Signature Forgery Detection System

Madan A S[1], Mahadevakumar DS[2], Kavyashree D G[3]
[1, 2] Dept of computer science
[3]Professor, Dept of computer science
[1, 2, 3] JSS College Arts,Commerce,Science(JSSCACS),Mysore,Karnataka,India

Abstract- *The convenience and speed of electronic transactions have revolutionized document handling and company operations in an increasingly digital age. However, with this age of digital revolution came new difficulties, one of which was the vulnerability to forgeries of signatures. The act of forging someone else's signature without authorization, usually with the aim of misleading or defrauding, is known as signature forgery. Serious repercussions from such fraudulent activity may include monetary losses, court cases, and weakened confidence in document verification procedures.*

For crucial documents like financial contracts, legal agreements, and official government documents to remain authentic and credible, signature forgery detection is crucial.

The manual inspection of signatures for differences has been the traditional method used by forensic professionals or individuals. However, this methodology is time-consuming, error-prone, and arduous. There is a pressing demand for automatic and precise signature forgery detection systems due to the increasing amount of digital documents.

Keywords- Convolutional Neural Network, signature, fraud, prediction, and forging.

I. INTRODUCTION

For security and verification reasons, it is still crucial to guarantee the legitimacy of signatures in the era of digital transactions and communications. This paper presents a novel technique that combines a convolutional neural network (CNN) and the Histogram of Oriented Gradients (HOG) to recognize faked signatures. From signature photos, the HOG descriptor identifies significant elements. It is well-known for its effectiveness in capturing shape and structure inside images. A CNN model that determines if the signatures are authentic or fake uses these features as input. We use grayscale conversion, denoising, and uniform resizing for our preprocessing operations on signature images. The approach attempts to address the inherent heterogeneity found in authentic signatures from the same person through rigorous training and validation procedures, a recognized problem in signature verification.

1.1 Scope: The aim of this project is to develop a robust and efficient system for identifying fake signature photos by applying deep learning methods, specifically Convolutional Neural Networks (CNNs). By automating the signature verification procedure, the suggested method aims to improve document security and enable quick identification of faked signatures.

1.2 Objective: Obtain a large collection of digital signature photos that includes both forged and authentic signatures, then prepare the dataset for testing and training. Create and execute a CNN-based model for detecting signature forgeries, making sure the network design is optimized for precise and effective detection. Validation and Training: The gathered dataset is used to train the convolutional neural network model, which is then cross-validated to ensure performance. Finally, hyper parameters are adjusted for best outcomes. Testing in Real-Time: Use the trained model to detect signature forgeries in real-time, allowing for quick and accurate signature verification across a range of apps. A system's performance can be assessed by utilizing criteria like F1-score, accuracy, precision, and recall. To show how better the suggested integration is, compare it with existing methods.

II. LITERATURE REVIEW

An investigation and evaluation of published sources, including academic books, journals, and other pertinent resources pertaining to a particular field of study, constitute a literature review. The principal aim of this text is to convey to the reader the current state of knowledge and emerging notions pertaining to a specific subject, as well as the benefits and drawbacks that come with it.
Four fundamental goals are included in a literature review.

- Demonstrates familiarity with an array of information and validates the validity of the job.
- It summarizes earlier research while demonstrating how it relates to the current project.
- synthesizes and incorporates existing knowledge about a subject.
- Shows how you have adapted other people's expertise and how your research has sparked fresh ideas.

CONVERTIONAL NEURAL NETWORKS FOR SIGNIFICATION: Examining Benchmark Data

In this research, a thorough investigation into the application of CNNs to signature verification is presented. The authors proved CNNs are better than conventional machine learning methods by conducting experiments on many public signature datasets. They also emphasized the significance of data augmentation and the ways in which various augmentation methods might affect the functionality of the model. All the same, this study was limited to CNNs and did not include feature extraction techniques like HOG.

III. EXISTING SYSTEM

Current signature forgery detection methods frequently rely on basic feature-based approaches or manual eye inspection. Subjective human verification methods have the potential to produce mistakes and cause delays in the detection of forgeries. Feature-based approaches may not be as successful against sophisticated forging tactics and may not be able to capture complicated patterns. Consequently, the accuracy and efficiency required for real-world applications may not be achieved by present technologies to the needed degree.

DISADVANTAGES OF EXISTING SYSTEM:

- Manual forecasting could not be entirely precise.
- Working with datasets that contain a lot of audio data degrades VM's performance, especially when target classes have overlapping traits.
- Data that is noisy and missing is sensitive

IV. PROPOSED SYSTEM

With CNNs' remarkable performance in image processing tasks, the suggested signature image forgery detection system will make use of their power. A variety of digital signature images, including both real and fake signatures, will be used to train the system. The CNN-based model will be able to accurately discern between genuine and fraudulent signatures by picking up complex patterns and features.

Benefits of the Submitted System:

- The height and stroke patterns of the signatures serve as the sole indicators of authenticity or forgery.
- A prediction system outperforms a manual one in accuracy.
- Even with a reduced quantity of data, accuracy can be attained.

VI. SYSTEM ARCHITECTURE DIAGRAM

The "Signature Forgery Detection using Histogram of Oriented Gradients (HOG) and Convolutional Neural Networks (CNN)" system requires multiple stages of design. The requirements determined during the feasibility study are effectively translated into a workable blueprint that developers can adhere to during the design process. This is an in-depth analysis of the design process: Design of System Architecture on a server-side Superior Architecture

The Client Interface serves as the platform for users to add signature photos. It should be web-based and easy to use; it might be developed with the help of frameworks like Angular or React.

• Server-side: CNN-based categorization, feature extraction, and image processing are handled by the backend system. Given Python's abundance of machine learning libraries, this server might be built with Flask or Django.

VI. MODULES

1.Collection of Data:

This study's dataset, which includes 5123 modified photos and 7491 real images, was obtained from CASIA version 2.0.The 224 x 224 pixel size criterion applies to every image in the dataset.

2. Initial Data Processing:

Parts of the dataset are strategically divided, with roughly 50–90% going to training and the remaining portion being set aside for testing. These sets (training and testing) are further divided into two groups: "forged images" and "genuine images."

3. Information Modelling:

One of the most important parts of this research is the training data segments, which serve as inputs for the Convolutional Neural Network (CNN) algorithm.
•The method is evaluated on the test dataset to determine its effectiveness after the training phase.

4. Building the Model:

• After training, if the accuracy rate is high enough, the next step is to create a model file that contains all of the knowledge that was acquired during the hard training process.

•One noteworthy development is the CNN's use of the VGG 16 architectural framework, which incorporates insightful information from the study of compression faults. Using the insights from Error Level Analysis (ELA) results, the main goal of this model is to distinguish between original and modified photos.

VII. IMPLEMENTATION

Python is utilized in the project's implementation as a programming language that is both procedure- and object-oriented. Module templates can be created and instantiated as needed thanks to object-oriented programming, which provides a modular approach by separating data and function memory locations.

The dynamically typed language Python, which has built-in garbage collection, is used to carry out the project's implementation. The procedural, object-oriented, and functional programming paradigms are all supported by Python. Python is well known for being a "batteries included" language and has an extensive standard library. The use of machine learning techniques in this research is noteworthy.

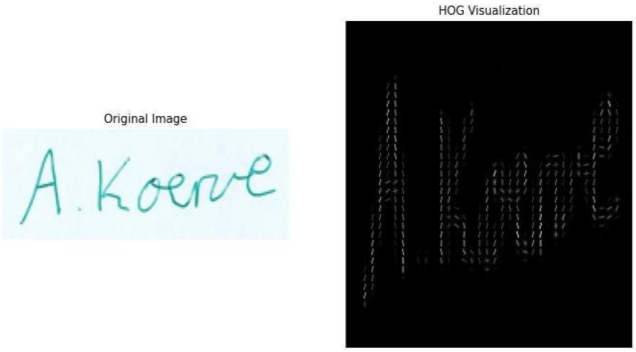
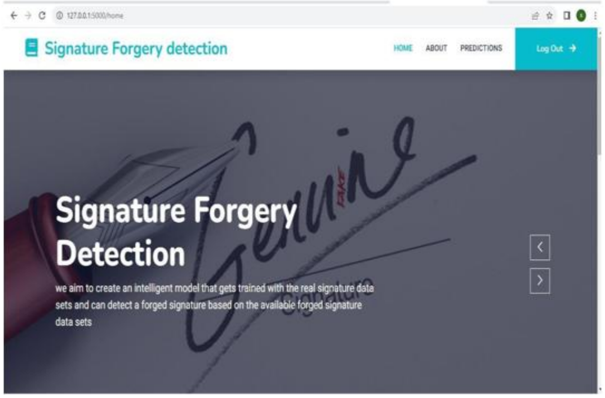


Fig no 7.1 Hog Visualization

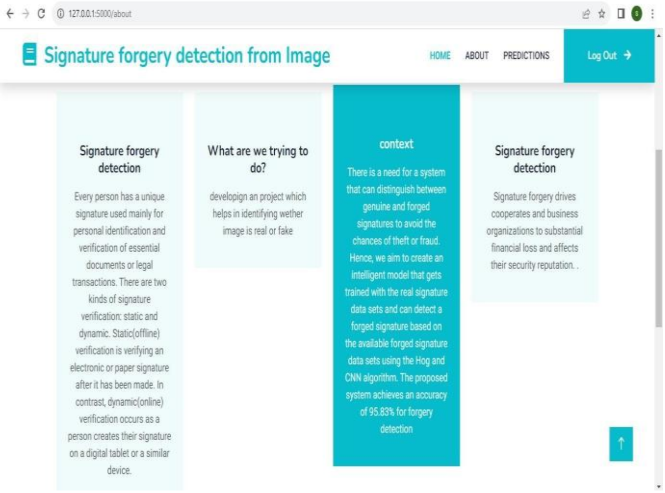


Signature Forgery detection

Signature Forgery Detection

we aim to create an intelligent model that gets trained with the real signature data sets and can detect a forged signature based on the available forged signature data sets

Fig.No 7.2: Screenshot of Home page



Signature forgery detection from Image

Signature forgery detection

Every person has a unique signature used mainly for personal identification and verification of essential documents or legal transactions. There are two kinds of signature verification: static and dynamic. Static(offline) verification is verifying an electronic or paper signature after it has been made. In contrast, dynamic(online) verification occurs as a person creates their signature on a digital tablet or a similar device.

What are we trying to do?

developign an project which helps in identifying wether image is real or fake

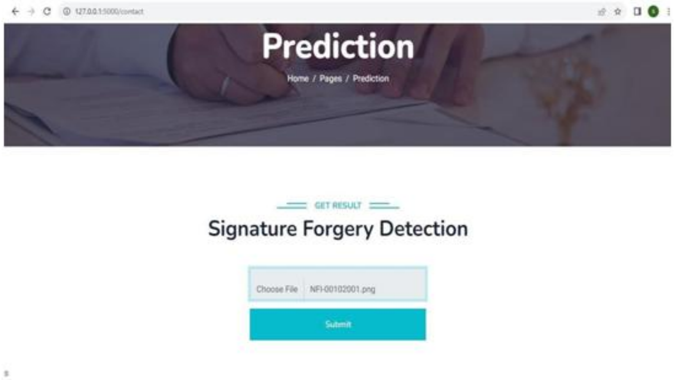
context

There is a need for a system that can distinguish between genuine and forged signatures to avoid the chances of theft or fraud. Hence, we aim to create an intelligent model that gets trained with the real signature data sets and can detect a forged signature based on the available forged signature data sets using the Hog and CNN algorithm. The proposed system achieves an accuracy of 95.83% for forgery detection

Signature forgery detection

Signature forgery drives cooperates and business organizations to substantial financial loss and affects their security reputation. .

Fig.No 7.3: About us page

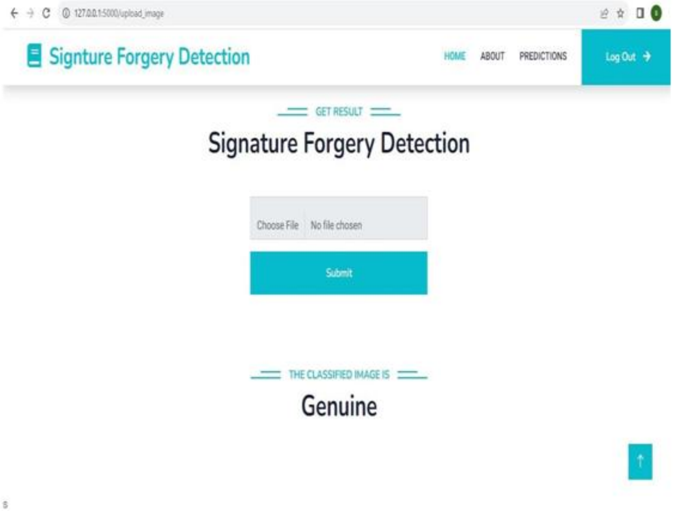


Prediction

Signature Forgery Detection

Choose File NFI-00102001.png

Fig.No 7.4: Screenshot of Prediction page



Signture Forgery Detection

Signature Forgery Detection

Choose File No file chosen

THE CLASSIFIED IMAGE IS

Genuine

Fig.No 7.5: Screenshot of Result page

VIII. CONCLUSION

The application of the Histogram of Oriented Gradients (HOG) technique proved to be beneficial in improving the precision and resilience of our signature forgery detection system. HOG is a crucial technique for extracting features from images and is particularly effective at identifying complex patterns and structures. HOG converts pixel information into a more abstract representation that is useful for identifying edge and texture elements. It is specifically designed to capture gradient orientations and magnitudes within local image regions. We used HOG as a pre-processing step in our signature forgery detection pipeline, which allowed us to fully utilise its potential. More research into adversarial training and resilient designs could improve the resilience of the system, strengthening it against adversarial attacks. The possibility of real-time detection is approaching, which would enable us to expand the capabilities of our system to validate signatures as they are being written.

REFERENCES

[1] Bhahadure, K., Kumar, R., and Tripathi, G. (2020). Deep learning-based detection of signature forgeries. The 4th International Conference on Electronics and Informatics (ICOEI), 2020, pages 160–164.

[2] Singh, A., Srivastava, P. K., & Mishra, S. (2020). Deep learning-based detection of signature forgeries. 665–669 in 2020's Sixth International Conference on Advanced Computing and Communication Systems (ICACCS).

[3] Lee, W. S., Yau, W. Y., and Gan, C. (2017). CNN properties are used to detect signature forgeries. 4502-4506, 2017 IEEE International Conference on Image Processing (ICIP).
LeCun, Y., Hinton, G., and Bengio, Y. (2015). profound understanding. 521(7553), 436-444; Nature.

[4] Szegedy, C., Reed, S., Anguelov, D., Liu, W., Jia, Y., Sermanet, P., & Rabinovich, A. (2015). Expanding on convolutions. IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Proceedings, 1–9.