International Journal for Modern Trends in Science and Technology
Volume 10, Issue 04, pages 375-380.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue04.html
DOI: https://doi.org/10.46501/IJMTST1004058

An Image-Based Signature Verification System for Enhanced Cheque Security

D.Uma [1] , Gade Pavan Satya Sai [2], Sangadala Jayalakshmi [2], Mallipudi Meher Keerthana [2], Tavitiki Mounika [2], Ainavilli Surya Revathi [2]

[1]Assistant Professor, Department of Computer Science Engineering, Pragati Engineering College, Surampalem , Andhra Pradesh, India.
[2]Department of Computer Science Engineering, Pragati Engineering College, Surampalem , Andhra Pradesh, India.

To Cite this Article
D.Uma, Gade Pavan Satya Sai, Sangadala Jayalakshmi, Mallipudi Meher Keerthana, Tavitiki Mounika, Ainavilli Surya Revathi, An Image-Based Signature Verification System for Enhanced Cheque Security, International Journal for Modern Trends in Science and Technology, 2024, 10(04), pages. 375-380. https://doi.org/10.46501/IJMTST1004058

Article Info
Received: 06 April 2024; Accepted: 18 April 2024; Published: 26 April 2024.

ABSTRACT

The use of signatures as biometric authentication methods is critical in banking and financial systems. There are two types of signatures: offline and online, with offline signatures being more common due to their simplicity and distinctiveness. Digital checks, like paper cheques, require both the payer and the payee to sign them. In this suggested technique, we provide a security system that verifies entry applications and evaluates password alternatives. The suggested technique will result in a system that can validate digital signatures online while passing bank checks, identifying defects, ensuring secrecy, and avoiding fraud. The purpose is to correctly evaluate the legitimacy of online digital checks that incorporate signatures.

Keyword's: Biometric, Deep Learning, Digital Cheque, Digital Signature, Financial systems

1. INTRODUCTION

A check is a document that can be submitted to a bank ordering it to pay the person whose name appears on it the specified amount. Checks are also included in the definition of "negotiable instrument". A negotiable instrument is a paper that, when delivered to a banker or by a certain date, guarantees the bearer's payment of the stated amount. Manual identification is a popular approach for recognizing phony checks. Without a question, the least effective way of combating check fraud is human identification. Employees must be able to identify fraudulent checks using visual cues such as security highlights. Furthermore, if the paper check is damaged, OCR will be unable to recognize it. As a result, an individual must manually clear the cheque. In that instance, the automated process will fail.

Furthermore, the current CITS-based paper cheque clearance process takes at least one day and maybe three working days to clear a cheque. Furthermore, the user must travel to the bank to deposit a cheque, which is both costly and time-consuming. Nowadays, it is unusual to see a check book out in the open. Only governments and a few respectable companies continue to accept paper checks. That is not without reason.

Overall, digital cheques have revolutionized how companies receive payments. It is a far faster, less expensive, and ecologically friendly solution to an ancient problem. Digital checks are electronic versions of paper checks. The payer signs digital checks, and the payee endorses them, much as paper checks. Check to procedure is strongly reliant on verification and authentication. A person's signature is a tangible depiction of who they are. It is used to distinguish between fraudulent and genuine signatures, verify the information, and then clear the check.

A digital check is usually handled as a payment request sent from the sender to their bank. Biometrics provides automated ways for verifying and identifying identities based on quantifiable physiological or behavioural traits such as signatures. One of the most extensively utilized and reliable biometric qualities for authenticating a person's identity is their signature. Detecting fraudulent signatures is a critical component of a signature verification system. To employ signature verification technology, a computer's USB port has to be connected to a digitizing tablet and a particular pen. The signature, regardless of its size or placement, may be produced on the digitizing tablet with a special pen.

"Signature verification and forgery detection" refers to the process of automatically and immediately checking signatures to ensure their legitimacy. A digital signature that has already been saved in a data format may be used for signature verification, however a handwritten signature on a document requires the computer to scan samples in order to conduct an inquiry. Convolutional neural networks (CNNs) are one of the most common types of deep neural networks. Because it uses 2D convolutional layers and mixes input data with learnt features, the CNN architecture is an excellent choice for processing 2D data, such as photographs.

Because CNNs execute the manual feature extraction for you, you don't have to be conversant with the features utilized to categorize images. CNN employs direct feature extraction from photos. Instead of being pre-trained, the essential characteristics are discovered when the network is trained on a set of pictures. The use of Deep CNNs to identify the signer and determine whether the signature is authentic. Individuals' signatures vary over time, making signature verification and authentication potentially time-consuming and error-prone.

As a result, a standard database including each person's signatures is required for assessing the performance of the signature verification system and comparing results produced using different methodologies on the same database. Python is used to extract attributes from each e-signature picture and provide a second step of verification via OTP to develop and train a model for the account holder's e-signature dataset to distinguish between legitimate and fake e-signatures using CNN from digital checks.

2. LITERATURE SURVEY

This work presents a perception- and probability-based method to signature verification. It indicates that before deciding whether or not to accept a signature, the system determines approximately to which class the signature belongs. Perception indicates the class to which a "signature" may belong; pattern classification based on state transition decides whether or not the signature genuinely belongs to that class. It also defines an exact closeness function. The spatial attributes of the whole graph and the HMM are combined in their system, and each feature is classified independently using a PNN Knowledge-based classifier. The account holder's signature is recognized and examined in the suggested method to verify a cheque [2]. The signature extraction procedure includes image capture, grayscale image the translation, binary image extraction (localized), and segmentation. The technique requires extracting a picture and then breaking it down into characters that will be translated. The localized information is compared to the previously obtained database from the given database. This method is portable because it is implemented in offline mode. This study proposes an efficient signing method as well as human verification for security. The suggested system uses a neural network approach to detect handwritten numbers from scanned input pictures. In contrast with the preceding, Unlike the rather slow merged image pixel comparison process, this method of handwriting detection is efficient and rapid. Initially, numerous people's handwriting samples are collected, and a form for handwritten digit input is created. This work addresses the subject of universal [4], unrestricted text recognition. They've presented a brand-new, data- and computationally-efficient neural network design that can be learned from start to finish on a variety of image

formats utilizing different line-level transcription sizes. They carried out a thorough series of experiments on seven publicly accessible benchmark datasets encompassing a range of text recognition sub-tasks, they have exhibited cutting-edge performance on all of them while utilizing the same architecture and making only minor hyperparameter changes. It discusses major breakthroughs in the preprocessing, [6] extraction, identification, and validation of handwritten fields on bank checks, as well as the most promising areas of research now. The article provides a thorough reference with several references to help researchers researching automated bank cheque processing. This study discussed the extension of.

3. SYSTEM ANALYSIS

A. EXISTING SYSTEM

The current system for "Online Digital Cheque the Signature Validation using Deep Learning Approach" would most likely include a secure web-based application for authenticating and validating digital signatures on online checks. The system would incorporate user authentication procedures to assure safe access, as well as multi-factor authentication alternatives for increased security. Users, both payers and payees, will be able to produce digital cheques within the platform, entering important parameters such as payee information, the amount, and adding digital signatures.

The deep learning model for signature verification would serve as the system's heart. This model would have been trained on a broad dataset of genuine and faked digital signatures in order to reliably distinguish between legitimate and fraudulent signatures. The verification procedure will be seamlessly incorporated into the digital cheque clearing system, guaranteeing that only valid transactions are handled.

To further security, the system would most likely utilize encryption techniques for data transfer and storage, safeguarding critical user and transaction information. Regular updates and security fixes would be made to address evolving risks. The user interface would be created with simplicity of use in mind, allowing users to move across the platform simply, check transaction histories, and access essential account data.

Testing would be an important stage in the development process, using a variety of testing approaches to check the system's dependability, security, and general performance. Once extensively tested, the system would be deployed on secure servers, with facilities for backups and recovery methods in the event of unanticipated issues.

.

DISADVANTAGES OF THE EXISTING SYSTEM

1. **False Positives and Negatives:**
One of the most significant issues in signature verification systems is the likelihood of false positives (valid signatures identified as forgeries) and false negatives (forged signatures classified as legitimate). The deep learning model's accuracy in detecting real and counterfeit signatures may not be flawless, resulting in mistakes in the verification process.
2. **Dependency on Training Data:**
The quality and representativeness of the training dataset have a significant impact on the deep learning model's efficacy. If the training dataset does not sufficiently capture the diversity of real-world signatures, the model may fail to generalize properly, resulting in erroneous verification.
3. **Resource Intensiveness:**
Deep learning models, particularly those intended for difficult tasks such as signature verification, may be computationally costly. This may limit the processing power and resources required, affecting the system's scalability and real-time performance.
4. **Adaptability to Evolving Fraud Techniques:**
Signature forging tactics may vary over time, and the current system may not be designed to react fast to new fraud methods. Regular updates and upgrades to the deep learning model would be required to counter new and sophisticated forging attempts.
5. **User Training and Familiarity:**
Users, particularly those new with digital signature processes, may have a learning curve as they adjust to the system. This restriction may cause problems during the generation of digital cheques or issues in interpreting the system's comments on signature verification.

B. PROPOSED SYSTEM

The proposed system's primary feature includes the ability to securely produce digital cheques, as well as options for entering payee information, selecting transaction amounts, and adding digital signatures. The deep learning model works smoothly with the system's

workflow, performing real-time verification during cheque processing. The objective is to limit the danger of false positives and negatives, ensuring that only genuine transactions occur while identifying and avoiding possible fraud.

To improve user experience and system security, the proposed system includes user authentication mechanisms, multi-factor authentication choices, and encryption protocols for data transfer and storage. Furthermore, the system promotes usability with an easy user interface, allowing users to easily traverse the platform, check transaction histories, and obtain essential account information.

The suggested solution intends to contribute to the larger goal of increasing confidence and security in online financial transactions by correctly authenticating the validity of digital signatures on checks. It intends to offer a dependable and fast method for banks and financial institutions to clear digital cheques, thereby maintaining secrecy, reducing fraud, and creating trust in the digital banking ecosystem.

ADVANTAGES OF THE PROPOSED SYSTEM

1. Improved Accuracy and Reliability:

The use of a deep learning model for signature verification improves the accuracy and reliability of the authentication process. By training the model on a broad dataset, the method hopes to decrease false positives and negatives, guaranteeing that only valid digital signatures are recognized while identifying possible forgeries more effectively.

2. Real-Time Verification:

The suggested technology allows for real-time authentication of digital signatures during the handling of online cheques. This feature improves the efficiency of money transactions by lowering the time necessary for validation and clearing. Real-time verification improves the overall security of the system by rapidly detecting problematic transactions.

3. Enhanced Security Measures:

The system contains strong security features, such as user authentication processes and multi-factor authentication possibilities. In addition, encryption mechanisms for data transfer and storage are used to protect sensitive user and transaction information. These security elements add to the system's overall integrity by safeguarding it against illegal access and data breaches.

4. User-Friendly Interface:

The suggested system promotes a user-friendly design, allowing users to explore the platform with ease. A straightforward design makes it easier to create digital cheques and gives users quick access to transaction history and account information. This user-centric strategy improves the overall user experience and fosters the wider adoption of digital cheque transactions.

5. Prevention of Fraud and Confidentiality Assurance:

By correctly confirming digital signatures on online checks, the method helps to avoid fraud. It takes a proactive approach to recognizing and minimizing possible hazards connected with forged signatures, which improves the overall security of financial transactions. Secure data handling techniques provide confidentiality by shielding sensitive information from unwanted access.

4. SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

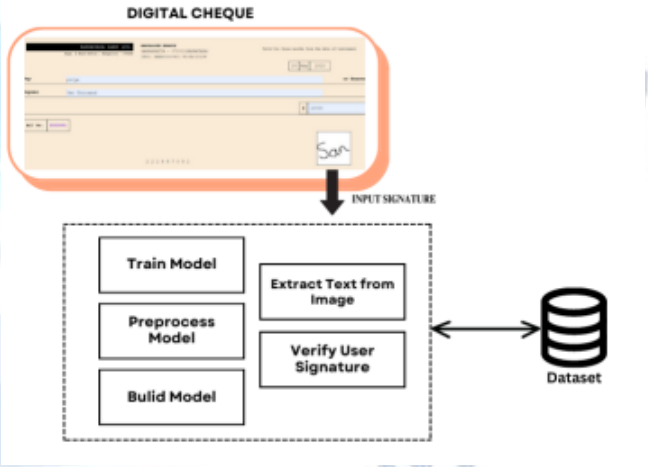

Fig. 1. Flowchart of proposed Model

5. SYSTEM IMPLEMENTATION MODULES

1. **User Authentication Module:**

This module handles user authentication for system access. It incorporates features such as username/password authentication and may include extra security measures such as multi-factor authentication to enable secure access to the digital cheque verification platform.

2. **Digital Cheque Creation Module:**

The Digital Cheque Creation Module enables users to safely create digital cheques. Users can provide payee information, set transaction amounts, and attach digital signatures. This module creates a digital version of a cheque, providing relevant information for the transaction.

3. **Deep Learning Signature Verification Module:**

The Deep Learning Signature Validation Module is fundamental to the system. This module includes a pre-trained deep learning model specifically suited for signature verification. It accepts digital signatures linked to digital cheques as input, runs them via the trained model, and returns a verification result confirming the legitimacy of the signature.

4. **Transaction Processing and Clearing Module:**

The Transaction Processing and Clearing Module manages the full process of digital cheques. It incorporates signature verification findings and makes valid transactions safer to process and clear. This module may feature interactions with financial systems to guarantee a smooth transaction flow.

5. **User Interface and Reporting Module:**

The User Interface and Reporting Module provide a user-friendly interface via which users may interact with the system. It enables users to generate digital checks, see transaction histories, and access important account information. Furthermore, this module may create reports on the status of transactions, including data about verified signatures and any flagged or rejected transactions.

These components work together to form a comprehensive system that handles user identification, digital cheque production, signature verification with deep learning, transaction processing, and user interaction. Not only does the modular approach improve the system's maintainability and scalability, but it also makes diagnosing and updating individual components easier.

6. RESULTS AND DISCUSSION

Login page

As shown in Figure 4, a login page is a page or screen that confirms a user's identity and grants access to a service or location that is only accessible to authorized users. The user must input a legitimate email address in the designated box. In order to log in, the user must have previously registered with the same email address. When the user enters a valid email address, they will receive an OTP. The user will be sent to the home page after submitting a valid OTP.

Register page

A registration page is a webpage that allows visitors to register or establish an account for the online application shown in Figure 5. After entering the required information, the user may submit the form to establish their account and gain access to the system.

Write cheque page

Figure 6 depicts the system's key component, the cheque interface. The interface is designed to seem like a cheque, as are typical offline checks. The user must input all of the essential information in the designated field, including the bearer's name and the sanctioned amount in both words and figures. After entering all of the required information, the user must use a mouse to sign the available area with a valid signature before hitting the "send" button. After checking the signature, the system will display the findings.

Cheque Authentication Success page

Only if the user's input signature is valid will this page be displayed. The user's name and the amount paid in.

Fig 2. Registering User

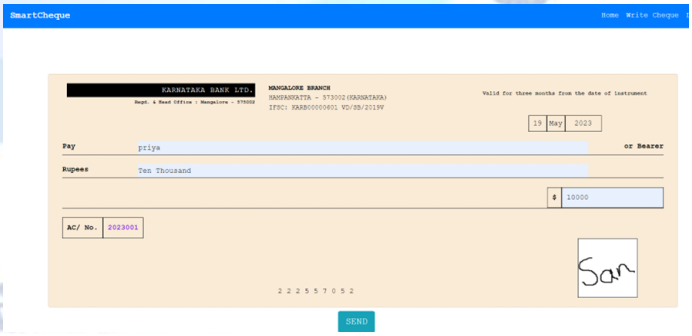

Fig 3. Cheque validation

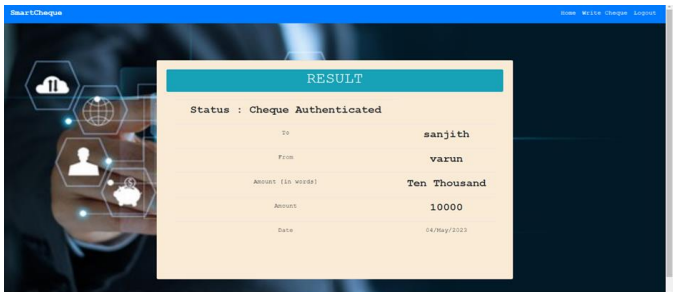

Fig 4. Check validation

7. CONCLUSION AND FUTURE WORK

The proposed deep learning-based online digital cheque clearance has the potential to significantly improve the speed and accuracy of the cheque processing system. Banks and other financial organizations may automate the process by utilizing deep learning algorithms, eliminating the need for manual involvement and reducing the likelihood of errors. Furthermore, providing an extra layer of protection to financial transactions increases fraud detection. Nonetheless, there are a few flaws that will need to be addressed in future development. One of the most pressing difficulties is developing deep learning models capable of handling a broad range of cheque types and handwriting styles. Another problem is to ensure that the models are accurate when recognizing and classifying the various components of a cheque. Furthermore, the success of online digital cheque clearance using 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 may be on developing a consistent check format that deep learning models can readily detect and interpret.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

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