

Signature Verification using CNN

Hrishikesh Mhaske¹, Rushikesh Bhalerao², Sanket Walke³, Vaibhav Gholap³, Prof. Puja Lingampalli⁵

Students, Department of Computer Engineering^{1,2,3,4}

Assistant Professor, Department of Computer Engineering⁵

Rajiv Gandhi College of Engineering, Karjule Haryana, India

Abstract: *One of the most popular verification biometrics is the signature. The usage of handwritten signatures in cheques, applications, letters, forms, minutes, etc. A person's handwritten signature must be individually identified because each individual's signature is unique by nature. Verifying signatures is a popular utilised technique for verifying someone while they are away. Human verification can be inaccurate and occasionally unsure. The most common method for confirming a person or a private is with a signature. A person's signature is used to identify them in all social, professional, and commercial contexts. The word "signature verification" is extremely important because it could be misused and lead to significant losses. The signature may be a behavioural biometric trait that combines the signer's neuromotor characteristics (e.g., how our brain and muscles, among other things, shape how we tend to sign) as well as sociocultural influences (e.g., the differences between Western and Asian styles). Through the ages, United Nations agency experts have constructed signature examinations to verify the validity of sample-supported rhetorical analysis.*

Keywords: CNN (Convolutional Neural Network), Signature Verification, Support Vector Machine, Biometric Analysis,

I. INTRODUCTION

We intended to develop the deep learning technology to recognise the human handwriting in a way that would also be simple for someone with less technical experience to utilise. The suggested technique is designed to determine whether a human handwritten signature is real or fake. A greater variety of photos, including examples of both real and fake signatures, are gathered as samples. For each class of photographs that were categorised as input images, a different amount of images were collected. To stop hostile individuals from using fake signatures, we suggested a Deep Learning (DL) based offline signature verification solution. The Convolutional Neural Network (CNN) is the Deep Learning (DL) technique employed in the study. If more feature extraction techniques are added to assist the CNN method and the human hand signature is correctly classified, it is projected that the success of the results will grow. The method for verifying human signatures uses a deep learning algorithm, which has numerous "layers" of neural network algorithms. As signatures pass through each layer, a condensed version of the data is presented to the following layer. The majority of machine learning techniques are effective when applied to datasets of up to a few hundred features. The quantity of features in an unstructured dataset like a picture, however, makes this approach difficult or impossible. As the deep learning algorithm traverses each layer of the neural network, it gradually gains more knowledge about the image of the signatures. The final output layer contains the results of the signature, which are then shown on the screen as either a real or fake signature.

II. LITERATURE SURVEY

The area of Handwritten Signature Verification has been broad lyre search edin the last decades and still remains as an open research problem. This project focuses on offline signature verification, characterized by the usage of static(scanned)images of signatures, where the objective is to discriminate if a given signature is genuine.

1. Biometric Signature Verification System

The phrase "biometric signature verification system based on freeman chain code and k-nearest neighbour" [1], Three issues were found during the analysis of the problem's historical context in StageThe first one is relevant to the SVS as a whole. Some solutions to this issue are defined since signatures are a sort of biometric that can alter with mood

environment, and age. A decent signature database needs to be updated at certain intervals in order to remain current and useful. In addition, one must sign consistently in order to create a string of signatures that are very similar to one another. The second issue is with the FCC generation, which was unable to extract from the damaged portions of the signature. the greatest contiguous portion of the signature is picked in order to reveal the FCC. The third issue had to do with verification in order to have a decent outcome. To get the desired results using k-NN, earlier steps, particularly pre-processing and feature extraction, must function effectively.

2. Multiple Neural Classifiers

The phrase "Signature verification using multiple neural classifiers" [2] - On Sun's Spark System, a prototype recognition system was developed using C. Ten separate people's samples were obtained for the experiment. Each person provided fifteen authentic signature samples, which were then collected. In addition, 100 random forgeries were utilised to evaluate the system. A series of trials were run to gauge the approach's effectiveness. In every experiment, five randomly chosen samples of each person's actual signature were used to train the classification nets. These nets had the same number of output nodes as there were participants in the experiment.

3. Two-Stage Neural Network Classifier

"A new neural network classifier-based two-stage neural network signature verification technique" [3] - This research suggests a fresh method for off-line signature verification and identification. The complete system is built on a two-stage neural network classifier with one class per network and 160 features divided into three subsets. Only small, fixed-size neural networks need to be trained during the first stage's training procedure, but the training method for the second stage is simple. The majority of our design work went towards incorporating the majority of the intelligence into the system's structure. There was no feature reduction method employed, and the guiding principle for choosing which features to include and which to exclude was to "use all features." and let the neural networks decide which ones are significant and which ones are not"

4. Signature Image Generation

"Synthetic off-line signature image generation" [5] In this work, a brand-new mechanism for creating static, offline signatures of new identities is proposed. In particular, the random variables of a statistical distribution of the features of the global signature are used to create the signature of the new synthetic identity. The outcomes closely resemble actual signature forms and characteristics of writing styles that are inferred from static signature databases. With the introduction of a natural variability from the synthetic individual attributes, new instances and forgeries of the synthetic identities are obtained. An ink deposition model based on a ballpoint is created for the creation of realistic static signature images as an added novelty. The static signature generator's range has been established to match the performance of two public databases as well as that of synthetic databases.

5. Static Signature Synthesis

"Static signature synthesis: A biometrics method inspired by neuromotor behaviour" [6], We provide a novel technique in this research for creating fake handwritten signature images for biometric applications. The methods we present mimic the motor equivalence mechanism, which splits human handwriting into two stages: the formulation of an effector independent action plan and its execution via the associated neuromuscular pathway. On a spatial grid, the activity plan is shown as a trajectory. This includes the signature text as well as its flourish, if any. Applying a kinematic Kaiser filter on the trajectory plan simulates the neuromuscular path. The pen speed, which is produced using a scalar version of the sigma lognormal model, determines the length of the filter. A deposit of ink Using a model to simulate the pen trajectory pixel by pixel, realistic static signature images are produced. The range of the synthesis parameters as well as the lexical and morphological characteristics of the synthesised signatures have been determined using real signature databases like the GPDS960 and MCYT Off-line Grey Signature corpuses. The results of the performance experiments demonstrate that it is possible to generate synthetic identities with varying levels of stability and skilled forgers. As a result, datasets of artificial signatures can be produced that perform similarly to databases of actual signatures. Additionally, depending on the demands of the researcher, we can modify the generated dataset to

produce sophisticated forgeries or straightforward forgeries that are simpler to spot. The average level of confusion between actual and artificial signatures according to perceptual evaluation is 44.06%, demonstrating the artificial signatures' realism. By examining how the type of pen and user count affect an automatic signature validator, the usefulness of the synthesised signatures is illustrated.

6. Modules

Add the specified image to the dataset and CNN training manual Utilising the keras preprocessing image data generator tool, we must input our data set and construct size, rescale, range, zoom range, and horizontal flip. Then, using the data generator tool, we import our image dataset from the folder. Fig.



FIG1. PHASES OF HUMAN SIGNATURE VERIFICATION

In addition to setting the target size, batch size, and class-mode from this function, we also set the train, test, and validation parameters here. the module will be trained using AlexNet We create training steps for each epoch, total epochs, An image is inputted into a convolutional neural network (ConvNet/CNN), a deep learning algorithm, which assign emphasis (learnable weights and biases) to distinct aspects in the image of the signature and be able to distinguish between different signatures.

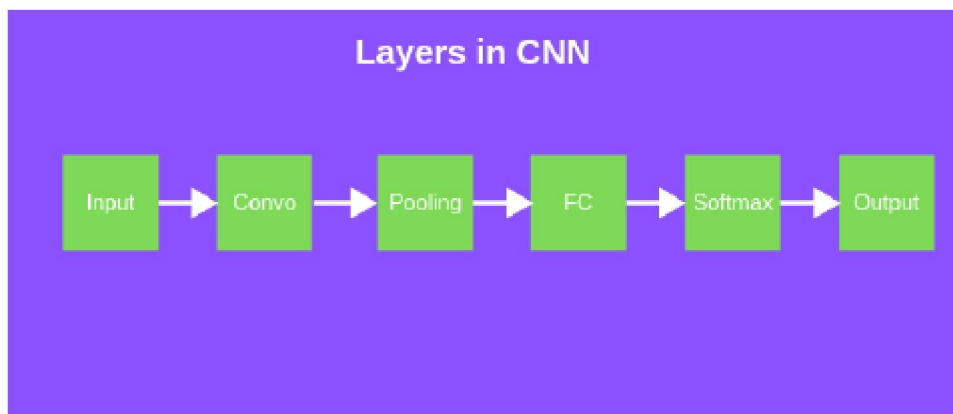


Fig. 2. Layers in Convolution Neural Network

Using the Django framework to deploy the model and forecast the outcome The trained deep learning model is transformed into a hierarchical data format file in this module, which is then used by our django framework to improve the user experience and forecast if a particular signature is genuine or fake.

III. IMPLEMENTATION AND RESULT ANALYSIS

3.1 Data Acquisition

To develop a knowledge base for each and every person, handwritten signatures are gathered, and some of the signatures' distinctive characteristics are retrieved. For assessing the effectiveness of the signature verification system and contrasting the outcomes achieved using the other techniques on the same database, a standard database of each person's authentic and forged signatures is required.

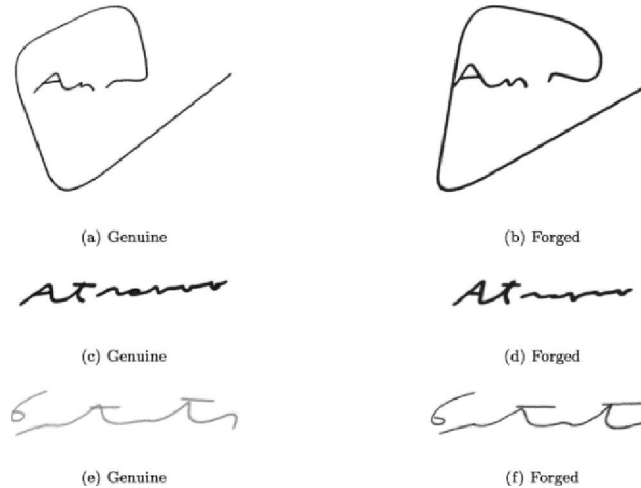


Fig. 3. Genuine and Forged Signatures

3.2 Pre-Processing

The scans of each signature are done in grey. This stage's goal is to standardise and prepare the signature for feature extraction. The pre-processing procedure enhances the signatures' quality and makes them better suited for feature extraction. A grayscale signature image is included in the preprocessing stage and converted to binary to facilitate feature extraction. The signatures received by signature are obtained in various sizes, thus resizing is done to make them standard size, which will make the signatures to standard size 256*256.

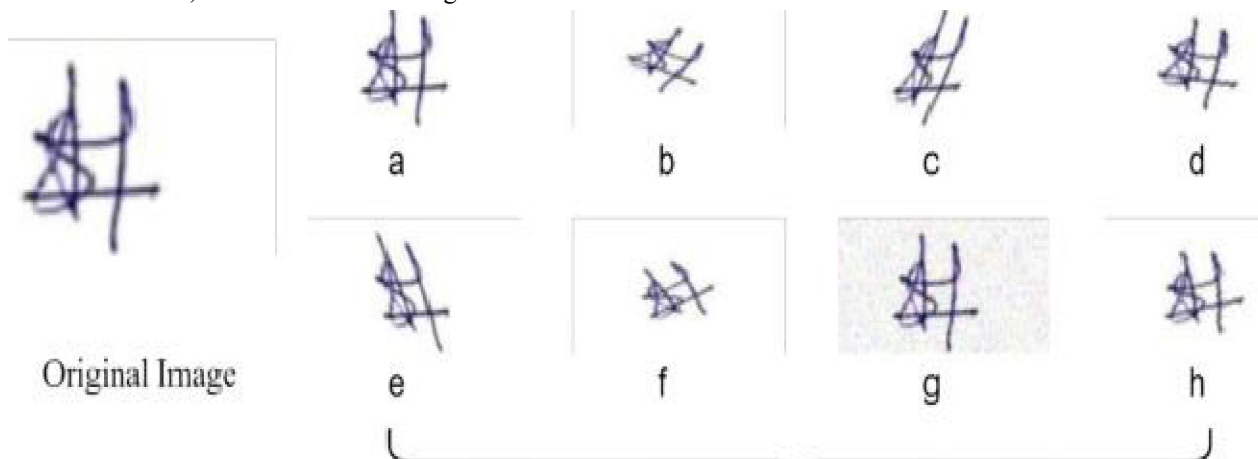


Fig. 4. Pre-Processing of Signatures

3.3 Classification

Every picture in the signature goes through a sequence of alternating convolution and max pooling layers. A predetermined number of feature maps are generated after each image in the signature has undergone the convolution process. These feature maps are then fed into the max pooling layer, which then generates pooled feature maps using the feature maps acquired from the convolution layer put before it. The following convolution layer receives this pooled feature map, and so on until the fourth maximum pooling layer is reached. The last max pooling layer's pooled feature

map is received, flattened, and delivered into the fully linked layers. The model will be finalised after multiple iterations of forward and backward propagation. After the model has been trained, it will be possible to forecast whether a signature is genuine or fake.

3.4 Overall Result

The database containing the signatures is tested after training the CNN models on the images of the signatures, and the outcome indicates whether the matching signature is real or fake.



Fig. 5. Sample output generated

IV. CONCLUSION AND FUTURE WORK

Embedded devices can use Convolutional Neural Networks, a very powerful and effective technique. The effectiveness of the algorithm can be confirmed using the aforementioned tests. All of these tests yield very comparable results. The training of signature datasets obtained from multiple perspectives is a crucial parameter to take into account, according to algorithm testing. The public will be helped in using their signatures in the safest and most effective way possible with the help of this intelligent human signature verification technology.

The project's future development will involve integrating online apps with artificial intelligence to use the human hand signature verification technique.

V. ACKNOWLEDGMENT

The heading of the Acknowledgment section and the References section must not be numbered. Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template

REFERENCES

- [1]. Bharadi, V. A. & Singh, V. I. (2014), 'Hybrid Wavelets based Feature Vector Generation from Multidimensional Data set for On-line Handwritten Signature Recognition', 5th International Conference-Conuence The Next Generation Information Technology Summit (Conuence pp.561-568).
- [2]. Chang, H., Dai, D., Wang, P. & Xu, Y. (2012), 'Online Signature Verification Using Wavelet Transform of Feature Function Architecture of an Online Signature Verification System', 11(2011), 3135-3142.
- [3]. Fernandes, J. & Bhandarkar, N. (n.d.), 'Enhanced online signature verification system', International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), Volume 3, Issue 6, November-December 2014, pp.205-209, ISSN 2278-6856.
- [4]. Fierrez-aguilar, J., Krawczyk, S., Ortega-garcia, J. & Jain, A. K. (2005), 'Fusion of Local and Regional Approaches for On-Line Signature Verification', Iwbrs 2005 LNCS 3781, 188-196.
- [5]. Hafemann, L. G., Sabourin, R. & Oliveira, L. S. (2017), 'Learning features for online handwritten signature verification using deep convolutional neural networks', Pattern Recognition 70, 163-176.

- [6]. Iranmanesh, V., Ahmad, S. M. S., Adnan, W. A. W., Yussof, S., Arigbabu, O. A. & Malallah, F. L. (2014), 'Online Handwritten Signature Verification Using Neural Network Classifier Based on Principal Component Analysis', *The Scientific World Journal* 2014, 1-9.
- [7]. Jain, A. K., Ross, A. A. & Nandakumar, K. (2011), Introduction, in 'Introduction to Biometrics', Springer, pp. 1-49.
- [8]. Kaur, M. R. & Choudhary, M. P. (2015), 'Handwritten Signature Verification Based on Surf Features Using HMM', 3(1), 187-195.
- [9]. Khalil, M., Moustafa, M. & Abbas, H. (2009), 'Enhanced DTW based on-line signature verification', *Image Processing (ICIP), 2009 16th IEEE International Conference on* pp. 2713-2716.
- [10]. Liu, Y., Yang, Z. & Yang, L. (2015), 'Online signature verification based on dictionary sparse representation', *IEEE Transactions on Cybernetics* 45(11), 2498-2511.
- [11]. Nagbhidkar, K. P. & Bagdi, P. V. (2015), 'Online Signature Verification on smartphone using discrete wavelet transforms', 2(2), 1-6.
- [12]. Nanni, L., Maiorana, E., Lumini, A. & Campisi, P. (2010), 'Combining local, regional and global matchers for a template protected on-line signature verification system', *Expert Systems With Applications* 37(5), 3676-3684.
- [13]. URL: <http://dx.doi.org/10.1016/j.eswa.2009.10.023>
- [14]. Parodi, M. & Gomez, J. C. (2014), 'Legendre polynomials based feature extraction for online signature verification. Consistency analysis of feature combinations', *Pattern Recognition* 47(1), 128-140.
- [15]. URL: <http://dx.doi.org/10.1016/j.patcog.2013.06.026>
- [16]. Plamondon, R., Pirlo, G. & Impedovo, D. (2014), Online signature verification, in 'Handbook of Document Image Processing and Recognition', Springer, pp. 917-947.
- [17]. Plotz, T. & Fink, G. a. (2009), 'Markov models for offline handwriting recognition: A survey', *International Journal on Document Analysis and Recognition* 12, 269-298.
- [18]. Rua, E. A. & Castro, J. L. A. (2012), 'Online signature verification based on generative models', *IEEE Trans. Syst., Man, Cybern. B, Cybern* 42(4), 1231-1242.
- [19]. Saffar, M. H., Fayyaz, M., Sabokrou, M. & Fathy, M. (2018), 'Online signature verification using deep representation: A new descriptor', *arXiv preprint arXiv:1806.09986*.
- [20]. Sharma, A. & Sundaram, S. (2016), 'An enhanced contextual dtw based system for online signature verification using vector quantization', *Pattern Recognition Letters* 84, 22-28.
- [21]. Thumwarin, P., Pernwong, J. & Matsuura, T. (2013), 'FIR signature verification system characterizing dynamics of handwriting features'.
- [22]. URL: <http://asp.urasipjournals.com/content/2013/1/183>