International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

Signature Verification through Convolutional Neural network

Riya Patil, Snehal Solat, Shailaja Shriramula, Radha Lokhande, Prof. Vaishali Anaspure

Information technology, Dhole Patil College of Engineering Pune.

***Abstract*- Ever since dawn of time, the practice of documentation verification has been crucially significant. Throughout centuries, emblems and other official markings have indeed been employed, but a signature having emerged being one of the most potent and well recognized means of verification, even currently. Distinctive signatures are one of the most valuable biometric traits and among the most often used kinds of documentation or transactional verification. Manual validation are some of the most time-consuming and inefficient methods of verification. As a result, an accurate and effective strategy has been described in this article to optimize the process that allows for quicker and more precise validation. The devised approach utilizes Convolutional Neural Networks to attain the signature verification after rigorous training using the leading signature datasets. The approach has been evaluated for its errors through in-depth assessment using experimentations that resulted in an acceptable performance.**

Keywords— *Signature Verification techniques, Convolution Neural Network, Decision Making, Image resizing, open CV.*

I. INTRODUCTION

A sign is commonly regarded as among the most legally binding kinds of verification used by banks and other financial entities. Because signatures include certain features that are behavior driven and dependent on the biomechanics of the individual client, they are regarded for the purpose of validation. A durable and incredibly effective verification technique is made possible by the low cost of construction and nearly universal adoption. Designations, titles, legal qualifications, and other kinds of individual identity that are closest to the individual can be used to create signatures.

Signatures are a type of control verification that may be used to authenticate a range of items, including checks, legal records, and correspondence. The signatures must therefore be examined to see if they are genuine and produced by the individual's own writing, or they're a fake performed by someone with malicious intentions. The erroneous attestation of a sign might be troublesome since it can allow another unlawful entity to have accessibility to somebody else's assets. In today's society, where authenticity is the foundation, biometric identification is a critical responsibility.

Biometric identification technology is often employed to safeguard a wide range of initiatives. The idea is to identify personal characteristics related to anatomical or psychological character traits. The first part, recognition, is based on bodily characteristics like fingerprints, faces, eyes, signs, and so on. Written signatures, on the other side, are acknowledged as perhaps the most popular and cheapest biometric authentication approach relying on morphological classification for a wide range of technologies, including organization documents, formal contracts, and banking transactions.

It is indeed a misconception to believe that a people's genuine signatures would indeed be unrecognizable if signed numerous occasions. Signatures need synchronization of the movements, neurotransmitters, eyesight, forearms, and fingers with the mind. The user's surroundings, fitness, mental capacity, disposition, and emotional reactivity at the moment of signing are all factors that influence the signature. Certain constituents may not appear the same in each signature as a consequence of various variables at play. The level of knowledge and precision required to fabricate a signature makes authentication far more difficult and important. Rather than signing fluently, the forger's primary goal is to create an accurate reproduction of the original signature.

As a result, manually verifying signatures is a time-consuming and error-prone process. There has been a significant increase in the number of forgeries, which are becoming increasingly complex. An appropriate and automated process must be implemented to minimize such instances and undertake correct authenticity assessment. For this purpose, this research paper defines an effective and useful methodology for the purpose of signature verification

The Literature Survey of chapter 2 of this research paper examines previous work. Section 3 delves into the approach in depth, while section 4 focuses on the outcomes evaluation. Finally, Section 5 brings this report to a close and gives some hints for future research.

II. LITERATURE SURVEY

Ping Wei [1] explains that signature verification is a difficult undertaking that necessitates the proper use of a variety of approaches. The researchers recommend a new inverse discriminative infrastructure for writer-independent written by hand signature verification that comprises of 4 weight-shared streams: multiple

discriminative channels that retrieve signature convolutional characteristics and 2 different invertible channels that monitor extraction of features to concentrate on signature moves. The sparse information problem in signature verification is solved using an inverted monitoring process and a multi-path concentration method. Experimental results demonstrate strategy is effective and has a lot of promise.

Eman Alajrami [2] expresses that signature verification and forgery detection is defined as the process of automatically and instantaneously checking signatures to establish whether they are genuine or not. However, almost all of the strategies have been shown to be ineffective owing to an inadequate knowledge. This paper has successfully constructed a model that can understand from signatures and draw conclusions about whether the signature in consideration is a fraud or not. This type can be utilized in a variety of government agencies that require handwritten signatures for authorization or validation. Although CNNs are used to acquire the signatures in this technique, the topology of the fully connected layer is indeed not ideal. This implementation may be considered extreme.

Mustafa S. Kadhm [3] states that this paper proposes a mechanism for verifying signatures that is quick, accurate, and trustworthy. The verification efficiency of the model was quite good. Additionally, the recommended extraction of features strategy that focuses on HSC used preprocessing techniques that allowed the algorithm to reach improved prediction performance. Furthermore, using three major different signature image databases, the proposed ANN design enhances the research findings with the minimum degree of precision. According to the authors of this paper, CNNs might be employed well in real-time authentication process for extraction of features using the weighted Softmax activation function, which has now been effectively employed in many identifiability issues in future.

Nehal Hamdy al-Banhawy [4] narrates a summary of commonly used preprocessing approaches, feature extraction techniques, and methodology for online and physical handwritten signature identification and verification systems was shown. An analysis of proposed systems used during recent research for identity verification, detection techniques, extraction of features, and offline and online technologies is also offered, along with a presentation of the dataset being used and results for each approach. Basis of the results of the assessment, it was concluded that using the SURF, SIFT, and summation of directed gradients approaches in combination with computational adjustment for extraction of features produced improved outcome.

Neha Sharma [5] introduces that many operations require offline signature verification, therefore a solution that could also identify authentic signatures against fraudulent signatures is required. In this research, the authors looked into a variety of signature verification demands, types, and approaches or models that may be utilized for this objective. The researchers' work over the preceding 3 decades were also mentioned by the writers. To achieve this goal, a variety of methodologies have been utilized, including architecture and machine learning. Because of their capacity to learn from original data or visuals, deep learning-based techniques have lately came to prominence.

Tushara D [6] states that signatures are needed to validate personal identify in all monetary operations, but that signature verification mechanisms still rely on painstakingly comparing signatures to approved signatures. As a consequence, a computer-based classification scheme is essential. An online signature verification method relying on neural network segmentation is proposed in this paper. The given system pulls a collection of coordinates and velocity information at multiple locations from the database server, through which a distinct specialized feature set is produced.

Deniz Engin [7] have published a comprehensive study on writer-independent offline verification and identification in a real-world environment, wherein the bank customers' obfuscated autographs are compared to their cleansed referenced signatures. To clean signatures before passing these to a CNN architecture to recover signature interpretations, the researchers introduced a stamp elimination approach that is based on Cycle GAN. Various verification parameters, fine-tuning techniques, and signature presentation approaches were also analyzed and studied by the authors. A qualitative evaluation was also conducted to show the situation's problems.

Prarthana Parmar [8] describes that signature is a behavioral biometric that is being used to validate individual identify, according to the definition. Because handwriting is an instinctive behavior and precise pen movements are consistent and cannot be readily manipulated when counterfeiting is undertaken, handwritten signatures are perhaps the most often used biometric feature. After analyzing all of the approaches for all of the processes to find offline signatures in this scientific report, this methodology was picked. Because this technique has been the most latest to be investigated, it offers a bigger prospective possibility for advancement. There have been breakthroughs in the effectiveness of detecting signature similarities and offering improved aid in evaluating whether a signature is authentic or fraudulent.

B. M. Rankin [9] created a technique for determining the probability of detection of particular artefacts and making sensor choosing judgments using automated spectroscopic signature assessment. The process is based

on characteristic distribution in a spectra that has been shown to be applicable to a wide range of primary objective, including passive VNIR and LWIR spectroscopy. Additionally, the quantifiable result of the technique is frequently linked to object implementation and monitoring.

Hsin-Hsiung Kao [10] present an automated human signature verification approach rely on a specific reference standard and a deep CNN structure. The researchers use a variety of methodologies to improve the validity of the experimental tests, which include background de-noising and preprocessing, the creation of controlled groups for different survey sizes and network infrastructure, through the use of visualization techniques providing prototype interpretability. The findings of the experiments reveal that automatic signature authentication can be done with just one reference standard.

Aravinda C.V [11] have incorporated statistics on publicly released offline handwritten signature databases along with knowledge on the databases used in these studies by the researchers. The authors also detailed the measures they undertook to establish a massive collection of handwritten documents signatures. The recently founded dataset is enormous, particularly when compared to any other public information dataset. The author planned to make this new dataset publicly available on their university's website so individuals could use it for research.

C. S. Vorugunti [12] discusses the proposed OSV technique for coping with data scarcity in online signature verification. To create synthetic signature examples, the scientists used Generative Adversial Networks, wherein a generator network trains to create fake samples depending on discriminator output. Ultimately, the study found that GANs can do complex tasks such as online signature authentication in a sentient way. The algorithm has better classification accuracy when discriminating between real and fake data. The researchers evaluated the proposed model and found that it generated the best outcomes when compared to previous state-of-the-art algorithms.

S. Soisang [13] explains a novel image features based on local binary patterns that combines Gradient Quantization Angle (GQA) also with Local Binary Patterns (LBP). LBGQAP stands for Local Binary Gradient Quantization Angle Patterns, which is a new textural features approach. Furthermore, the researchers used ANN classifications to overcome the difficulty of verifying offline handwritten signatures. The empirical research was conducted using CEDAR databases. The results showed that LBGQAP outperforms other program as part of training and testing sets uniformity. Moreover, the LBGQAP has greater F-Measure, Recall, and Precision scores than that of the LBP.

III SYSTEM ARCHITECTURE

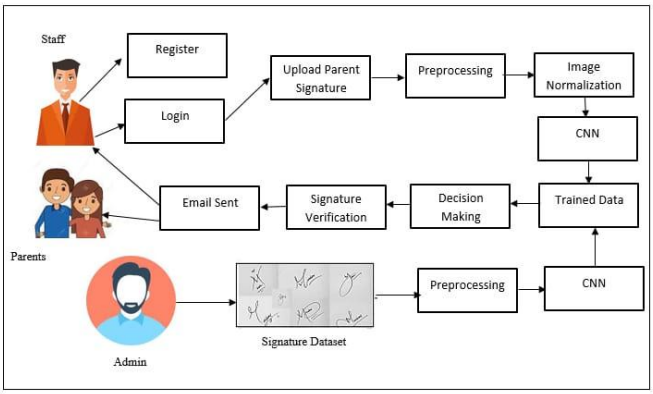

Figure 1: System Overview Diagram

The above picture 1 depicts the proposed technique for verification of signatures. The steps that are involved in the process are explained in depth as below.

Step 1: Data collection and Preprocessing – A well classified signature dataset is downloaded from the URL : https://www.kaggle.com/datasets/divyanshrai/handwritten-signatures. This dataset contains many images with the signatures for the both forged and real types. These signature images are classified in numbered directories with the real and forged names. Once these signatures are classified then they are set to resize based on the folder hierarchy using the python programming language. Here the directories are recursively traversed to obtain their respective paths. The images in the obtained path are resized using the CV2 object of Open CV for the dimension of 150 X 150. The resized image objects are converted into Grayscale for the proper training purpose. After resizing and gray scaling, the images are again stored in the same path to prepare proper dataset to train using the Convolution neural network.

Step 2: Training through convolution neural network: To train the signature dataset train and test paths are set initially. Then the total numbers of 238 Train and test images are used for the 16 batch numbers and 500 Epochs. An image Data generator object is created with the depth ratio of 1:255 to create train and test data objects. This ratio is set to analyze the pixels to its extreme depth with the mentioned ratio.

Required parameters are loaded into the train and test data objects for the size 150 X 150, batch size 16 for color mode gray scale. The last parameter is loaded as class mode with categorical value.

A sequential neural network model for the convolution neural network is created as a model for the gray scale color channel mentioned as 1 for dimension of 150 X 150 images. Then model is added with the 32

kernels with size 3 X 3 for the first layer. Followed by this for the second layer another convolutional layer is added with 64 kernels with size 3X3 . The first and second both the layers are powered with " Relu" Activation Function. In the next step the model is added with a one maxpooling 2D layer with the kernel size 2 X2 to collect the neurons in 2D matrix. This max pooling 2D layer is ended with a Dense layer with 25 %.

Third layer is added with 128 kernels with size 3 X 3 with " Relu" Activation function along with a max pooling 2D layer with kernel size 2X2. The same is applies to the fourth layer to end with a dropout percentage of 25 with a Dropout layer.

After this entire neural network is flatten to collect the neurons with a Dense layer of size 1024 and with a dropout percentage of 50%. Finally the trained data are collected for the 24 classes of signature with activation function " Softmax". The losses are estimated while training the data through categorical cross entropy with an optimizer called' Adam". Then in the end the model is invoked using the fit_genrator function for 500 epochs to obtain the trained data in an .h5 file. The Architecture of convolution neural network is depicted in the below figure 2.

Layer	Activation
CONV 2D 32 X 3 X 3	Relu
CONV 2D 64 X 3 X 3	Relu
MaxPooling2D 2 X 2	
Dropout 0.25	
CONV 2D 128 X 3 X 3	Relu
MaxPooling2D 2 X 2	
CONV 2D 128 X 3 X 3	Relu
MaxPooling2D 2 X 2	
Dropout 0.25	
Flatten	
Dense 1024	Relu
Dropout 0.25	
Dense 24	Softmax
Adam Optimizer	

Figure 2: Convolution Neural network architecture

Step 3: Testing through Decision Making - Here in this step a signature is verified using the earlier trained model data that was stored in .h5 file along with the current model. The prediction produces an integer value that eventually indicates the matched Signature name from the dictionary. This Information is enough to take the decision for the real and forged signatures for the given input.

IV. RESULTS AND DISCUSSIONS

The presented approach for Signature Verification is implemented on a Windows Operating System based laptop and is coded in python programming language. The methodology is coded using the Python programming language utilizing the Spyder Integrated Development Environment. And for the Deployment as the application proposed method uses the Swing framework of Java through Netbeans IDE . The implementation Laptop consists of a standard configuration such as an Intel Core i5 Processor along with 8 GB of RAM and 1 TB of Hard Drive Storage.

The in-depth evaluation of the presented technique for signature verification must be accomplished to determine the deployment accuracy of the Convolutional Neural Networks. This is due to the fact that the CNN approach is central to the entire approach and has a great influence on the entire methodology. Therefore, it is paramount that the CNN approach is deployed with minimum error. Thus, the error attained is measured through the use of the RMSE or Root Mean Square Error in the section given below.

Performance Evaluation through Root Mean Square Error

The error achieved in the proposed approach has been determined through the use of the RMSE approach. The RMSE technique has been one of the most effective and useful methodologies that investigates the error attained by the verification process of the presented approach. The error measurement is performed between the expected signature verifications and the achieved signature verifications. The RMSE is mathematically depicted using the equation 1 below.

$$\mathrm{RMSE}_{fo} = [\sum_{i=1}^{N} (z_{f_i} - z_{o_i})^2 / N]^{1/2}$$

Where

$\sum$ - Summation.

$(Z_{fi} - Z_{oi})^2$ - Differences Squared for the signature verifications.

N - Number of Images.

For initiating the RMSE evaluation the MSE or the Mean Square Error needs to be evaluated. The MSE calculation is performed for the error achieved between the actual signature verifications and the achieved signature verifications. The values for these verifications are extracted through the use of extensive trials that are performed with varying amount of input. The outcomes of executing these trials have been recorded in the table 1 given below.

Trial No.	No. of Expected Signature Verifications	No. of Achieved Signature Verifications	MSE
1	6	5	1
2	7	7	0
3	9	9	0
4	10	10	0
5	11	10	1
		RMSE	0.632

Table 1: Mean Square Error Measurement

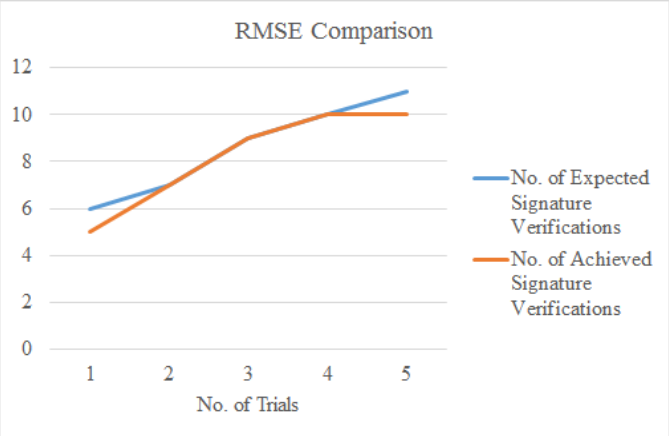

Figure 3: No of Expected Verifications V/s No of Obtained Verifications

The results recorded in the table 1 above are being used for the purpose of achieving the graph depicted in the figure 2 above. The graph depicts the error achieved by the proposed approach for the purpose of attaining the signature verifications through the use of the Convolutional Neural Networks. The outcomes of the experimentation indicate a very low error rate that is indicative of the proper deployment of the CNN component of the methodology. The MSE achieved initially is extracted and the square root is performed on its value to get the RMSE. The attained RMSE value of is highly satisfactory and a suitable result for a first time implementation of such a system for signature verification.

V CONCLUSION AND FUTURE SCOPE

Signatures are the integral identity of every individual, so to protect them a strong mechanism is required by the many sectors like banking, academics and other business sector. The deep learning models are considered as the one of the best solution for this, Hence, this research is concentrated on the implementation of convolution neural network for the verification of the real time signatures.This research weaved in the sense of verifying the signatures of the parents of the students of an academic institution. Before this process signatures of the parents are trained using the Convolution neural network. While testing the signature the college admin upload the signatures of the parents on the document to verify it as real or forged. If the signatures are forged then a precautionary Email will be send to parents regarding this through gmail host. The proposed model is also evaluated using the RMSE , which yields a value of 0.632 . The value of RMSE indicates the better performance of the system in the first trail only.

For the future research purpose this model can be enhanced to work as the readymade API and also as the web services to provide services to different sectors.

REFERENCES

[1] P. Wei, H. Li and P. Hu, "Inverse Discriminative Networks for Handwritten Signature Verification," 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019, pp. 5757-5765, doi: 10.1109/CVPR.2019.00591.

[2] M. Barhoom, Alaa & Abu-Naser, Samy & Alajrami, Eman & Abu-Nasser, Bassem & Musleh, Musleh & Khalil, Ahmed. (2019). Handwritten Signature Verification using Deep Learning, 2019.

[3] Mohammed, Mamoun & Kadhm, Mustafa & Ayad, Hayder. (2021). an accurate signature verification system based on proposed HSC approach and ANN architecture. Indonesian Journal of Electrical Engineering and Computer Science. 21. 215-223. 10.11591/ijeecs.v21.i1.pp215-223.

[4] Nehal Hamdy Al-banhawy, Heba Mohsen, Neveen Ghali2, "Signature Identification and Verification Systems: A Comparative Study on the Online and Offline Techniques", Future Computing and Informatics Journal, 2020.

[5] Neha Sharma et al, "A Comprehensive Study on Offline Signature Verification", 2021 J. Phys.: Conf. Ser., 2021.

[6] Tushara D, Shridevi Raddy, Shreya K M, Spoorthy Y, 2021, Signature Verification System using Neural Networks, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCCDS – 2021.

[7] Engin, Deniz & Kantarcı, Alperen & Arslan, Secil & Ekenel, Hazım. (2020). "Offline Signature Verification on Real-World Documents", 2020.

[8] P. Parmar et al, "A Survey of Handwritten Signature Verification System Methodologies", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN: 2349-5162, Vol.6, Issue 5, page no.1-6, May – 2019.

[9] B. M. Rankin, T. P. Lippa and J. B. Broadwater, "Spectral Information Content Algorithm for Automated Signature Assessment," IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium, 2020, pp. 1790-1792, doi: 10.1109/IGARSS39084.2020.9323899.

[10] Kao, Hsin-Hsiung & Wen, Che-Yen. (2020). "An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach. Applied Sciences." 10. 3716. 10.3390/app10113716.

[11] A. C.V, L. Meng and U. K. R. K.R, "An approach for signature recognition using contours based technique," 2019 International Conference on Advanced Mechatronic Systems (ICAMechS), 2019, pp. 46-51, doi: 10.1109/ICAMechS.2019.8861516.

[12] C. S. Vorugunti, P. Mukherjee and V. Pulabaigari, "Online Signature Profiling using Generative Adversarial Networks," 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), 2020, pp. 894-896, doi: 10.1109/COMSNETS48256.2020.9027369.

[13] S. Soisang and S. Poomrittigul, "New Textural Features for Handwritten Signature Image Verification," 2021 7th International Conference on Engineering, Applied Sciences and Technology (ICEAST), 2021, pp. 20-24, doi: 10.1109/ICEAST52143.2021.9426314.