iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** X **Month of publication:** October 2024

DOI: https://doi.org/10.22214/ijraset.2024.64585

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue X Oct 2024- Available at www.ijraset.com

Advanced Algorithms for Offline Signature Recognition and Enhanced Forgery Detection Mechanisms

Vishwanath V K[1], Prashanthini B M[2]
[1]*Assistant Professor, Department of CS&E, BIET, Davangere*
[2]*Assistant Professor, Department of BCA, BIHE, Davangere*

Abstract: ***In contemporary society, signatures hold significant importance in various critical documents such as bank cheques, passports, and driver's licenses. Unfortunately, they can be counterfeited through various means, giving rise to issues like fraudulent identifications, identity theft, and cyber-attacks. To mitigate this problem, our project is centered around the development of a system that discerns the authenticity of a signature, distinguishing between genuine and forged signatures within a dataset. We have employed Convolutional Neural Networks (CNN) and deep learning for this purpose. This choice is driven by the understanding that signatures evolve over time due to a range of behavioral factors like age, mental state, and physical well-being. Consequently, our system is designed to adapt and learn from diverse training datasets, enhancing its accuracy in detection. While online and offline signature verification methods exist, our project primarily focuses on the latter, specifically targeting the detectionof forged offline signatures.***

Keywords: Signature Recognition, Forgery Detection, Image Processing, Signature Variability, Fraud Detection System, Computer Vision, Pattern Recognition, Authentication Technology

I. INTRODUCTION

In an era defined by an ever-increasing reliance on digital communication and transactions, the threat of signature forgery remains a significant and urgent issue. Signature forgery involves the illegal replication or imitation of an individual's signature with the malicious intent to deceive or commit fraud.Whether appearing on financial documents, legal contracts, or identification cards, the ability to accurately and swiftly detect forged signatures is crucial for maintaining the integrity of various processes and institutions. The field of offline signature verification and forgery detection is a complex domain filled with significant challenges, where the consequences of forgery can lead to substantial financial losses and damage the security reputation of cooperating and commercial organizations. Handwritten signatures have served as a fundamental means of authentication for centuries, utilized across sectors such as banking, legal documentation, and government processes. As technology advances, the necessity for robust and secure methods of signature verification becomes increasingly critical. Manual verification processes are not only labour-intensive but also prone to human error, rendering them inadequate for the modern demands of efficiency and security. Therefore, developing automated systems for signature verification and forgery detection is essential to meet contemporary standards and protect against fraud. Handwritten signatures remain a fundamental means of personal verification and authorization. Their importance spans across financial transactions, legal documents, and numerous other critical processes, underscoring their role in establishing identity and ensuring document integrity. However, the widespread issue of signature forgery presents a significant threat to the authenticity and security of these processes. In response to these challenges, this project aims to develop an advanced system for offline signature recognition and forgery detection using deep learning techniques.

Historically, handwritten signatures have been essential for authentication in sectors such as banking, legal documentation, and government processes. Their longstanding role and ubiquity make them a cornerstone of identity verification. However, as technological progress accelerates, the limitations of traditional signature verification methods have become increasingly evident. Manual verification, despite its historical reliability, is now impractical given modern demands for efficiency, accuracy, and heightened security.

The banking industry, in particular, faces significant risks due to its handling of sensitive information, official paperwork, and adherence to stringent government regulations (such as those from LIC). This makes the need for a robust system capable of distinguishing between authentic signatures and forgerieseven more critical, serving as a defence against theft and fraud.

©IJRASET: All Rights are Reserved

To address this challenge, leveraging biometric features unique to each individual presents a promising solution. While biometrics cover a range of possibilities, this project focuses on signatures as a distinctive biometric identifier. Signatures are influenced by various factors including an individual's mental state, body position, writing surface, and environmental conditions, making them a complex yetreliable indicator for identity verification.

II. LITERATURE SURVEY

In their 2021 study, Kshitij Swapnil Jain et al. aimed to develop a system for detecting forged signaturesusing a Convolutional Neural Network (CNN). Manual detection of forgery has inherent limitations, making automation highly desirable. The CNN in their system functions as both a feature extractor anda classifier, effectively capturing distinctive forgery traits . Similarly, in 2021, Kiran, Lakkoju Chandra, et al. focused on active methods for detecting digital signature forgery. They utilized a dataset of 2000 RGB images, which were preprocessed before training a Convolutional Neural Network (CNN) comprising three input layers, three hidden layers, and an output layer .

In their 2020 study, Poddar et al. introduced an innovative offline signature recognition and forgery detection system leveraging deep learning techniques. Their method integrates Convolutional Neural Networks (CNN) with the Crest-Through Method, the SURF algorithm, and Harris corner detection, creating a robust framework for identifying forged signatures.

In their study, a comparison between Support Vector Machines (SVMs) and Hidden Markov Models (HMMs) in offline signature verification is presented, highlighting their effectiveness in handling intrapersonal variability and discerning interpersonal similarity across various forgery scenarios. Another significant contribution, titled "An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach," proposes a method for verifying offline handwritten signatures using a single known genuine signature. This approach addresses challenges related to training with limited feature samples. To mitigate these challenges, the paper proposes two strategies: firstly, leveraging local features dispersed throughout the signatures using an explainable deep learning method and a unique local feature extraction approach; secondly, focusing on learning the characteristics of forged signatures in a binary classification problem, thereby compensating for the lack of genuine signature features by utilizing a larger set of forged signature samples.

The paper discusses recent developments in off-line signature verification, emphasizing the extraction of features from static signature images. Initial preprocessing includes converting the images to Portable Bitmap (PBM) format, followed by boundary extraction and feature extraction. Particularly highlighted is the Modified Direction Feature (MDF), integrated with other global features, to enhance accuracy and reliability in signature verification systems.

III. METHODOLOGY

Convolutional Neural Networks (CNNs) have proven highly effective across a wide range of image processing tasks in recent years. Unlike traditional approaches that rely on manually selected features extracted from images for classification, CNNs automate this process by learning features directly fromthe data. The architecture of a CNN typically consists of multiple layers starting from raw pixel inputs. Each layer performs computations on the input and passes the results to the next layer, ultimately feeding into a linear classifier. The parameters of these layers are learned through backpropagation, where gradients of the classification loss with respect to each parameter are computed and used to update the parameters to minimize the loss.

In the context of signature verification systems, which involve tasks like data retrieval, preprocessing, feature extraction, identification, and performance analysis, CNNs offer significant advantages. For off-line signature verification specifically, where signatures are captured as images, CNNs excel in automatically discerning relevant features without the need for intricate manual feature engineering. This capability ensures a balanced approach between minimizing False Acceptance Rates (FAR) and False Rejection Rates (FRR), crucial for the system's accuracy and reliability.

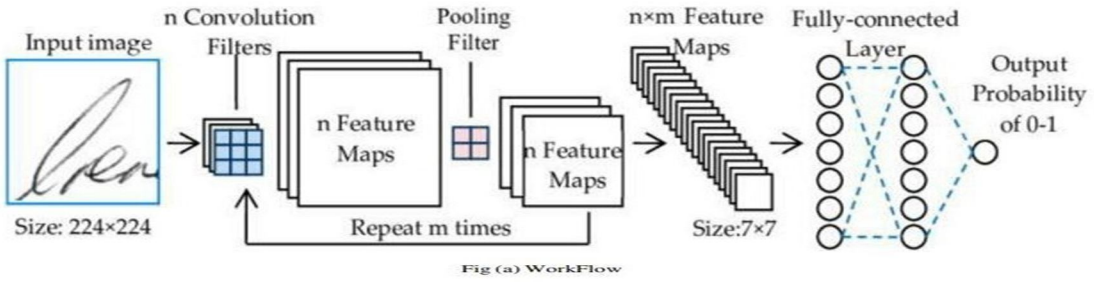


Fig (a) WorkFlow

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue X Oct 2024- Available at www.ijraset.com

IV. EXPERIMENTAL RESULTS

The experimental research presents results from offline signature recognition and forgery detection using a CNN model. Figure (a) illustrates the interface for image upload, while (b) depicts the uploadedimage prepared for prediction. Figure (c) indicates that the selected signature was identified as fraudulent, whereas Figure (d) shows that the selected signature is confirmed as original. These figures demonstrate the CNN model's effectiveness in distinguishing between genuine and forged signatures, showcasing its potential for robust signature verification applications.

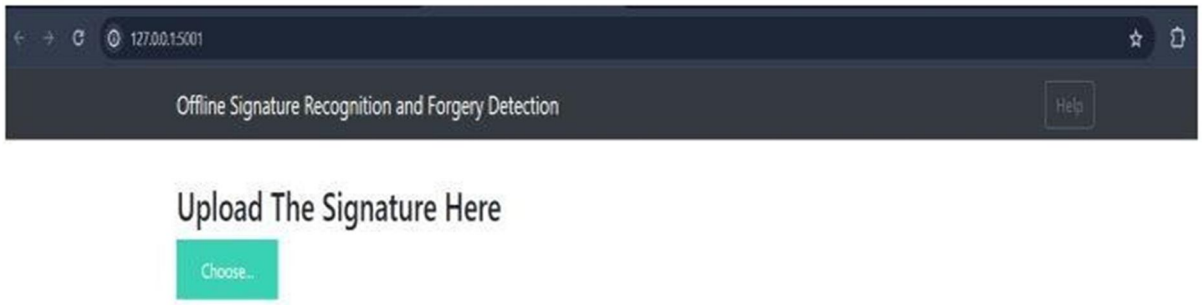


Fig (a) shows the option to upload the image



Fig (b) shows the uploaded image and ready for prediction

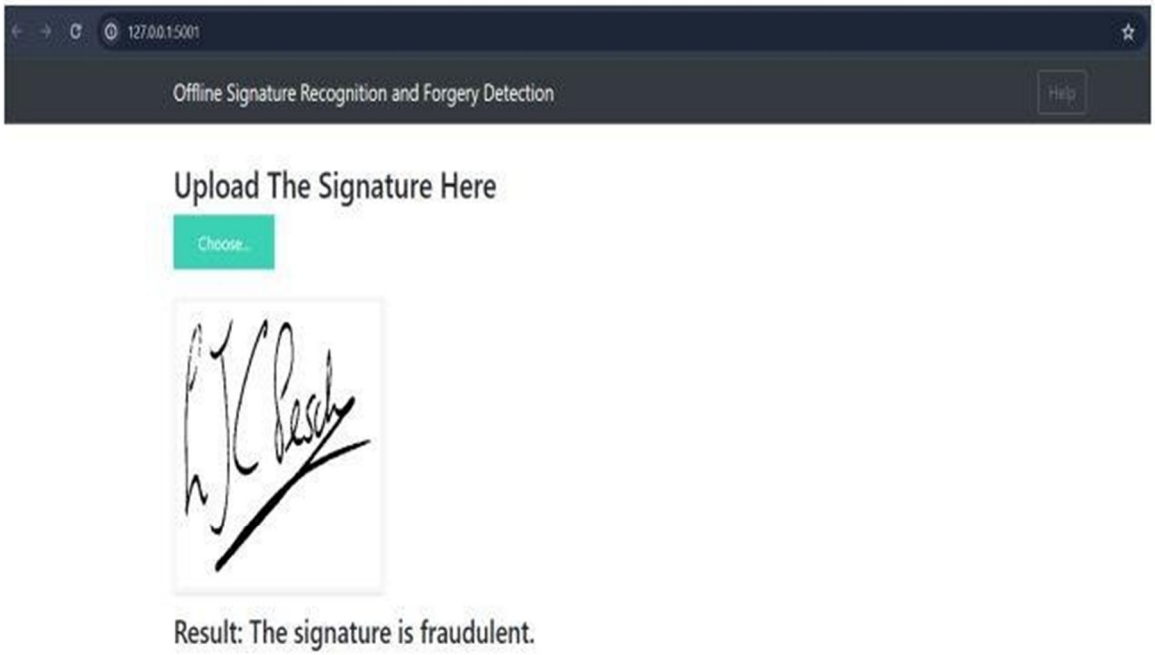


Fig (c) shows the selected signature was fraudulent



Fig (d) shows the selected signature is original

V. CONCLUSION

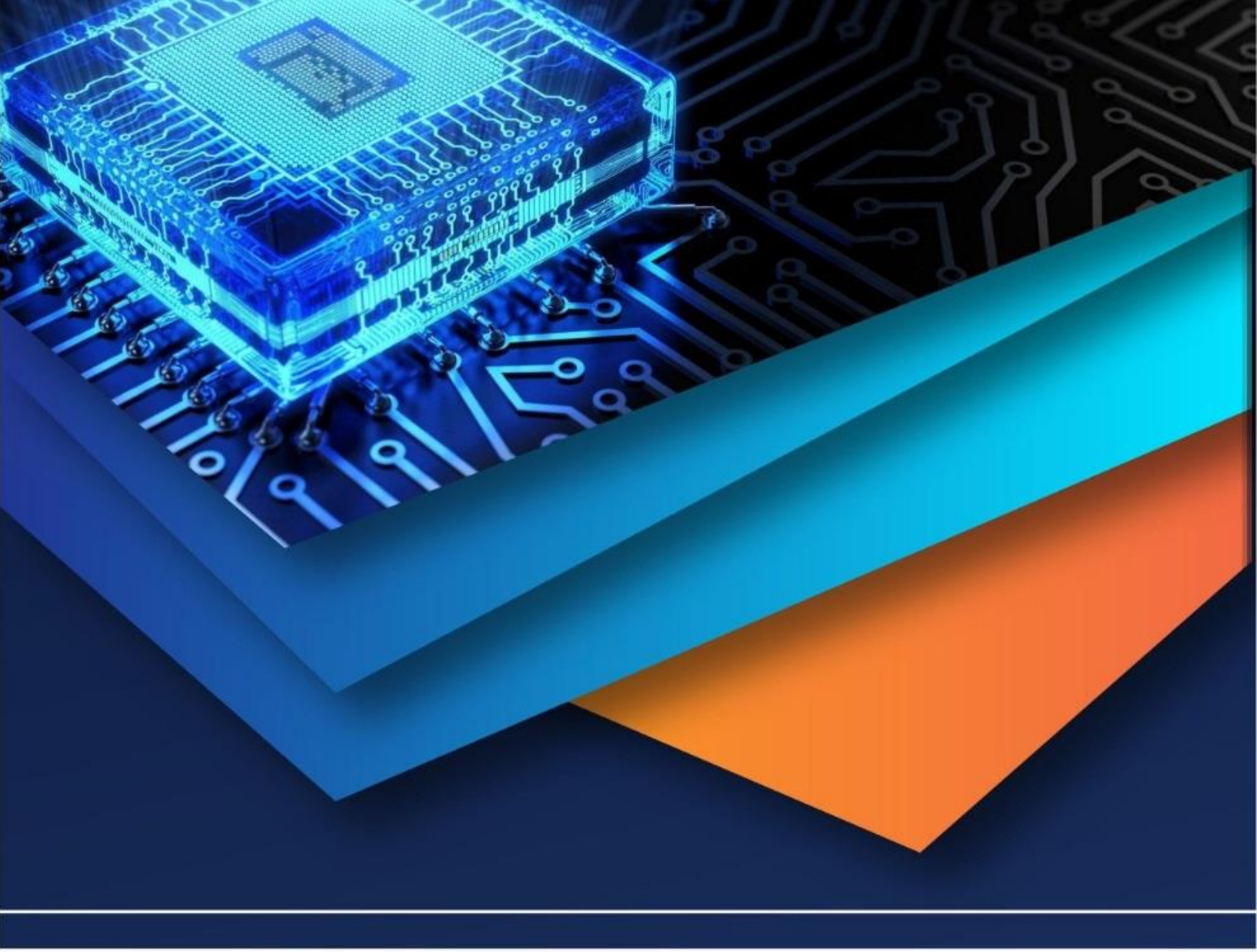
In conclusion, the development of an Offline Signature Recognition and Forgery Detection System represents a crucial initiative with profound implications for document authentication and security. By leveraging advanced technologies like Convolutional Neural Networks (CNN), the Crest-Through Method, SURF algorithm, and Harris corner detection algorithm, our goal is to establish a robust solution capable of accurately distinguishing between genuine and forged signatures.

This project holds significant promise for applications in sectors such as banking, legal documentation,and authentication processes, thereby enhancing security and reliability across various industries. Through continuous refinement and development, our aim is to deliver a system that not only meets current standards but also adapts to address emerging security challenges effectively in the future.

REFERENCES

[1] Kshitij Swapnil Jain, et al. “HANDWRITTEN SIGNATURES FORGERY DETECTION” (2021). International Research Journal of Engineering and Technology (IRJET) Volume: 08 Issue: 01 | Jan 2021.
[2] Kiran, Lakkoju Chandra, et al. "Digital signature Forgery Detection using CNN." (2021).
[3] Poddar, Jivesh, Vinanti Parikh, and Santosh Kumar Bharti. "Offline signature recognition and forgery detection using deep learning." Procedia Computer Science 170 (2020): 610-617.
[4] Longcamp, M., Boucard, C., Gilhodes, J.C., Anton, J.L., Roth, M., Nazarian, B., Velav, J.L.: Learning through hand- or typewriting influences visual recognition of new graphic shapes: Behavioral and functional imaging evidence. Science Journal of Cognitive Neuroscience 20, 802– 815(2008)
[5] G. Dimauro, S. Impedovo, G. Pirlo, A. Salzo, A multi-expert signature verification system forbankcheck processing, IJPRAI 11 (05) (1997) 827–84

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)