iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.61171

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 IV Apr 2024- Available at www.ijraset.com

Enhancing Digital Cheque Security: A Machine Learning Approach to Signature Fraud Mitigation

Mr. G. Satya Mohan Chowdary[1] , Kankatala Suchitra Devi[2], Noorunnisa Begum[3], Tatikonda Sumanya[4], P Gireesha Syamala[5]

[1]*Assistant Professor* , [2, 3, 4, 5]*B.tech Students Department of Information Technology, Pragati Engineering College, Surampalem , Andhra Pradesh, India*

Abstract: ***Banks and financial systems must utilize signatures as a biometric authentication mechanism. There are two kinds of signatures: offline and online. Offline signatures are the favoured choice due of their simplicity and uniqueness. Digital checks require the same signatures as traditional checks: payer and payee. Using this proposed way, we develop a security system that validates entry applications and evaluates password alternatives. In addition to clearing bank checks and identifying problems, the proposed method will create a system for online digital signature validation, confidentiality, and fraud prevention. The goal is to successfully validate the legitimacy of online-generated digital checks using signatures.***

Keywords: Biometric, Deep Learning, Digital Cheque, Digital Signature, Financial systems.

I. INTRODUCTION

A check is a document that you can give to a bank that instructs it to pay the person whose name appears on it the specified amount. Checks are also a "negotiable instrument". A negotiable instrument is a paper that, when delivered to a banker or by a certain date, guarantees that the bearer will pay the agreed-upon amount. Hand identification is typically used to identify counterfeit checks. Manual identification is without a doubt the least effective approach to prevent check fraud. Employees must be able to identify fake checks using visual indicators such as security highlights. Furthermore, if the paper check is destroyed, OCR will be unable to recognize it. As a result, the check must be manually cleared. When this occurs, the automated process will not function. Furthermore, clearing a check using the existing CITS-based paper technique takes at least one day and up to three working days. Furthermore, the user must travel to the bank to deposit a check, which costs money and time. Nowadays, it is almost rare to see a checkbook exposed. The only institutions that still accept paper checks are governments and a tiny handful of reputable businesses. That has a motive behind it. Digital checks have generally altered how businesses are paid. It is a considerably speedier, less expensive, and environmentally friendly solution to solve a long-standing problem. A digital check is an electronic equivalent of traditional paper checks. Digital checks, like physical checks, are endorsed by the payee and signed by the payer. The check-to procedure relies heavily on authentication and verification. A person's signature serves as a concrete representation of their identity. It is used to validate information, differentiate between forged and genuine signatures, and then clear checks. A digital check is often processed as a payment request, which the sender submits to their bank. Biometrics refers to automated procedures for verifying and identifying individuals based on physiological or behavioral qualities that may be quantified, such as signatures. A person's signature is one of the most prominent and dependable biometric features for confirming their identification. Detecting counterfeit signatures is one of the most important aspects of a signature verification system. In order to use signature verification technology, a computer’s USB port must be linked to a digitizing tablet and a specific pen. No matter the size or placement of the signature, it may be made on the digitizing tablet using a special pen. The act of automatically and instantaneously confirming signatures to determine whether or not they are authentic is known as ”signature verification and forgery detection”, a handwritten signature on a document needs the computer to scan samples in order to undertake an investigation, but a digital signature that has already been recorded in a data format may be used for signature verification. CNNs are one of the most common types of deep neural networks. Because it employs 2D convolutional layers and mixes input data with learned features, the CNN architecture is an excellent choice for processing 2D data, such as photographs. You don't need to understand the characteristics utilized to identify photographs because CNNs execute the manual feature extraction for you. CNN uses direct feature extraction from photographs. Rather of being pre-trained, the relevant elements are discovered after training the network on a series of photos. Deep CNNs are used to verify the signature and identify the signer. A person's signature changes with time, which can make the authentication and verification procedure lengthy and prone to errors.

As a result, a standard database including each individual's signature is necessary to evaluate the effectiveness of the signature verification system and compare the results of different ways on the same database. To develop and train a model for the account holder's e-signature dataset, features are retrieved from each e-signature image, and Python is used to provide a second level of verification via OTP. This enables the account holder to identify between genuine and fraudulent e-signatures using CNN from digital checks.

II. LITERATURE SURVEY

This work presents a signature verification approach that is based on perception and probability [1]. It implies that the system estimates which class a signature belongs to before deciding whether or not to accept it. A signature's perception specifies the class to which it "possibly" belongs; actual membership in that class is determined by pattern categorization based on state transition. Furthermore, a precise proximity function is defined. In their method, the HMM and all of the spatial properties of the graph are integrated, and each feature is classified independently using a PNN Knowledge-based classifier. The suggested method[2] for confirming a check involves recognizing and examining the account holder's signature. The signature extraction procedure includes picture acquisition, grayscale image translation, localized binary image extraction, and segmentation. To use it, first extract an image and then divide it into locally created letters. The localized data is compared to the database that was previously acquired from the specified database.

Because this method is done offline, it may be portable. In addition to offering human verification as security, this work introduces an effective sign mechanism. The proposed system[3] use a neural network technique to recognize handwritten numerals in scanned input pictures. Unlike the prior, sluggish molded photo pixel comparison approach, our handwriting identification technology is quick and efficient. The first stage is to collect handwriting samples from numerous people and create a form that takes handwritten numbers. In this paper[4], they addressed the issue of universal, unconstrained text recognition. A unique, data- and computationally efficient neural network architecture has been described, which can be trained from scratch on various image sizes and line-level transcription sizes.

Using the same architecture and very modest hyperparameter tweaks, they exhibited state-of-the-art performance on seven publicly accessible benchmark datasets encompassing a variety of text recognition sub-tasks via a rigorous series of tests. It discusses[5] the most promising research areas currently being pursued, as well as major findings in the preprocessing, extraction, identification, and verification of handwritten fields on bank checks. To assist researchers researching automatic bank check processing, the article offers a detailed reference section with many sources. This paper [6] covers the extending of the courtesy amount and date for Malaysian bank checks. The system's extraction and detection module was well-built, but the recognition results were unimpressive. Potential causes of failure were studied in order to identify areas for improvement and future risks. They provided several innovative suggestions that served as the foundation for the check reading method that our team developed in this study [7]. Their concentration was on reading legal quantities and then assessing the recognition results.

Hidden Markov Models were offered as a tool for determining the legal quantity. The HMM (Hidden Markov Model) is particularly beneficial because the legal number does not have to be broken down into characters or actual words. [8] designed and tested an SVM classifier based on RBF Kernel on the SURF CASIA dataset, which provides an accuracy of 96.25%, and the SIFT CASIA dataset, which yields an accuracy of 98.75%. Author [9] provided an HMM-based solution with 96.78% accuracy for the OnOffSignHindi-75 dataset in this work. This technique was then tested against the SVM algorithm, which yielded an accuracy rating of 99.69%. In the study [10], a self-created dataset was treated to the Kullback Leiber Divergence technique, yielding 96.50% accuracy.

According to the publication [11], the Bangla Offline Signature Dataset's Local Binary Pattern Features achieve an accuracy of 75.34% when using the K-Nearest Neighbor approach and 90.36% while using the Support Vector Machine algorithm. According to the study [12], the discrete wavelet transform accuracy for the dataset created separately using SVM is 99.40%, whereas for the dataset created independently using KNN it is 98.44%. The discrete wavelet transform obtained 99.41% accuracy using random forest. The MCYT-75, CEDAR, GPDS160, and Brazilian PUC-PR datasets were used in this study's [13] application of the CNN-based model and handcrafted feature extractor (CLBP) SVM: Linear, RBF approach, and the outcomes were notable. In this work, the MCYT-75, CEDAR, GPDS-160, and Brazilian PUC-PR datasets were used to create an accuracy of 94.84% utilizing the Model Agnostic Meta-Learning (MAML) technique [14].

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

III. SYSTEM ANALYSIS

A. *Existing System*

A secure web-based application designed to make it easier to authenticate and validate digital signatures on online checks would most likely comprise the present "Online Digital Cheque Signature Verification using Deep Learning Approach" system. To ensure safe access, the system would have user authentication mechanisms. Multi-factor authentication could also be used for added security. Users of the platform, both payers and payees, will be able to generate digital checks with digital signatures and other relevant components such as payee information and amount.

The deep learning model employed for signature verification would function as the system's brain. To accurately discriminate between valid and counterfeit digital signatures, this model would have been trained on a range of datasets. The seamless integration of the verification procedure into the digital check clearing system would ensure that only valid transactions were executed.

The system's intended use of encryption techniques would safeguard sensitive user and transaction data during transmission and storage. To combat new threats, security fixes and updates would be applied on a regular basis. Because of the thorough design of the user interface, users will be able to easily verify transaction histories, access relevant account details, and browse the site.

Testing is an important step in the development process, and it involves a number of testing approaches to confirm the system's overall performance, security, and dependability. The system would be put on secure servers after comprehensive testing, with backup and recovery mechanisms in place in case of unexpected events.

DISADVANTAGES OF THE EXISTING SYSTEM

1) *Negative and false positives:* The possibility of false positives—valid signatures identified as forgeries—and false negatives—forged signatures identified as legitimate—is one of the primary issues with signature verification systems. There may be problems in the verification process if the deep learning model is not completely accurate in distinguishing between fraudulent and real signatures.
2) *Reliance on Instructional Data:* The quality and representativeness of the training dataset significantly influence how well the deep learning model works. Inadequate coverage of real-world signature variability in the training dataset may impair the model's ability to generalize accurately, resulting in imprecise verification.
3) *Resource Intensity:* Deep learning models can be computationally demanding, especially when designed for complex tasks such as signature verification. This could constrain the amount of processing power and resources required, affecting the system's scalability and real-time performance.
4) *Adaptability to Changing Fraud Tactics:* Over time, signature forgery tactics may evolve, and the current system may not be intended to respond quickly to new fraud strategies. To tackle new and complex counterfeit efforts, the deep learning model should be updated and enhanced on a regular basis.
5) *User Training and Familiarity:* When adjusting to the system, users may experience a learning curve, especially if they are unfamiliar with digital signature procedures. This restriction may cause errors when creating digital checks or make it more difficult to understand the feedback provided by the system when confirming a signature.

B. *Proposed System*

The suggested system's major features include the ability to securely create digital checks, as well as options for entering payee information, defining transaction amounts, and attaching digital signatures. During the check processing, the deep learning model performs real-time verification by seamlessly integrating into the system workflow. The goal is to detect and prevent potential fraud while reducing the risk of false positives and negatives and ensuring that only legitimate transactions occur.

The proposed system comprises user authentication mechanisms, multi-factor authentication options, and data transit and storage encryption techniques to improve user experience and system security. The system also prioritizes usability, with an easy-to-use user interface that allows users to quickly browse the platform, check transaction histories, and obtain relevant account information.

The proposed approach successfully confirms the authenticity of digital signatures on checks, adding to the overall goal of strengthening confidence and security in online financial transactions. Its goal is to give banks and other financial institutions with a dependable and efficient mechanism to clear digital checks while protecting privacy, preventing fraud, and increasing trust in the digital banking sector.

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

IV. SYSTEM DESIGN

A. System Architecture

Below diagram depicts the whole system architecture.

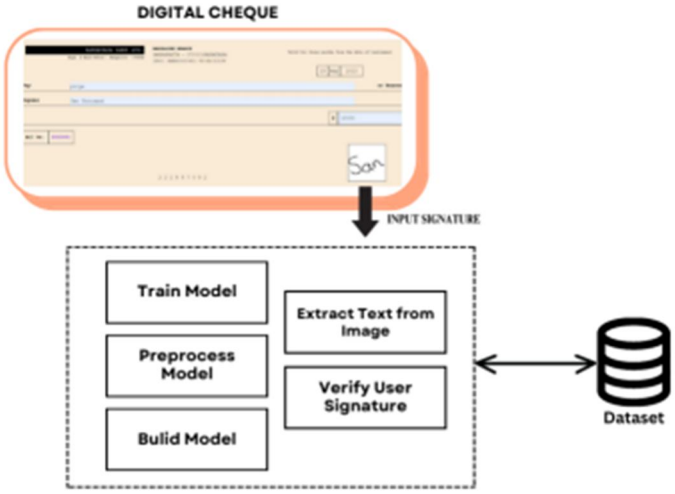


Fig 1. Methodology followed for proposed model

IV. SYSTEM IMPLEMENTATION

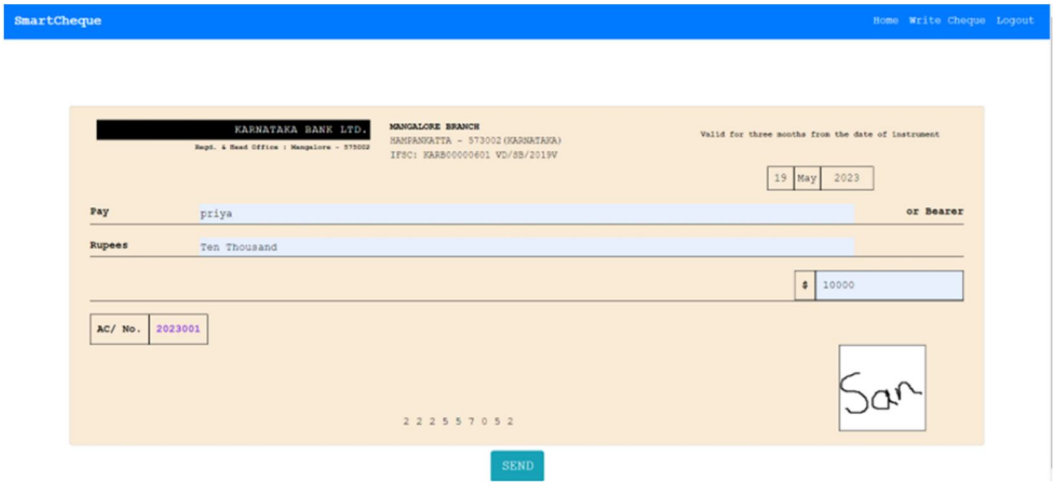
MODULES

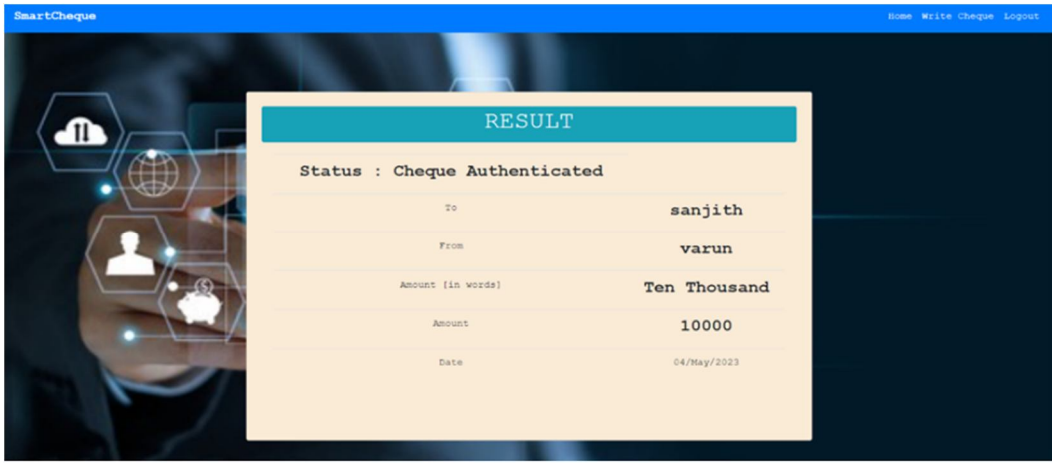
1) *Module for User Authentication:* This module manages user authentication when they log into the system. The digital check verification platform includes features such as username/password authentication and may even include additional security measures such as multi-factor authentication to ensure secure access.
2) *Digital Check Creation Module:* This module allows users to safely create digital checks. Users can enter payee information, determine transaction amounts, and insert digital signatures. This module is responsible for creating a digital image of a check and adding the necessary transaction data.Deep Learning Signature
3) *Verification Module:* The Deep Learning Signature Verification Module is the brains of the system. This module includes an advanced deep learning model for signature verification. It accepts digital signatures added to digital checks as input, runs them through a trained model, and returns a verification result confirming the signature's authenticity.
4) *Transaction Processing and Clearing Module:* The Transaction Processing and Clearing Module manages the whole digital check workflow. It integrates the results of the signature verification process, making it easier to securely process and clear valid transactions. This module may include communication with banking systems to ensure that transactions move smoothly.
5) *User Interface and Reporting Module:* The User Interface and Reporting Module allow users to engage with the system in a simple and intuitive manner. It allows users to access account information, monitor transaction history, and create digital checks. This module can also generate reports on transaction status, such as confirmed signatures and transactions that have been reported or denied.

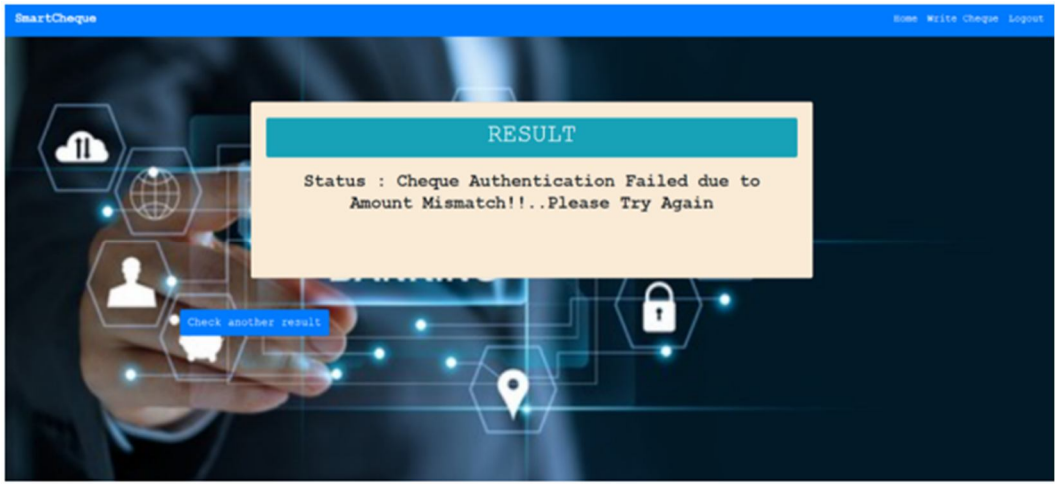
Together, these components form a complete system that handles transaction processing, user interaction, deep learning-based signature verification, digital check generation, and user authentication. The modular design improves the system's maintainability and scalability while also making individual components easier to upgrade and troubleshoot.

V. RESULTS AND DISCUSSION

The cheque interface represents the system's fundamental component. The UI is designed to look like a real check. The user must provide all required information in the specified field, including the bearer's name and the approved amount stated in words and numbers. After entering the essential information, the user must use a mouse to legitimately sign the available space before clicking the "send" button. Following signature verification, the system will indicate if the discoveries were successful or not.







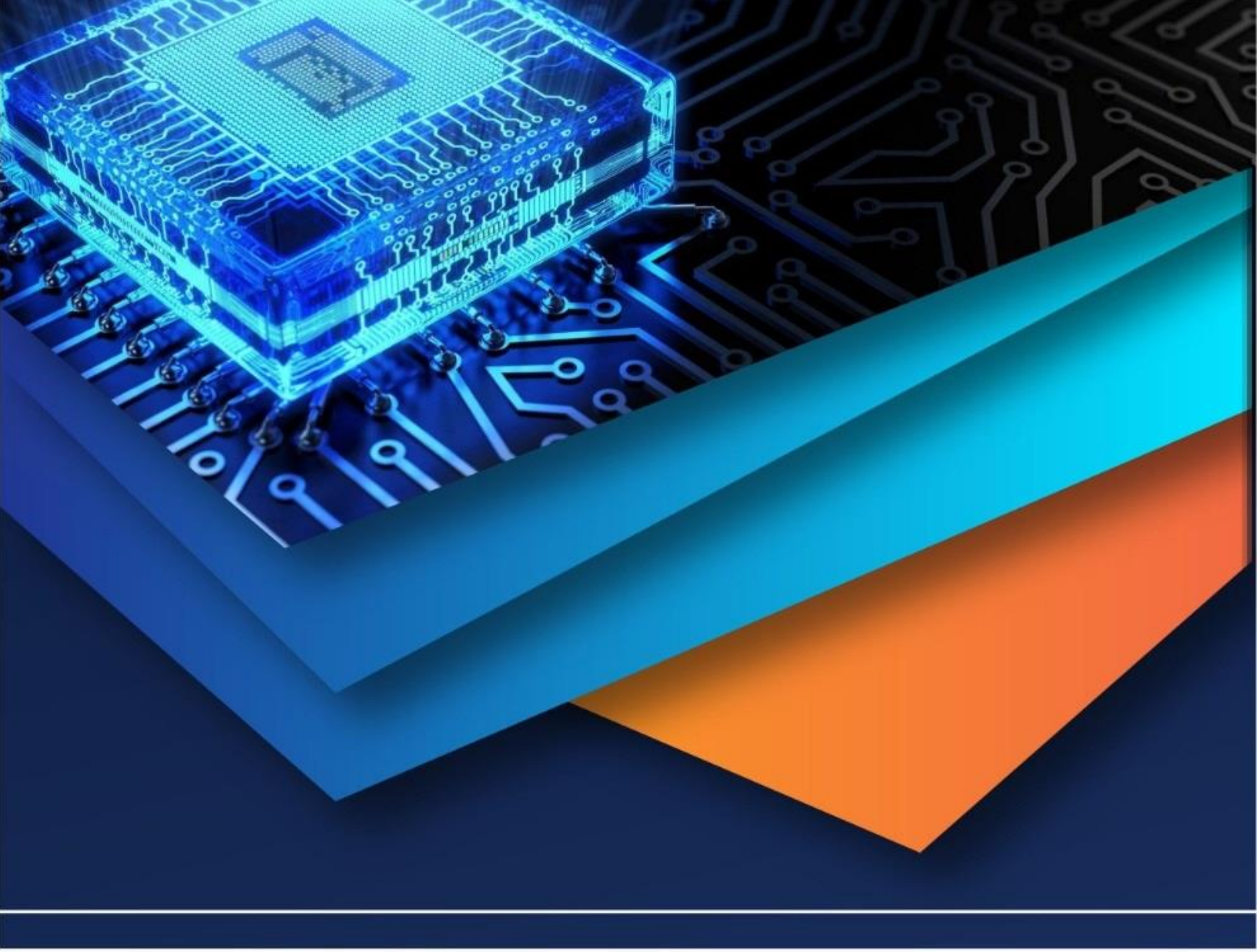
VI. CONCLUSION AD FUTURE WORK

The proposed deep learning-based online digital cheque clearance system has the potential to greatly increase check processing speed and accuracy. Banks and other financial institutions may use deep learning algorithms to automate the process, removing the need for human intervention and decreasing the risk of errors. It also improves fraud detection by adding an additional security layer to financial transactions. Still, a few issues will need to be addressed in the future project.

One of the most difficult challenges is creating deep learning models capable of handling a wide variety of check forms and handwriting styles. Another problem is ensuring that the models recognize and categorize the various components of a cheque accurately. Furthermore, the success of online digital cheque clearance through deep learning would be dependent on the development of a dependable and secure system capable of handling massive quantities of transactions in real time. Future research should focus on increasing the robustness and accuracy of deep learning models. More advanced algorithms, training data, and testing procedures can be employed to accomplish this. Another focus area could be developing a uniform check format that deep learning models can readily detect and process.

REFERENCES

[1] Sook Chin Chiew , Xin Yuan Law , Ren Zhang Tan , XinYing Chew, Khai Wah Khaw "Digital Recognition by Deep Learning Techniques: A Proposed Digit Recognizer to Automate Cheque Deposition",In Amity Journal of Computational Sciences (AJCS) 2019
[2] Mukesh Jha, Madhur Kabra, Sahil Jobanputra, and Prof. Rupali Sawant, "Automation of Cheque Transaction using Deep Learning and Optical Character Recognition", In Second International Conference on Smart Systems and Inventive Technology (ICSSIT 2019)
[3] Saleem Ulla Shariff, Maheboob Hussain, Mohammed Farhaan Shariff, "Automated bank cheque verification using image processing and deep learning methods", Springer Science+Business Media, LLC, part of Springer Nature 2020
[4] Victor Carbune, Pedro Gonnet, Thomas Deselaers, Henry A. Rowley, Alexander Daryin, Marcos Calvo, Li- Lun Wang, Daniel Keysers, Sandro Feuz, Philippe Gervais, "Fast multi-language LSTM-based online handwriting recognition", International Journal on Document Analysis and Recognition (IJDAR) (2020) 23:89–102
[5] Girish C. J, Mrs. Geetha G. P "Design of Bank Cheque Validation System", International Journal of Engineering Research Technology (IJERT) 05, May-2015
[6] Mohit Mehta, Member, IACSIT, Rupesh Sanchati and Ajay Marchya, "Automatic Cheque Processing System", International Journal of Computer and Electrical Engineering, 2018
[7] Sebastian Salazar-Colores, Eduardo Cabal-Yepez, "A Fast Image Dehazing Algorithm Using Morphological Reconstruction" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 28, NO. 5, MAY 2019
[8] T Naseer and N Dogru. Signature recognition by using sift and surf with svm basic on rbf for voting online. International Conference on Engineering and Technology (ICET), pages 1–5, 2017.
[9] A Ferrer Miguel, Chanda Sukalpa, Diaz Moises, Chayan Kumar Banerjee, Anirban Majumdar, Carmona Duarte Cristina, Acharya Parikshit, and Pa Umapada. Static and dynamic synthesis of bengali and devanagari signatures. IEEE Transactions on Cybernetics, 48(10):2896–2907, 2018.
[10] P Mondal and N Kundu. An automated handwritten signature detection approach for e-security purposes. Third International Conference on Science Technology Engineering Management (ICONSTEM), pages 409–413, 2017.
[11] S K Jadhav and M K Chavan. Symbolic representation model for offline signature verification. 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pages 1–5, 2018.
[12] A Beresneva, A Epishkina, and D Shingalova. Handwritten signature attributes for its verification. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pages 1477–1480, 2018.
[13] Luiz G. Hafemann, Robert Sabourin, and Luiz S. Oliveira. Characterizing and evaluating adversarial examples for offline handwritten signature verification. IEEE Transactions on Information Forensics and Security, 14(8):2153 – 2166, January 2019.
[14] L. G. Hafemann, R. Sabourin, and L. S. Oliveira. Meta-learning for fast classifier adaptation to new users of signature verification systems. IEEE Transactions on Information Forensics and Security, 15:1735–1745, 2020



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY