. complex signature component. As a result, the CNN feature extractor's data is used to create a feature vector. Each input image is passed through a succession of convolutional layers with filters (kernels), a pooling layer, fully connected layers, and the SoftMax function to classify an object with probabilistic values between 0 and 1. This process is done to train and test the deep learning CNN model.

The below figure shows the complete flow of CNN to process an input image and classify the objects based on values.

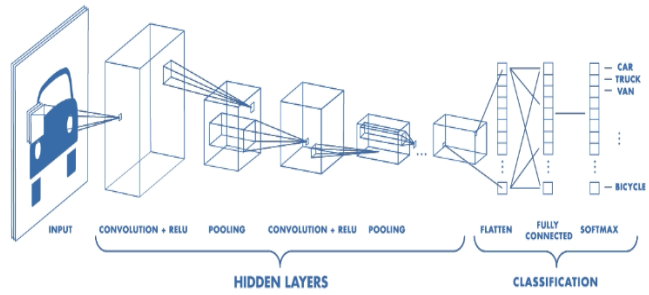


Fig. Layers of CNN

Convolutional layer: It is the first layer to extract features from an input image. Convolutional preserves the relationship between pixels by learning image features using small squares of input data. It is a mathematical operation that takes two inputs, such as an image matrix and a filter or kernel.

Stride: Stride is a parameter of the neural network's filter that modifies the amount of movement over the image. And it has many pixels shifted over the input matrix. When the stride is 1, we move the filters 1 pixel at a time; when the stride is 2, we move filters 2 pixels at a time, and so on.

Padding: Sometimes filters do not perfectly fit the input image. Then we have two options:

- Pad the picture with zeros (zero padding).
- Drop the part of the image where the filter did not fit. This is called valid padding, which keeps only the valid part of the image.

Non-Linearity (ReLu): ReLu stands for the rectified linear unit for a non-linear operation, which applies the non-saturating activation function f(x)=max (0, x). The purpose of ReLu is to introduce non-linearity into our CNN [5].

Pooling Layer: A pooling layer would reduce the number of parameters when the images are too large. Spatial pooling, also called sub-sampling or down sampling, reduces the dimensionality of each map while retaining important information. Spatial pooling layers can be of different types:

- Max Pooling
- Average Pooling
- Sum Pooling

Max Pooling takes the largest element from the rectified feature map. Taking the largest element could also take the average pooling or the sum of all elements in the feature map, which is called sum pooling

Fully Connected Layer: After several convolutional and max pooling layers, the final classification is done via fully connected layers. We flattened out the matrix into vectors and fed them into a fully connected layer, like a neural network.

3. Methodology:

The machine is supplied with the datasets. The samples are tested and trained using these databases. The public datasets are made up of image data for numerous signature examples. This information is transformed into a structure that can be processed. Both authentic and fake fingerprints can be found in the data. Each picture is categorized as either authentic or fake before being stored in a different directory.[23]

Pre-processing of data:

The pictures in the datasets are not identical and are not all oriented in the same way. Data pre-processing is required for this goal. The information is presented as pictures. A pre-processing method is used to enhance certain image features that are crucial for the subsequent processing of data samples or to reduce unwanted distortions in image data. Pre-processing includes resizing the picture, noise removal, grayscale to bitmap conversion, and RGB to grayscale conversion.

- RGB to Greyscale Conversion**:** This transforms all colour information to greyscale and removes all other colours. Images are depicted as a 3-pixel-deep matrix with X and Y dimensions. Red, green, and blue numbers on each plane range from 0 to 255. Each RGB colour's average pixel value is merged. Each colour band's luminance is merged to create an approximate grayscale value or 24 bits to 8 bits.

- Noise Removal: Any type of noise present in the picture is known to the analyst, and its quality is undefined. Noise is the result of errors in the acquisition process, which results in pixel values that do not represent the truth. To improvise the process, a known type of noise is very sparingly added to the grayscale picture.

  This procedure entails the removal of all commotion and the addition of salt and pepper noise

- Grayscale to bitmap: A matrix is created when a picture is converted from grayscale to bitmap.
- Resizing: The matrix to standard image size is changed.

Extracting Features:

Creation of features that could be compared using this process. The extracted image features are used as input in the following steps. There are three types of features: universal, mask, and grid. Wavelet coefficients and the Fourier coefficient are provided by global characteristics. Information about the signature line orientations is provided by the mask features.

Information about the general look and signature is provided by grid features [15].

Splitting Data:

In a two-part split, where one portion is used to evaluate and the other to train the model, the data is divided into two or more subsets. We will receive a smaller collection of data for training, and a larger set for testing.

Cross-Validation:

The next step uses data cross-validation to compare pictures and determine which are fake and which are authentic after training and testing.

Classification:

Procedure for determining whether an autograph is genuine. The extracted feature is compared with saved pictures following the feature extraction stage. whether the characteristics are considered to be fake or authentic.

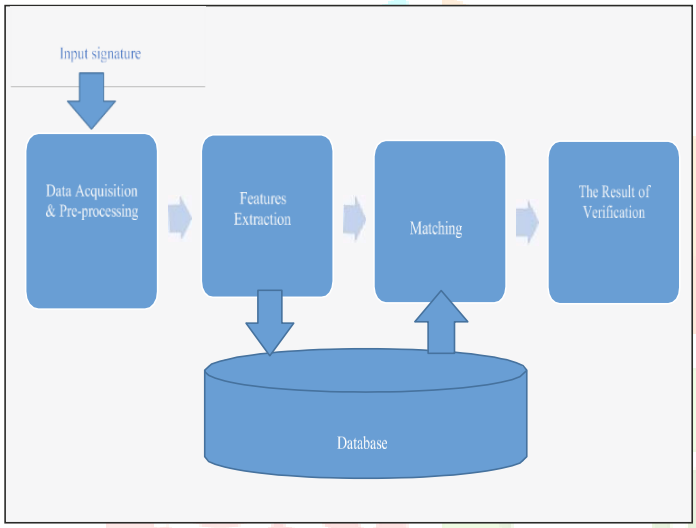


Fig. Signature Verification System

4. Conclusion:

The suggested system is capable of making forecasts for forgery detection by learning from signatures. The growing digitalization of many facets of daily life as well as new problems in offices and agencies calls for effective user verification techniques. Wherever a signature is used as a form of authentication, including banks and educational organizations, the system can be used. Because they can solve some issues comparatively easily, neural networks have proven successful in a variety of applications. Convolutional neural networks, the most effective model for picture recognition and verification, are used in this system. When given access to examples of real and fake signatures of the same individuals whose signatures were previously seen during training, CNN does a great job of verifying signatures. CNN correctly identified the input images as either genuine or fake, with two class labels for the result.

5. References:

[1] Gideon J., Kandulna A., Kujur AA., Diana A., Raimond K. Handwritten Signature Forgery Detection Using Convolutional Neural Networks 8th International Conference on Advances in Computing and Communication (ICACC-2018).

[2] Poddar J, Parikh V, and Varti SK Offline Signature Recognition and Forgery Detection using Deep Learning The 3rd International Conference on Emerging Data and Industry 4.0 (EDI40), Warsaw, Poland, April 6–9, 2020.

[3] Kshitij Swapnil Jain, Udit Amit Patel, Rushab Kheni (2021). Handwritten Signatures Forgery Detection using CNN. International Research Journal of Engineering and Technology (IRJET), vol 08 issue:01| Jan 2021.

[4] Handwritten Signature Verification using Local Binary Pattern Features and KNN 2019: Tejas Jadhav.

[5] Collobert, Ronan; Weston, Jason A Unified Architecture for Natural Language Processing: Deep Neural Networks with Multitask Learning Proceedings of the 25th International Conference on Machine Learning.

[6] Bin Xiao, Yang Wei, Xiuli Bi, and Weisheng Li (2020). Image Splicing Forgery Detection Combining coarse to redefined convolutional neural networks and adaptive clustering Information Science. 511:172–191.

[7] Ruiz, V., Linares, I., Samchez, A., and Velez, J.E. (2020). Off-line Handwritten Signature Verification Using Compositional Synthetic Generation of Signatures and Siamese Neural Networks Neurocomputing. 374:30-41.

[8] S Jerome Gideon, Anurag Kandulna, Aron Abhishek Kujur, r, Diana, and Kumudha Raimond (2018) Handwritten Signature Forgery Detection Using Convolutional Neural Networks Procedia Computer Science. 143:978–987.

[9] Hafemann L. G., Sabourine R., and Oliveria L. S., Learning feature for offline handwritten signature verification using deep convolutional neural networks and pattern recognition, volume 70, 2017, pages 163–176, ISSN 0031-3203.

[10] Syed Faraz Ali Zaidi and Shahzaan Mohammed, "Biometric Handwritten Signature Recognition".

[11] Albawi, T. A. Mohammed, and S. Al-Zawi, "Understanding of a Convolutional Neural Network,", *2017 International Conference on Engineering and Technology (ICET)*, pp. 1–6, 2017.

[12] S. Sadak, N. Kahraman, and U. Uludag, "Handwritten signature verification system using sound as a feature," in Proceedings of the 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), pp. 365–368, Milan, Italy, July 2020.

[13] V. Bonde, P. Narwade, and R. Sawant, "Offline signature verification using a convolutional neural network," in Proceedings of the 2020 6th International Conference on Signal Processing and Communication (ICSC), pp. 119–127, Noida, India, March 2020.

[14] H. A. B. Nehal and M. Heba, "Signature identification and verification systems: a comparative study on the online and offline techniques," Future Computing and Informatics Journal, vol. 5, no. 1, 2020.

[15] A Comparative Study among Handwritten Signature Verification Methods Using Machine Learning Techniques Zainab Hashim, Hanaa M. Ahmed, and Ahmed Hussein Alkhayyat, 2022.

[16] Kancharla, K., Kamble, V., and Kapoor, M.: Handwritten signature recognition: a convolutional neural network approach. In: 2018 International Conference on Advanced Computation and Telecommunication (ICACAT), pp. 1–5. IEEE (2018).

[17] Jadhav, T.: Handwritten signature verification using local binary pattern features and KNN. Int. Res. J. Eng. Technol. (IRJET) **6**(4), 579–586 (2019).

[18] Sam, S.M., Kamardin, K., Sjarif, N.N.A., and Mohamed, N.: Offline signature verification using deep learning convolutional neural network (CNN) architectures GoogLeNet inception-v1 and inception-v3. Procedia Computer Science, **161**, 475–483 (2019).

[19] Yapici, M.M., Tekerek, A., and Topaloglu, N.: Convolutional neural network-based offline signature verification application. In: 2018 International Congress on Big Data, Deep Learning, and Fighting Cyber Terrorism (IBIGDELFT), pp. 30–34. IEEE (2018).

[20] Mohapatra, R.K., Shaswat, K., and Kedia, S.: Offline handwritten signature verification using CNN inspired by Inception V1 architecture. In: 2019 Fifth International Conference on Image Information Processing (ICIIP), pp. 263–267. IEEE (2019)

[21] Sudharshan, D.P., and Vismaya, R.N.: Handwritten signature verification system using deep learning. In: 2022 IEEE International Conference on Data Science and Information Systems (ICDSIS), pp. 1–5. IEEE (2022)

[22] Tamrakar, P., and Badholia, A.: Handwritten signature verification technology using deep learning—a review. In: 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 813–817. IEEE (2022)

[23] Mosher, Q.S., and Hasan, M.: Offline handwritten signature recognition using a deep convolutional neural network. Eur. J. Eng. Technol. Res. **7**(4), 44–77 (2022).