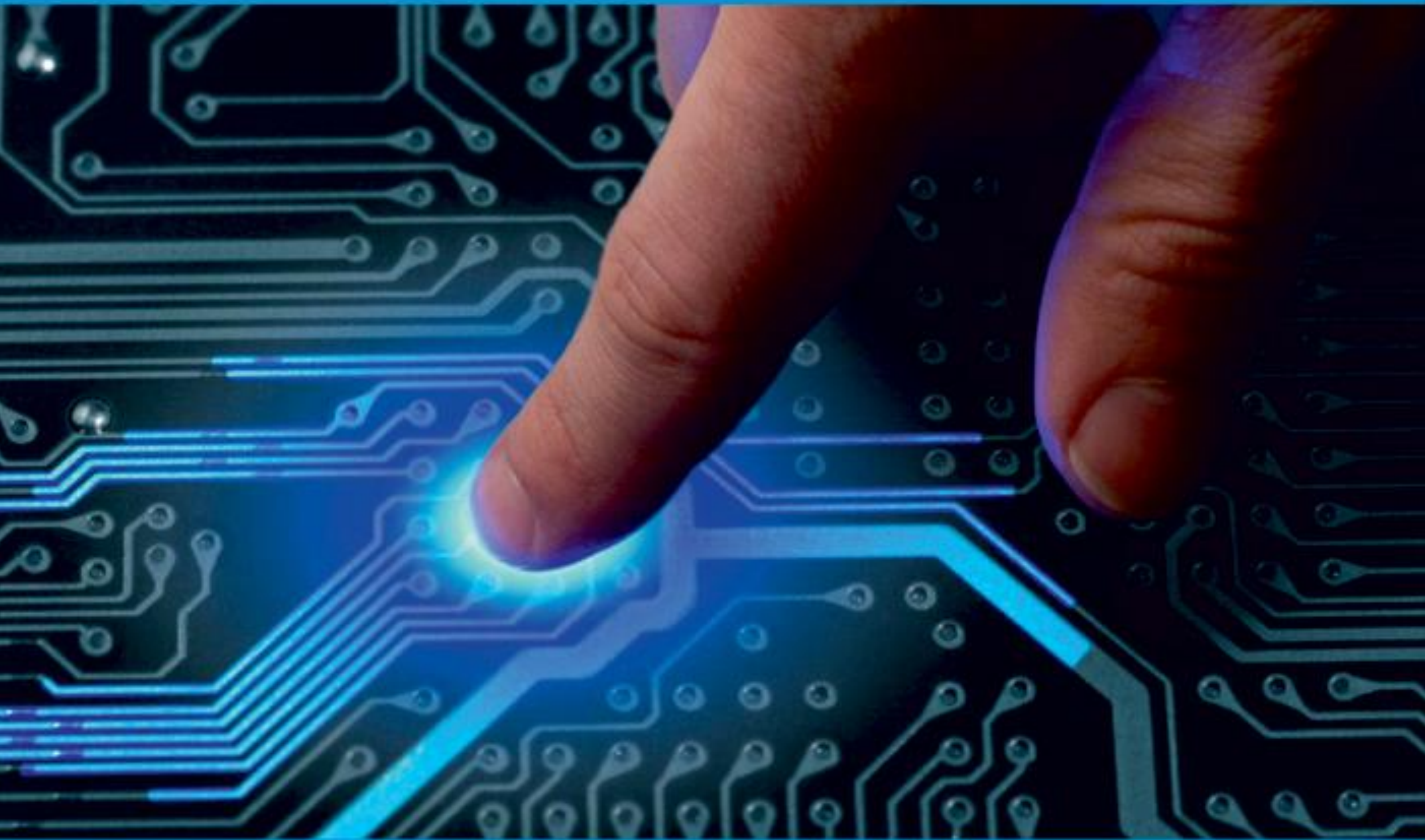
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204086 |

Offline Signature Recognition and Forgery Detection

Abhishree K M, Anu R, Archana Bai U, Ashwini Yallappa Hunagund, Prof. Vishwanath V K, Prof. Shankar Sarji

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India

U.G. Student Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India

Assistant Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India

Assistant Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India

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 detection of 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 marked by an ever-expanding reliance on digital communication and transactions, the specter of signature forgery looms large as a significant and pressing concern. Signature forgery entails the illicit act of replicating or imitating an individual's signature with the malicious intent to deceive or perpetrate fraud. Whether affixed to financial documents, legal contracts, or identification cards, the ability to discern and promptly detect forged signatures assumes paramount importance in safeguarding the integrity of diverse processes and institutions. The arena of offline signature verification and forgery detection emerges as a complex terrain fraught with serious challenges, where the repercussions of signature forgery inflict substantial financial losses and tarnish the security reputation of cooperating and commercial organizations.

Handwritten signatures have been a crucial means of authentication for centuries, used in various sectors such as banking, legal documentation, and government processes. As technological advancements continue, the need for robust and secure methods of signature verification becomes paramount. Manual verification processes are not only time-

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204086 |

consuming but are also susceptible to human error, making them inadequate for the modern demands of efficiency and security.
Handwritten signatures continue to serve as a fundamental means of personal verification and authorization. From financial transactions to legal documents, the reliance on signatures underscores their significance in establishing identity and ensuring the integrity of documents. However, the prevalence of signature forgery poses a substantial threat to the authenticity and security of various processes. In response to these challenges, this project endeavors to develop an advanced system for offline signature recognition and forgery detection using deep learning techniques. Handwritten signatures, with their longstanding history as a means of authentication, have played a crucial role in various sectors, including banking, legal documentation, and government processes. Their ubiquity and historical significance make them a hallmark of identity verification. However, as we navigate the era of technological progress, the shortcomings of traditional signature verification methods have become increasingly apparent. Manual verification processes, despite their historical reliability, are becoming impractical in the face of modern demands for efficiency, accuracy, and heightened security. The banking industry, given its involvement with sensitive information, official paperwork, and compliance with stringent government regulations (such as LIC), stands particularly vulnerable to the perils of signature forgery. Consequently, the imperative for a robust system capable of distinguishing between authentic signatures and forgeries becomes all the more crucial, serving as a bulwark against the likelihood of theft or fraud. One avenue to address this challenge involves harnessing the biometric features unique to each individual. While biometric features encompass a spectrum of possibilities, this project focuses specifically on the signature as a distinctive biometric identifier, recognizing its dependence on a myriad of factors, including the individual's state, body position, writing surface, and environmental conditions.

II. LITERATURE SURVEY

In their 2021 study, Kshitij Swapnil Jain et al. aimed to develop a system for detecting forged signatures using a Convolutional Neural Network (CNN). Manual detection of forgery has limitations, making automation desirable. The CNN serves as both a feature extractor and a classifier, capturing distinctive forgery traits[1]. In their 2021 study, Kiran, Lakkoju Chandra, et al. focus on active methods for detecting digital signature forgery. They use a dataset of 2000 RGB images, preprocess them, and train a Convolutional Neural Network (CNN) with three input layers, three hidden layers,and an output layer[2].

Poddar et al. (2020) introduced an innovative offline signature recognition and forgery detection system using deep learning techniques. Their method combines Convolutional Neural Networks (CNN), Crest-Through Method, SURF algorithm, and Harris corner detection [3].

A comparison of SVM and HMM classifiers in the off-line signature verification: The paper compares Support Vector Machines (SVMs) and Hidden Markov Models (HMMs) in offline signature verification, highlighting their effectiveness in absorbing intrapersonal variability and discerning interpersonal similarity through various forgery scenarios. “An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach”: This paper proposes an offline handwritten signature verification method utilizing a single known genuine signature, addressing challenges related to training with limited feature samples To overcome this, two strategies are proposed: firstly, leveraging local features dispersed throughout signatures using an explainable deep learning method and unique local feature extraction approach. Secondly, focusing on learning characteristics of forged signatures in a binary classification problem, compensating for the lack of genuine signature features by utilizing ample forged signature samples.

Global Features for the Off-Line Signature Verification Problem: The paper presents advancements in off-line signature verification, focusing on feature extraction from static signature images. Preprocessing involves conversion to a Portable Bitmap (PBM) format, followed by boundary extraction and feature extraction, notably the Modified Direction Feature (MDF) combined with other global features.

III. METHODOLOGY

Convolutional Neural Networks (CNNs) have tested no-hit in recent years at an outsized variety of image processing-based machine learning tasks. Several different strategies of playacting such tasks as shown in the architecture revolve around a method of feature extraction, during which hand-chosen options are extracted from a picture fed into a classifier to make a classification call. Such processes are solely as sturdy because of the chosen options, which

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204086 |

regularly take giant amounts of care and energy to construct. Against this, in CNN, the options fed into the ultimate linear classifier all learned from the dataset. A CNN consists of a variety of layers as shown in the architecture, beginning at the raw image pixels, that each performs an easy computation and feeds the result to the successive layer, with the ultimate result being fed to a linear classifier. The layers computation area unit supports a variety of parameters that are learned through the method of backpropagation, during which for every parameter, the gradient of the classification loss with relation to that parameter is computed and therefore the parameter is updated to minimize the loss performed. The look of any signature verification system typically needs the answer of 5 sub- issues: data retrieval, pre-processing, feature extraction, identification method, and performance analysis. Off-line signature verification just deals with pictures non-heritable by a scanner or a photographic camera. In an associate degree off-line signature verification system, a signature is non-heritable as a picture. This picture depicts a private sort of human. The method needs neither be too sensitive nor too rough. It should have a proper balance between an occasional False Acceptance Rate (FAR) and an occasional False Rejection Rate (FRR). Convolutional Neural Networks (CNNs) have indeed demonstrated remarkable success in various image processing-based machine learning tasks in recent years. Unlike traditional methods that rely on handcrafted features, CNNs automatically learn features from the data, making them highly effective in tasks such as image classification, object detection, and segmentation.

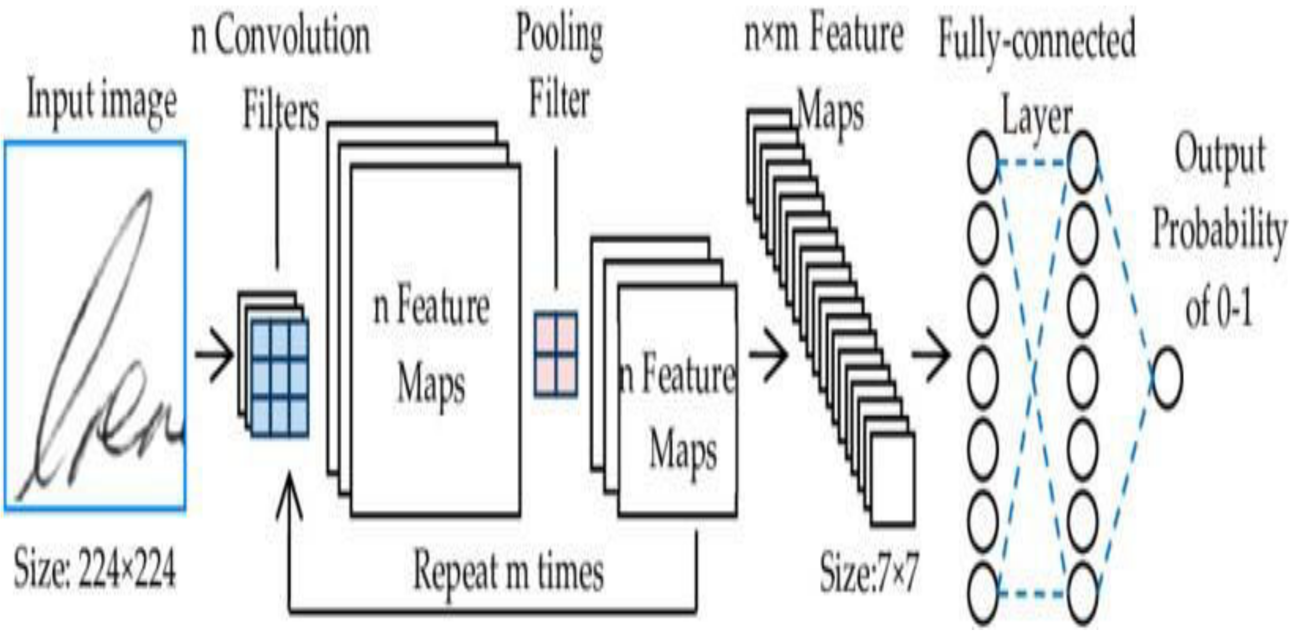


Fig (a) WorkFlow

IV. EXPERIMENTAL RESULTS

The following figures shows the results of offline signature recognition and forgery detection on CNN model. Fig(a) shows the option to upload the image (b) shows the uploaded image and ready for prediction (c) shows the selected signature was fraudulent (d) shows the selected signature is original.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204086 |

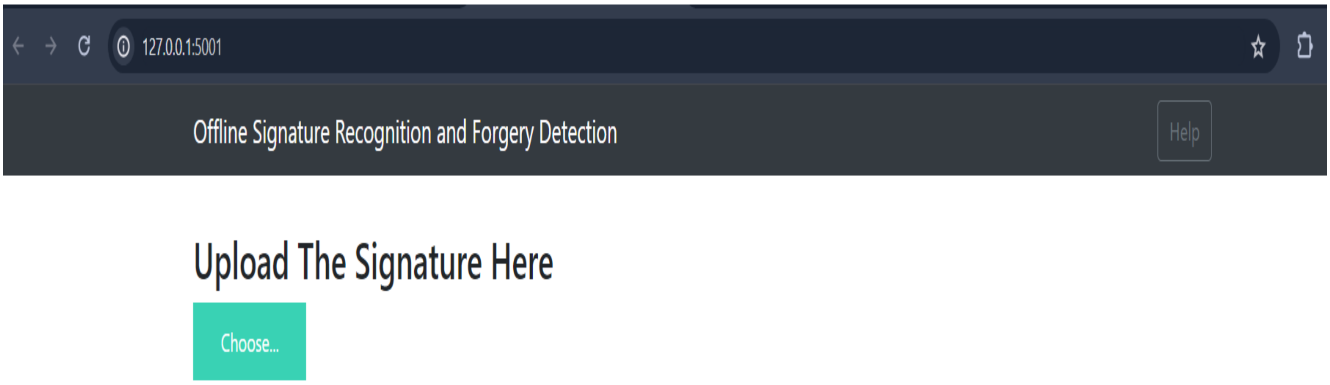


Fig (a) shows the option to upload the image

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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204086 |

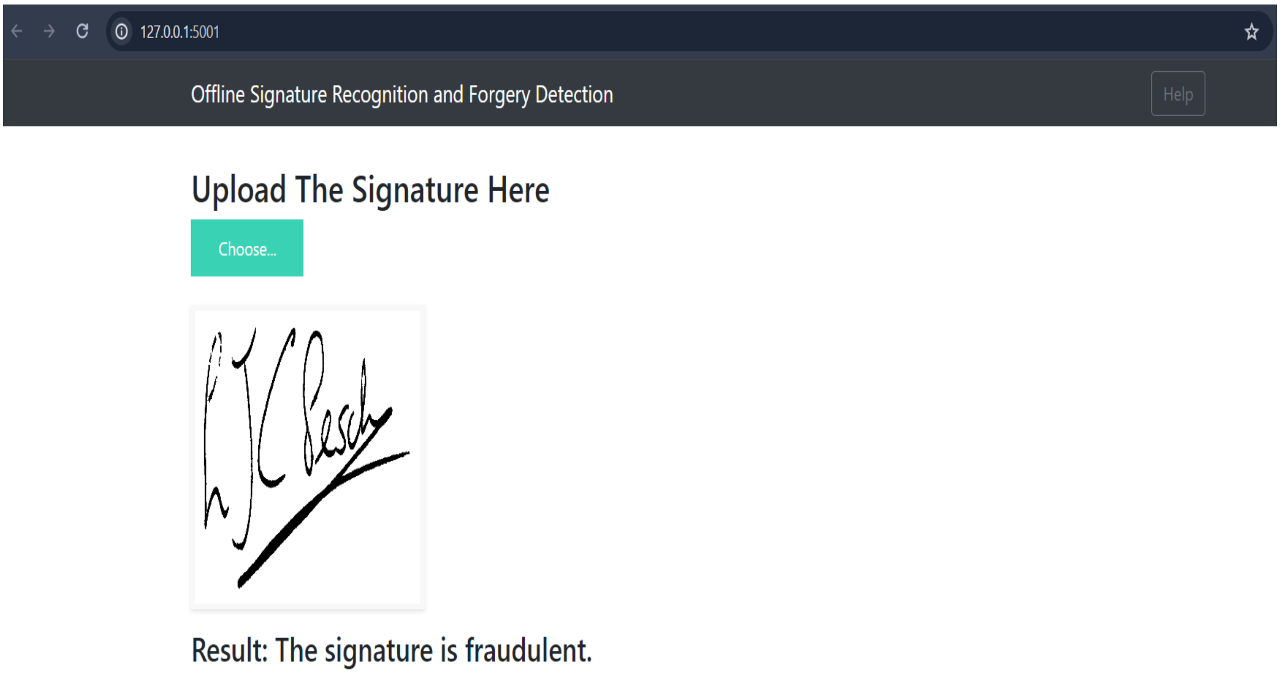


Fig (c) shows the selected signature was fraudulent

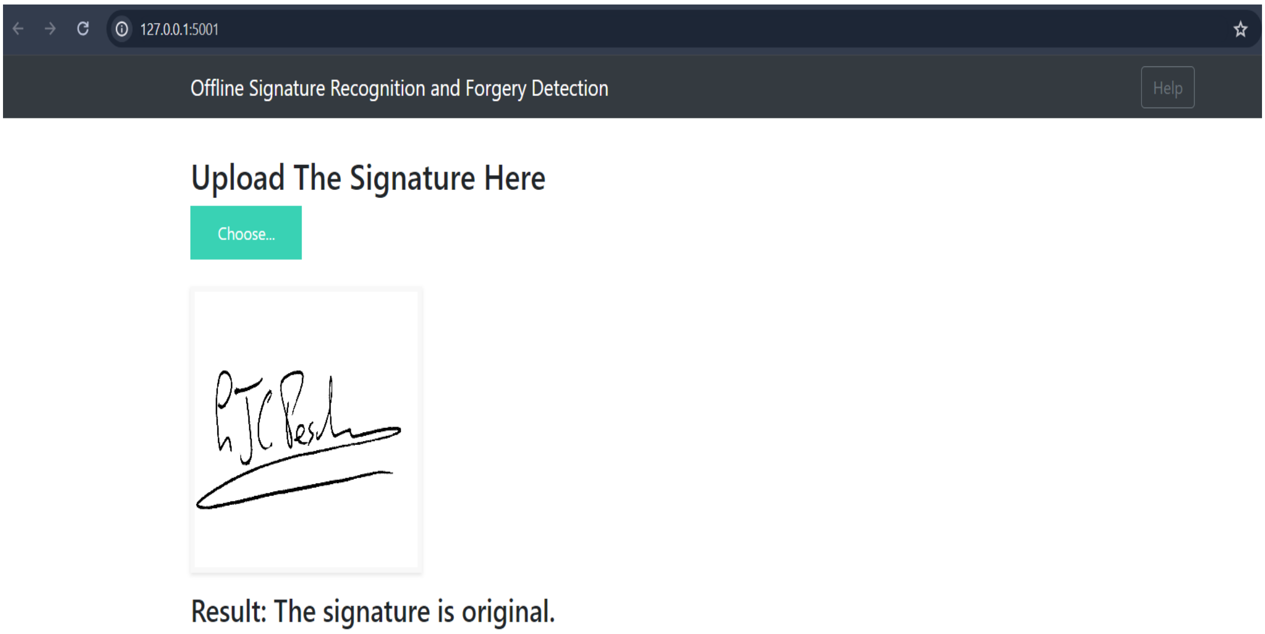


Fig (d) shows the selected signature is original

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204086 |

V. CONCLUSION

In conclusion, the development of an Offline Signature Recognition and Forgery Detection System is a critical endeavour with significant implications for document authentication and security. Through the integration of advanced technologies such as Convolutional Neural Networks (CNN), Crest-Through Method, SURF algorithm, and Harris corner detection algorithm, we aim to create a robust solution capable of accurately discerning between genuine and forged signatures.

Overall, this project holds great potential for applications in fields such as banking, legal documentation, and authentication processes, contributing to enhanced security and trustworthiness in various industries. Through ongoing development and refinement, we aim to deliver a system that not only meets current standards but also adapts to evolving security challenges 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 for bankcheck processing, IJPRAI 11 (05) (1997) 827–84

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details