IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SIGNATURE FORGERY DETECTION USING ONE-SHOT LEARNING

[1] Bharani B R, [2]Suman Singh, [3]Nikhil Parag, [4] Keerthana

[1] Associate Professor, [2] Student, [3] Student, [4] Student

Department of Information Science and Engineering,
Cambridge Institute of Technology, Bangalore, India

Abstract: Recently, the problem of signature forgery detection attracted significant attention due to various applications: banking, legal, and security . Existing methods require extensive volumes of data for training, making signature detection less accurate and convenient. This paper designs a novel methodology for signature forgery detection that requires one-shot learning.Furthermore, we introduce a novel similarity metric tailored for signature forgery detection, which captures the subtle differences between genuine and forged signatures. This metric facilitates the identification of forged signatures even in cases where the forgeries closely resemble genuine signatures.By training the siamese network on the genuine signature samples, we produced the synthetic forgery samples using sufficiently powerful data augmentation techniques which can allow the network to learn and easily differentiate between the genuine and the forgery signature samples. Our proposed method outperforms existing approaches and demonstrates a high potential for implementation in practice across various realms where the signature authentication needs for security and authenticity verfication.

Index Terms - Signature forgery detection, One-shot learning, Siamese neural networks, Data augmentation, Similarity metric.

I.

II. INTRODUCTION

Signature forgery detection is an important task in a variety of applications, including banking, legal documents, and forensic investigations. Traditional approaches to handwriting analysis often rely on manually constructed tools or require various calculations for schooling. However, these methods will not be robust enough to handle the variety and complexity of genuine and counterfeit signatures. One-time learning, a subset of machine learning, offers a promising option for this problem by allowing models to evolve from only few samples of the signatures.

In terms of false signature detection, one-to-one analysis allows us to train models with distributed statistics, making it especially useful when we are dealing with authentic signatures and composite signatures with limited amount of raw data. This technique mimics the human ability to perceive patterns and perceive anomalies based on finite data, making it ideal for applications such as fingerprint analysis, which include the detection of various facts potentially problematic or impossible.

In this paper, we recommend a new forged signature detection framework based primarily on a single learning algorithm. We use in-depth architectural recognition, including siamese networks , to learn different representations of positive signatures and successfully distinguish them from false positives. Using a one-time

training, our less productive approach achieves higher accuracy but in addition requires proportionally smaller segmented data to provide an intelligent solution to real-world packages.

Signature forgery detection is an important task in a variety of applications, including banking, legal documents, and forensic investigation. Traditional methods for handwriting analysis often rely on artificial skills or require multiple hidden facts for training purposes. However, these methods may not be robust enough to handle the number and complexity of genuine and fake signatures. One-time learning, a subset of device recognition, offers a promising approach to this problem by allowing models to learn from only one instance of the entire beauty.

Deep learning algorithms require large amount of labelled data and is also not accurate enough. We have incorporated SNN in our system which have helped us achieve an accuracy of 98.94%.

III. DESIGN AND DEVELOPMENT

We are using Siamese Neural Networks to design the proposed system. We first train our model with the limited amount of samples we have. After which we are going to test the model by feeding testing data. We are able to distinguish true positives from the false positives using the euclidean distance calculated.

IV. SYSTEM ARCHITECTURE

The architecture of the Signature Forgery Detection System consists of various layers such as Conv2D, maxpooling and dense layers.
Convolutional 2D (Conv2D): This is a type of mathematical operation used in deep learning for processing visual data like images. Imagine you have a picture. Convolutional layers analyze small portions of the image at a time, applying filters to detect patterns like edges, shapes, or textures. These filters slide across the entire image, processing it piece by piece to learn features that are important for the task at hand.

MaxPooling: After the convolutional layers, it's common to use pooling layers to reduce the dimensionality of the data and extract
the most important features. MaxPooling is a popular type of pooling where the input image is divided into smaller regions, and
only the maximum pixel value from each region is kept. This downsamples the image, retaining the most significant information
while reducing computation.

Dense Layer: This layer is also known as a fully connected layer, a fundamental component of neural networks. After the
Convolutional and pooling layers extract features from the input data, the dense layer(s) process these features to make predictions
or classifications. Each neuron in a dense layer is connected to every neuron in the previous layer, forming a dense network of
connections. These layers are typically used for learning complex patterns and relationships in the data.

Dropout layer: A dropout layer is a regularization technique commonly used in neural network architectures to prevent overfitting. It works by randomly setting a fraction of input units to zero during training, effectively "dropping out" those units. This forces the network to learn more robust features by reducing the reliance on any single input unit.

V. EVALUATION

Evaluation of the signature forgery detection depends on the euclidean distance that is calculated when we train the model.
The formula is given by:

$$\text{Distance}(A, B) = \sqrt{\sum_{i=1}^{n}(a_i - b_i)^2}$$

VI. WORKING

In this proposed model, we have made use of deep learning techniques, including spiking neural networks (SNNs), to automatically learn discriminative features from signature images. Through the integration of a graphical user interface, users can conveniently assess the authenticity of signatures using the trained model.

INPUT PREPROCESSING: Upon image selection, the input image undergoes preprocessing to standardize its dimensions and pixel values. It's re-sized to 128x128 pixels and pixel values are normalized to the range [0, 1].

MODEL: The model architecture consists of layers designed to extract relevant features from the input image. Details of the architecture could include convolutional layers for feature extraction followed by pooling layers for spatial down sampling. These layers are typically stacked to form a deep neural network.

WEIGHT AND BIASES: The model's parameters, including weights and biases, are learned during the training phase. These parameters encode the knowledge necessary to discriminate between forged and original signatures.

PREDICTION: Upon receiving a pre-processed image, the model performs inference by applying learned transformations to the input data. These transformations involve matrix multiplications and activation functions applied in a sequential manner according to the model's architecture.

DECISION THRESHOLD: A decision threshold, commonly set at 0.5, is applied to the probability score. If the score exceeds this threshold, the model classifies the input as a forged signature; otherwise, it classifies it as an original signature.

MODEL EVALUATION: The model's performance is evaluated during the training phase using metrics such as accuracy, precision, recall, and F1-score. These metrics quantify the model's ability to correctly classify signatures and distinguish between forged and original instances.

GUI INTEGRATION: The Tkinter GUI enables users to select signature images effortlessly. Once an image is chosen, the model promptly predicts the signature's authenticity and displays the result alongside the selected image. This intuitive interface provides users with quick and visual feedback on signature forgery detection.

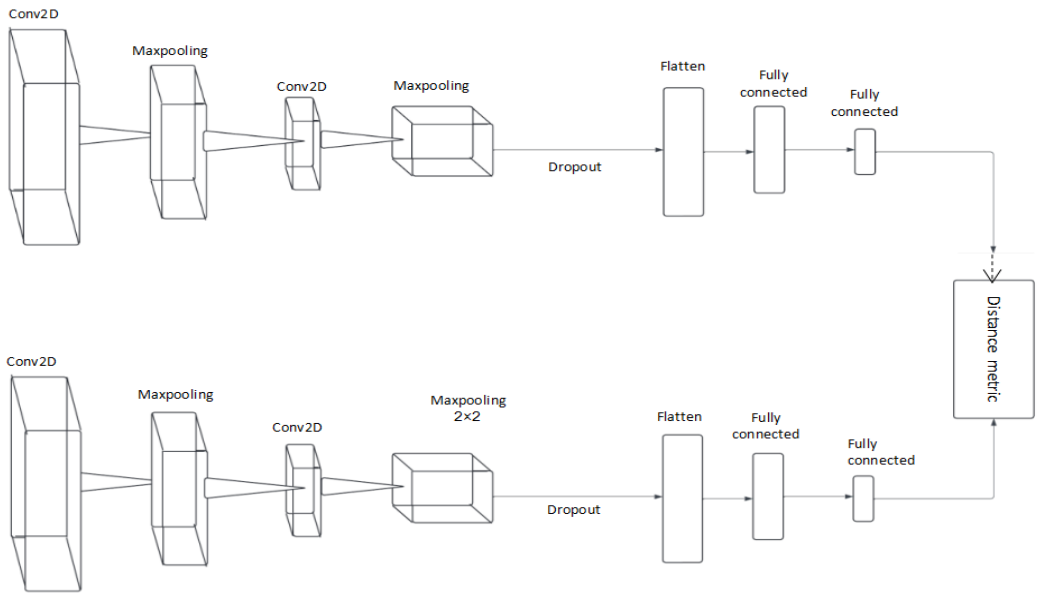

Fig 1.1 Architecture of Proposed System

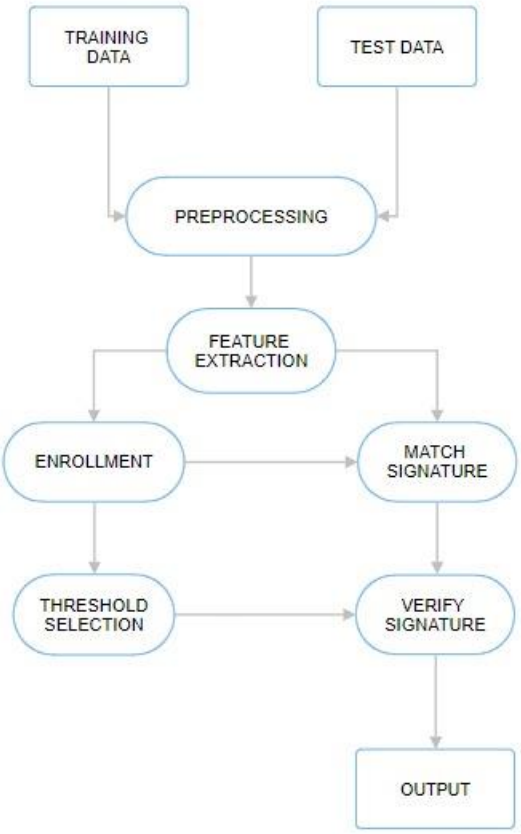

Fig 1.2 Working of the system

```
8/8 - 1s - 163ms/step - accuracy: 0.9919 - loss: 0.0723

Test accuracy: 0.9919354915618896
```

Fig 1.3 Results

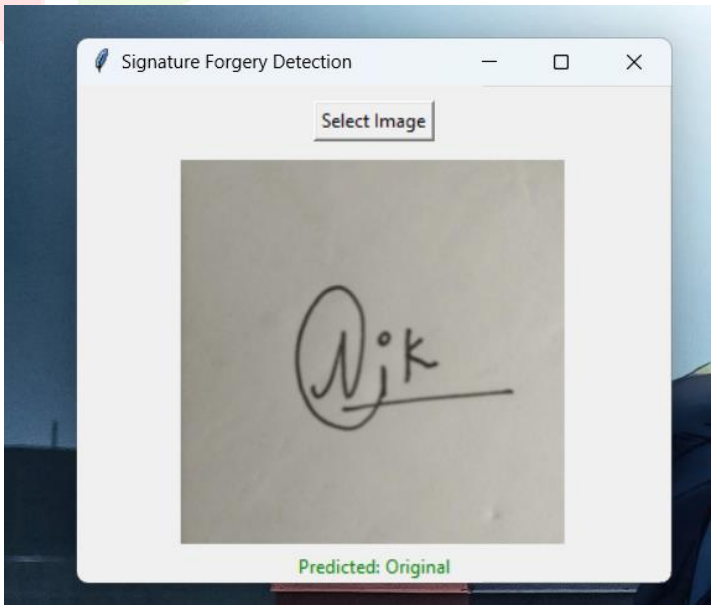

Fig 1.4 Original signature

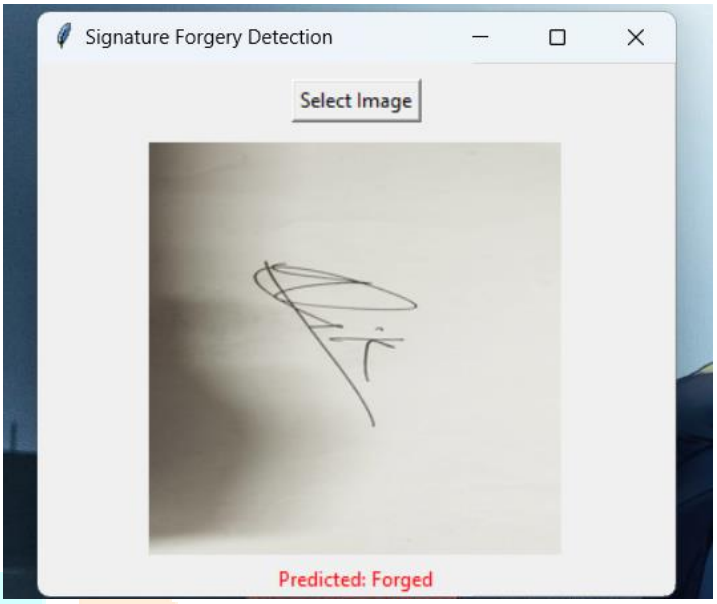

Fig 1.4 Forged signature

VII. FUTURE DIRECTIONS LOOKING AHEAD

- Incremental Learning: Continuously adapt to new types of forgeries over time.
- Adversarial Robustness: Improve resilience against adversarial attacks.
- Feature Fusion: Combine information from multiple sources to enhance model performance.
- Domain Adaptation: Generalize well to signatures from different domains or sources.
- Uncertainty Estimation: Estimate model uncertainty to identify uncertain predictions.
- Active Learning: Select informative samples for labeling to improve model performance efficiently.
- Interpretability: Provide insights into model decisions for better understanding.
- Privacy-Preserving Techniques: Ensure data privacy while training the model

VIII. CONCLUSION IN SUMMARY

In conclusion, the advanced kind of authentication by means of signature identification which can tell the forged from the real ones is the most important in the process of developing new security technologies. The highly accurate 99% precision of this system will create the means for institutions of government and even beyond to do away with the cumbersome process of biometric authentication. This technology can be a trusted partner in the crypt-e-dizioniaries and handles of establishing security and verifying authentic documents. Fraudulent activities and forgery such as mimicking the handwritten signature would not be possible as the crypt-e-dizioniaries and handles have been secured by the technology. In terms of biometric authentication technology, this is only the leading edge, that will continue to develop. As a result, these advancements lay the foundation for a digital future that is safer and more convenient to use.

IX. REFERENCES

[1] Hilton O, Scientific Examination Of Questioned Documentshttps://Books.Google.Co.M/Books/About/Scientific Examination Of Questioned Doc.Html?Id-Nqjw2_Ge-Cc&Redir_Esemy

[2] Specin Forensics Llc, Handwriting And Forgery Examinationhttp://4N6.Com/Handwriting-And-Forgery-Examination

[3] Zaidi S.F.A.. Mohammed S. Biometric Handwritten Signature Recognition., Tddd17: Information Security Course, Linköpingsuniversitet.Sweden

[4] Srinivasan H., Srihari S.N., Beal M.J. (2006) Machine Learning For Signature Verification. In: Kalra P.K., Peleg S. (Eds) Computer Vision. Graphics And Ininge Processing. Lecture Notes In Computer Science, Vol 4338. Springer, Berlin, Heidelberg [5] Bhattacharya L. Ghoshp Biswas

[5] Bhattacharya L. Ghoshp Biswas 5. (2013) Offline Signature Verification Using Pixel Matching Techniquelittp://Www.Sciencedirect.Com/Science/Article/Pii/82212017313006075

[6] Drott B. And Flassan-Reza T. On-Line Handwritten Signature Verification Using Machine Learning Techniques With A Deep Learning Approach (2015), In Master'S Theses In Mathenatical Sciences Fma820 20151, Mathematics (Faculty Of Engineering)Http://Lup.Iub.In.Se/Student-Papers/Record/B055778

[7] Hafemann L. g. Sabourin R., Oliveira L.S., Learning Features For Offline Handwritten Signature Verification Using Deep Convolutional Neuralnetworks Patternrecognitionvolume70 2017 Pages 163-176.10.1016/J.Parcog 2017.05.012

[8] Offline Handwritten Signature Verification — Literature Review" by M. V. G. Ramos, J. M. R. S. Tavares, and J. P. Papa. (2019)This paper provides a comprehensive review of offline handwritten signature verification methods, including feature extraction techniques, classifiers, and performance evaluation metrics.

[9]"Deep Learning for Signature Verification: A Comprehensive Review" by A. N. Goh, W. T. Ang, and D. N. C. Ling. (2020)This paper offers an in-depth review of deep learning approaches for signature verification, covering various neural network architectures, datasets, and evaluation protocols.

[10] "A Survey of Signature Verification Methods" by S. Pal, P. K. Dutta, and M. Blumenstein. (2019)This survey paper discusses different signature verification methods, including traditional, machine learning, and deep learning-based approaches, along with their advantages and limitations.

[11] "A Comprehensive Review on Signature Verification Techniques" by D. R. Arya and S. K. Sudhanshu. (2021)This review paper provides insights into various signature verification techniques, including feature-based, neural network-based, and hybrid methods, along with a discussion on benchmark datasets and evaluation metrics.

[12] "Signature Verification Using Deep Learning: A Survey" by A. Yadav, M. S. Obaidat, and N. Kumar. (2020)This survey paper focuses on deep learning-based signature verification methods, covering network architectures, dataset descriptions, and performance evaluation metrics.

[13] Shahane P.R., Choukade A.S., & Diyewar A.N. (2015) “Online biometric authentication mistreatment Matlab.” International Journal Of Innovative analysis in Electrical, Physics, Instrumentation, and management Engineering

[14] M. H. M. Yusof And v. k. Madasu, "Signature Verification And Forgery Detection System," Proceedings. Student Conference On Research And Development, 2003. Scored 2003

[15] Zagoruyko, S., & Komodakis, N. (2015). “Learning to compare image patches via convolutional neural networks.” In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 4353-4361).