IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11496

SIGNATURE FORGERY DETECTION USING TENSORFLOW AND VGG16

Priyanka J[1], Sahana S R[2], Shreya V N[3], Sukanya V N[4], Rajath A N[5]

UG student Department of Computer Science and Engineering,

GSSS Institute of Engineering and Technology for Women, Mysuru, VTU, Belagavi, India[1,2,3,4]

Assistant Professor, Department of Computer Science and Engineering,

GSSS Institute of Engineering and Technology for Women, Mysuru, VTU, Belagavi, India[5]

Abstract: Signatures play a vital role in various sectors such as banking, finance, and commerce, serving as unique identifiers for individuals. Nonetheless, they present challenges as even slight similarities between two signatures authored by the same person can exist. To tackle this issue and prevent identity fraud in banks and other organizations, forgery detection systems employ machine learning algorithms and concepts like VGG16. These systems utilize structural parameters and local variations within signatures to accurately match them against a database. Implementing such software ensures secure validation across numerous platforms including loan applications, legal document signings, and other relevant processes.

I. INTRODUCTION

The significance of signature verification is paramount as signatures, unlike passwords, are unique to individuals and cannot be altered or forgotten. They serve as crucial means of authentication. Techniques for signature verification are categorized into offline and online methods. Offline verification involves minimal hardware usage with images captured by a camera, while online verification employs more hardware connected directly to computers. Features used in offline verification are simpler, involving preprocessing and feature extraction from a signature database. Automatic offline signature verification solutions fall into handcrafted feature extraction algorithms and deep learning methods, with the latter being highly regarded due to their prowess in image recognition. Despite the recent focus on deep learning with small-scale data, many methods still require a substantial number of samples for training. Our paper proposes an offline handwritten signature verification method utilizing convolutional neural network (VGG16). Signature forgery detection finds applications in net banking, passport verification, credit card transactions, and bank checks, necessitating the development of automatic signature systems to protect individual identities.

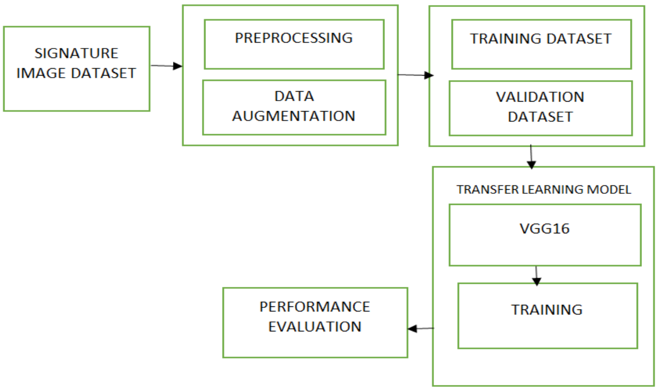


Fig. 1 : Architecture

The process begins with input images of signatures, which are pre-processed to enhance clarity and standardize dimensions. These pre-processed images are then fed into the VGG16 network, where multiple layers of convolutional and pooling operations extract hierarchical features. The resulting feature vectors are then passed through fully connected layers, facilitating classification into genuine or forged signatures. Fine-tuning of VGG16 may also be employed to adapt the network to the specific characteristics of signature data. Through extensive training on labelled datasets, the model learns to discern subtle differences between authentic and forged signatures, thus enabling accurate detection of fraudulent attempts.

II. ALGORITHM

- **TensorFlow**

TensorFlow stands out as an open-source platform for crafting end-to-end Machine Learning applications. Functioning as a symbolic math library, it utilizes dataflow and differentiable programming to execute diverse tasks, particularly centered around training and inference of deep neural networks. This versatile framework empowers developers to construct machine learning applications through an array of tools, libraries, and community resources. Notably, TensorFlow, spearheaded by Google, reigns as the foremost deep learning library globally. Google extensively integrates machine learning across its products, enhancing search engine capabilities, translation services, image captioning, and recommendations, exemplifying Tensor Flow’s widespread utility and impact.

- **VGG16**

The VGG16 convolutional neural network, renowned for its 16-layer depth, excels in visual tasks with high accuracy. It simplifies hyper parameters, using 3x3 filters in convolutional layers and 2x2 max-pooling layers with strides of 1 and 2, respectively. Trained on a dataset of over a million images, VGG16 captures diverse features. With an input size of 224x224, it normalizes gradients for smooth ascent, adeptly managing gradients of varying magnitudes. This approach ensures robust performance in tasks such as image classification, making VGG16 widely favoured model architecture in the field of computer vision.

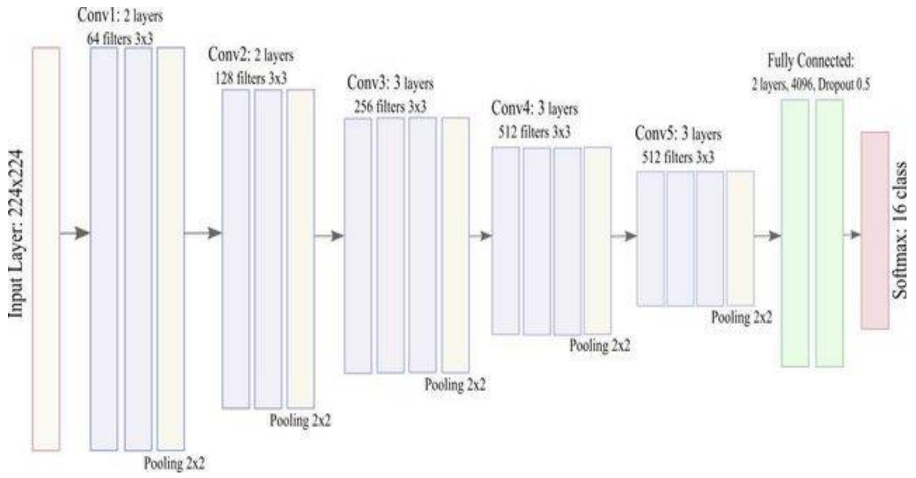


Fig. 2: Visual Geometry Group

III. EXISTING SYSTEM

Currently, signature verification predominantly relies on manual processes, wherein authorized personnel visually inspect signatures for authenticity in banks and other sectors. While some systems integrate machine learning algorithms like support vector machines (SVM) for classification, their accuracy is hindered by the extensive pre-processing required.

These algorithms necessitate meticulous data preparation, including feature extraction and normalization, which can be cumbersome and error-prone. Consequently, the reliance on human judgment persists due to the perceived limitations of automated systems. However, advancements in deep learning offer promising avenues for enhancing accuracy and efficiency in signature verification by mitigating the need for intricate pre-processing and leveraging the power of neural networks to discern subtle patterns within signatures.

DOI: 10.17148/IARJSET.2024.11496

IV. PROPOSED SYSTEM

In the realm of signature forgery detection, the adoption of deep learning algorithms, particularly leveraging frameworks like TensorFlow and architectures such as VGG16, presents notable advantages. These algorithms streamline the preprocessing phase by enabling direct input of raw signature images into the model, circumventing the need for extensive feature engineering or data normalization. This not only simplifies the overall pipeline but also minimizes potential information loss during preprocessing, ensuring crucial forgery detection details are retained. Moreover, the VGG16 architecture's depth and capability to capture intricate features play a pivotal role in distinguishing subtle disparities between authentic and counterfeit signatures. Harnessing its hierarchical representations, the model adeptly learns discriminative patterns indicative of forgery, resulting in heightened accuracy compared to conventional machine learning methods. The fusion of TensorFlow's resilience and VGG16's feature extraction prowess empowers the system to effectively identify signature forgeries, rendering it a compelling solution for real-world applications necessitating precise authentication mechanisms.

V. LITERATURE SURVEY

[1] “Signature Verification Using a Siamese Time Delay Neural Network" by Jing Wu And Wenbin Liu et al. (2022)”
The authors proposed a signature verification system that uses a Siamese Time Delay Neural Network (STDNN) to extract features from signatures and perform classification. The system was tested on the MCYT-100 signature dataset and achieved good accuracy.

[2] “A Hybrid Approach for Offline Signature Verification Based on Machine Learning and Handcrafted Features" by Singh and Vatsa (2022)”
The authors proposed a hybrid approach that combines machine learning techniques with handcrafted features for offline signature verification. The system was tested on the SigComp2011 dataset and achieved good accuracy.

[3] “Offline Handwritten Signature Verification: A Survey" by M. Diaz-Cabrera et al. (2021)”.
This survey focuses on offline signature verification techniques, including feature extraction, classification, and performance evaluation. The system was tested on the MCYT-75 signature dataset and achieved an efficient accuracy.

[4] "Handwritten Signature Verification: A Comprehensive Survey" by Awais M. Kamboh et al. (2021)”.
This survey provides a comprehensive overview of various techniques used for signature verification, including offline and online methods, and discusses their advantages and disadvantages.

[5] "A Survey on Multimodal Biometric Authentication Systems: Handwritten Signature Verification" by S. Ahmad and S. Saba (2020)”.
The paper covers different aspects of multimodal biometric systems, including feature extraction techniques, fusion methods, and evaluation metrics. It also reviews different types of modalities used in multimodal biometric systems, such as signature, face, voice, and fingerprint. The authors discuss the strengths and weaknesses of various multimodal biometric systems and provide a comparative analysis of different methods.

VI. PROBLEM STATEMENT

A signature serves as a widely recognized form of writing, employed by individuals to formally endorse documents or express agreement to specific terms, sometimes carrying legal obligations. Financial documents, vital in government, business, and legal realms, encompass bank letters, property deeds, checks, corporate paperwork, currency, and bonds. Historically, individuals have forged signatures for financial gain, evolving methods over time. The proliferation of technology, especially computers, has notably influenced signature practices. With increasing instances of signature forgery, a significant cybercrime, there's a growing imperative to develop deep learning models capable of discerning genuine signatures from forgeries, leveraging pattern recognition to enhance security measures.

VII. METHODOLOGY

- **Dataset loading**

The dataset is downloaded to the machine and loaded into our machine for running in the program for training and testing the data. The dataset is a public dataset which consists of many images of signature data. The signature data consists of

DOI: 10.17148/IARJSET.2024.11496

images which are both fake and original images. Each of the images in the dataset consists of a directory with name fake or forged.

- **Data pre-processing**

The data for the research method is taken from a dataset which consists of a large number of signature images. The images are so large that no two images may be in the same orientation and have similar features. For this purpose, we need to implement preprocessing for the images so that we can treat each image equally which will allow for testing and training to be done efficiently. The pre-processing process includes removing the colours from RGB to grey scale, resizing the image, removal of blurs on the image, etc. according to Douglas J. Kennard (2012). The images will also be cropped and rotated in order to fit in the uniform style. We try to remove the noise from the images binary processing is also carried out in order to convert the image into s binary format.

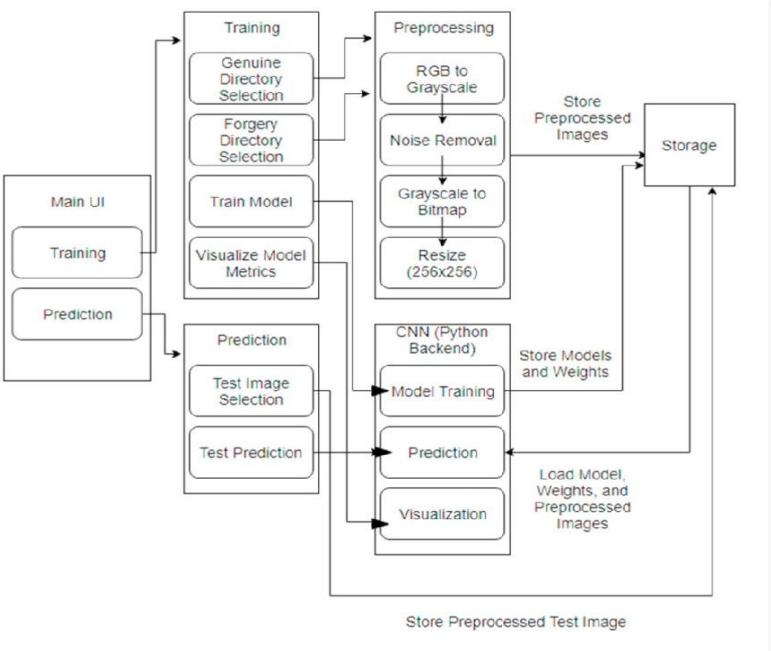


Fig.3: Methodology

- **Dataset splitting**

In this step, we are ready to split the data for training them to the respective algorithms we are going to use. From the training data, we are going to get a smaller set which will be sent to the testing data from which we compare the images and get the output.

- **Define algorithm model**

After finalising the data for splitting we have to define the algorithms which we are going to use in the machine. There are two algorithms which we are going to use here VGG16 or VGG16. Each of the algorithms is not used simultaneously. Firstly, we run a particular algorithm, either VGG16 or VGG16, do the training and testing and find the accuracy of the image which indicates the authenticity of the signature image. Next, we run the second algorithm in the same way and check the output. Thus, the process for both algorithms is the same but is run in different steps.

- **Cross-validation**

After the training and testing, the data are cross-validated in the next process to compare and check for the comparison between the images and to find out which one is fake and which one is original. This result will go through as the final output that will be displayed and thus we get the metrics. Thus the best accuracy giving model will be adopted for the prediction.

DOI: 10.17148/IARJSET.2024.11496

VIII. RESULTS

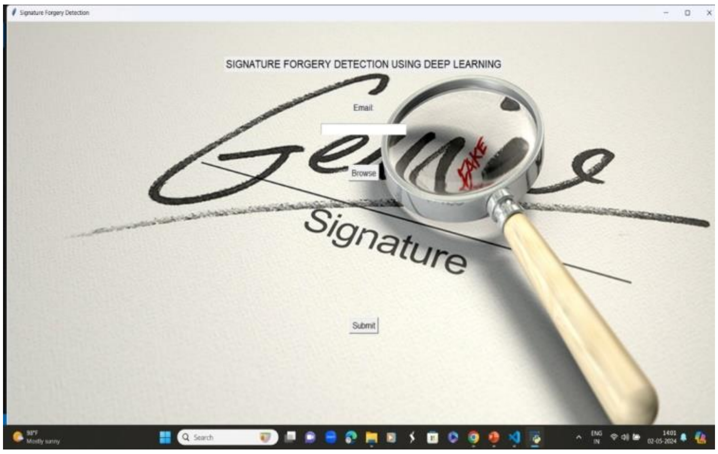

Signature Forgery Detection
SIGNATURE FORGERY DETECTION USING DEEP LEARNING
Email
Browse
Submit

Fig.4: Main Page

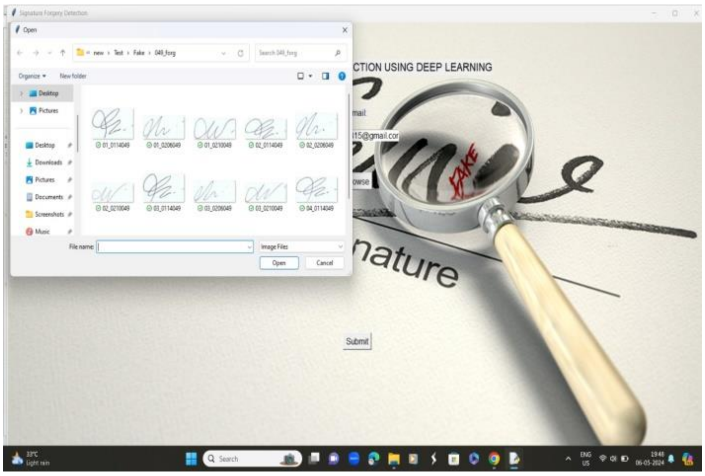
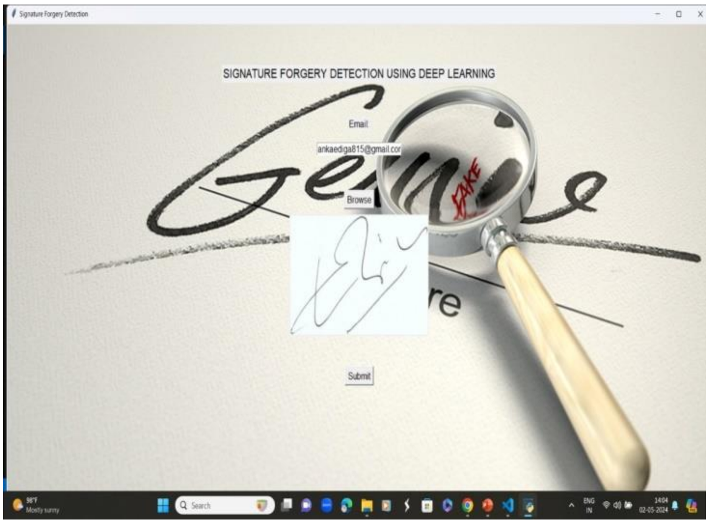


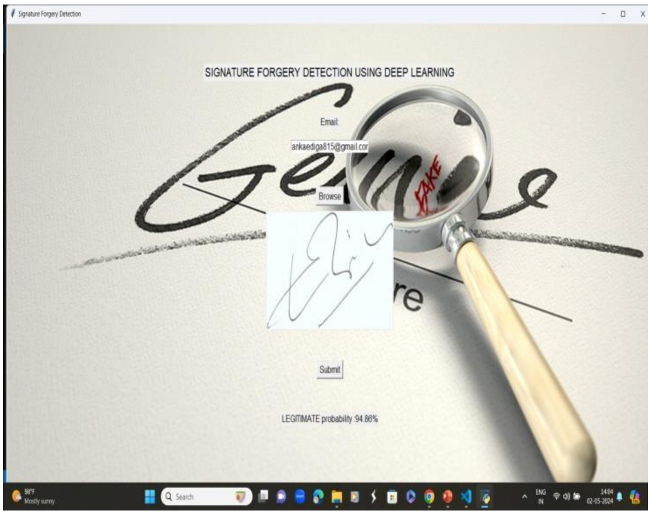
Fig.5: Selecting a Image


Signature Forgery Detection
SIGNATURE FORGERY DETECTION USING DEEP LEARNING
Email
Browse
Submit

ankaedigaa815@gmail.cor

Fig.6: Add Signature

DOI: 10.17148/IARJSET.2024.11496



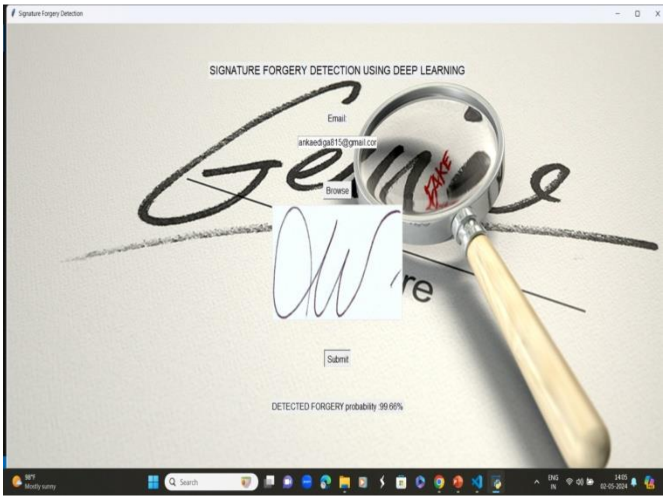
Signature Forgery Detection

SIGNATURE FORGERY DETECTION USING DEEP LEARNING

Email: ankaediga815@gmail.cor

LEGITIMATE probability :94.86%

Fig.7: Signature Detected as Real



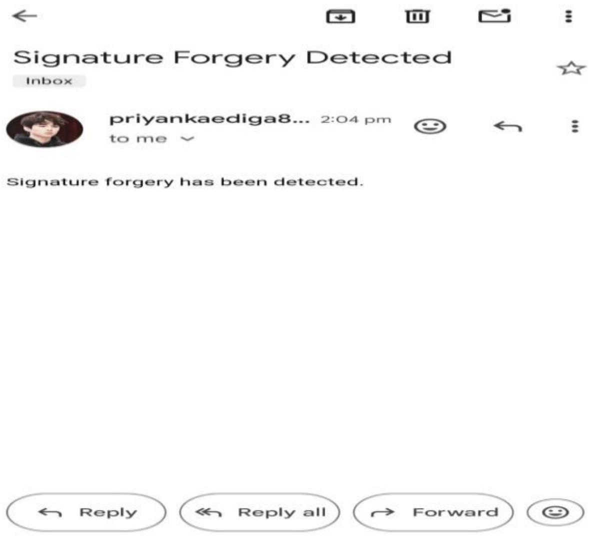
Signature Forgery Detection

SIGNATURE FORGERY DETECTION USING DEEP LEARNING

Email: ankaediga815@gmail.cor

DETECTED FORGERY probability :99.66%

Fig.8: Signature detected as Forged



Signature Forgery Detected

priyankaediga8... 2:04 pm

to me

Signature forgery has been detected.

Fig.9: Email Sent to the Particular Person

DOI: 10.17148/IARJSET.2024.11496

IX. CONCLUSION

Handwritten signatures serve as crucial markers for authentication, but detecting forgeries amidst their inherent variability presents a formidable challenge. As society transitions towards digitalization, the demand for robust verification methods intensifies. Through the integration of Python programming and Convolutional Neural Networks (CNNs) like VGG16, a novel approach emerges to bolster offline signature verification. This method meticulously analyses various signature attributes, including stroke patterns and pressure, enabling the identification of skilled forgeries with enhanced accuracy and efficiency. In contemporary digital landscapes, where remote transactions prevail, robust authentication mechanisms are imperative. This methodology not only fulfils this need but also offers a promising avenue for reinforcing security in legal and social contexts. Leveraging advanced technologies like CNNs empowers the system with sophisticated pattern recognition capabilities, thereby fortifying the integrity of signatures. Consequently, the proposed method signifies a significant advancement in combating fraudulent activities while instilling trust and reliability in authentication processes within an increasingly digitalized world.

REFERENCES

[1]. An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach 2020: Hsin-Hsiung Kao * and Che-Yen Wen.

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

[3]. Offline Signature Recognition and Verification System using Efficient Fuzzy Kohonen Clustering Network (EFKCN) Algorithm 2017: Dewi Suryani, Edy Irwansyah∗, Ricki Chindra.

[4]. Offline signature Verification 2017: Dr. M. Narayana and L. Bhavani Annapurna, K. Mounika.

[5]. 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.

[6]. 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).

[7]. A Study on Preprocessing and Feature Extraction in offline Handwritten Signatures 2015: Sm Abdullah Al-Mamun and Tansin Jahan Daffodil.

[8]. A Survey on Signature Forgery Detection Techniques" by Umapada Pal and Sankar Pal. https://ieeexplore.ieee.org/document/7346548

[9]. Signature Forgery Detection Using Deep Learning: A Comparative Study" by Asim Munawar, Muhammad Imran Malik, and Mudassar Raza: https://www.mdpi.com/2079-9292/9/5/843/htm

[10]. Forgery Detection in Offline Signature Verification Using Image Processing Techniques" by Rajan Kumar Gupta and Ashok Kumar. https://link.springer.com/chapter/10.1007/978-981-15-5254-7_68

[11]. Offline Signature Verification and Forgery Detection using Deep Learning Techniques" by Srinivasa Rao, K. S., and Suryakanth V. Gangashetty. https://ieeexplore.ieee.org/abstract/document/8822722

[12]. Signature forgery detection using deep learning techniques." Expert Systems with Applications. https://www.sciencedirect.com/science/article/pii/S0957417420300835