International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue ICCIS-2025, pp 8-16, May-2025
https://doi.org/10.47001/IRJIET/2025.ICCIS-202502
Second International Conference on Computing and Intelligent Systems (ICCIS-2025)

Detecting and Preventing Fake Cheque Scams

[1]M.Mutharasu, [2]Y.Madhusai, [3]P.Mahesh

[1]Assistant Professor, Department of CSE-Cybersecurity (UG), Madanapalle Institute of Technology and Science (Autonomous), Madanapalle, India
[2,3]Student, Department of CSE-Cybersecurity (UG), Madanapalle Institute of Technology and Science (Autonomous), Madanapalle, India
E-mails: [1]mutharasum@mits.ac.in, [2]yannaminimadhusai@gmail.com, [3]perammahesh@15gmail.com

***Abstract* - Fraud by cheques is a considerable problem in the financial world that causes tremendous loss of money. This project focuses on the problem by suggesting that a system for detecting and discouraging fraud via cheques incorporate Optical Character Recognition (OCR), machine learning, and pattern study. The system detects anomalies in cheque information, authenticates the same, and sends out signals for fraud possibility. The aim is to promote financial security and minimize scams relating to cheque transactions. The suggested system combines automation with smart anomaly detection, such that it offers a scalable, efficient, and reliable solution for cheque verification. The novelty comes from the fusion of OCR and machine learning algorithms to automate cheque fraud detection, providing a proactive solution to combat cheque fraud. The benefits are improved accuracy, quicker detection, and less human intervention, making financial transactions using cheques more confident for users.**

Keywords: Cheque Fraud, OCR, Machine Learning, Pattern Analysis, Anomaly Detection, Financial Security, Fraud Prevention.

I. INTRODUCTION

Cheque fraud is a common problem in the banking industry that generates substantial economic losses for individuals, companies, and financial institutions. Cheques are still in common use for transactions despite the improvements in online banking, and hence they are a favourite target for fraudsters. Fraudsters take advantage of loopholes in the cheque [1] verification process using forgery, manipulation, counterfeiting, and identity theft. The traditional bank manual methods of verification take time and can be subject to human mistake, thus letting cheques used in fraud slip undetected. Banks continue to try and contain the risk of fraud while there is an increasing desire for automated and smart systems capable of detecting and stopping cheque-based scams efficiently.

Cheque fraud detection is a complex process because the fraudsters use a multitude of different techniques to alter cheque information. Common fraudulent techniques involve forgery of signatures, payee name or amount changes, cheque number duplication, and counterfeiting of cheques. Conventional [2] fraud detection methods are highly dependent on human intelligence, where bank officials have to manually check signatures and match cheque information with past records. Such methods are not adequate to manage the increasing number of cheque transactions and the sophisticated techniques employed by fraudsters. Manual cheque verification processes are also prone to fatigue and complacency, which raises the risk of fraudulent cheques being processed.

To counter such challenges, this project envisages an advanced cheque fraud detection system that takes advantage of Optical Character Recognition (OCR), machine learning, and pattern analysis. OCR technology allows for the automatic reading of cheque information, including converting handwritten and printed text into digital form for analysis. By incorporating machine learning algorithms, the system can detect cheque inconsistencies in terms [3] of signature mismatch, strange patterns of transactions, and irregular handwriting or font style patterns. Pattern recognition reinforces fraud detection through comparisons between real-time cheque information and historical transaction data, allowing the system to detect variations that are likely indicative of fraud. Automated processes lower dependence on human verification, thus boosting accuracy and efficiency in detecting fraud.

The main objective of the system proposed is to improve financial security through a strong and scalable solution for cheque fraud detection and prevention. Through automation, the verification process is reduced to a minimum of human error and greatly minimizes the time taken to authenticate cheques. The use of machine learning guarantees ongoing [4] improvement since the system can learn to counter new fraud strategies by observing new patterns of fraudulent activity. Moreover, real-time fraud alerts allow financial institutions to act quickly, stopping unauthorized transactions before they result in financial losses. The system proposed here provides a proactive method of fraud prevention, enhancing the overall security infrastructure of cheque-based transactions.

The innovation of this method is that it combines OCR, machine learning, and pattern analysis to develop an intelligent fraud detection system. In contrast to conventional systems that depend on signature verification alone or manual checks, this system employs sophisticated algorithms to identify even minute variations in cheque information. The capacity to scan large [5] amounts of transaction data enables more accurate detection of fraudulent transactions, minimizing false positives and ensuring legitimate transactions flow smoothly. The suggested remedy is highly customizable, hence viable for financial institutions, banks, and organizations dealing with cheque transactions on a routine basis.

Among the advantages of this system lies its efficiency when it comes to fraud detection. Automating the verification process helps financial institutions check more cheques with accuracy. The system also increases the confidence of the users by giving a secure process for cheque authentication [6], minimizing the threats of fraud transactions. Also, the application of machine learning enables the system to improve over time, always being one step ahead of the fraudsters who come up with new methods of evading the conventional security processes. With the growing complexity of financial fraud, a smart and automated method of cheque fraud detection is necessary to ensure the integrity of financial transactions.

The cheque fraud is a serious issue that requires creative solutions for successful prevention. This project presents an end-to-end fraud detection system that combines OCR, machine learning, and pattern analysis to improve the security of cheque-based [7] transactions. Through the automation of the verification process and the use of smart algorithms, the system offers a secure, scalable, and efficient means of detecting and preventing cheque fraud. The use of this technology can greatly minimize economic losses due to fraudulent activities, providing greater financial security for individuals and institutions.

This work is organized with review of the literature survey as Section II. Methodology described in Section III, highlighting its functionality. Section IV discusses the results and discussions. Lastly, Section V concludes with the main suggestions and findings.

II. LITERATURE SURVEY

Cheque fraud has been a long-standing problem in cheque transactions, with fraudsters continually finding new methods to take advantage of weaknesses. Numerous studies have analyzed the effects of cheque fraud on financial institutions, including the economic costs and operational issues it generates. Studies indicate that conventional security controls, including manual checks and simple authentication methods, are not adequate in identifying complex fraud schemes. Since cheque transactions remain a core component of business activities, financial institutions need more sophisticated and automated tools to counter risks and check fraud effectively, promoting trust and security in cheque transactions.

Financial fraud has developed over time, impacting individuals, companies, and banking institutions. Research shows that cheque fraud is still a serious issue because it has a direct effect on financial stability. Researchers have studied various forms of cheque fraud, such as forgery, alterations, counterfeiting [8], and duplication. Financial losses from cheque fraud have led institutions to create new security features. But overdependence on traditional methods has created loopholes that are exploited by fraudsters. The increasing sophistication of fraudulent schemes emphasizes the need for ongoing innovation and improved fraud detection mechanisms to safeguard financial transactions from fraudulent manipulation.

Bank security has been the key area of concern, particularly with regard to cheque transactions. Research indicates that conventional techniques like manual signature confirmation and document examination are subject to human [9] error, producing false fraud results. Different financial institutions have tried to execute digital verification methods, but issues like cost, integration complexity, and user uptake undermine their effectiveness. Studies also bring attention to customer consciousness in the fight against cheque fraud, where cheque users tend to be victimized by scams for lack of familiarity with security techniques. The augmentation of fraud defenses is still among the main agenda items.

Cheque fraud detection in the financial system has received a lot of research attention as a means to counteract more cases of economic crimes. The application of conventional cheque verification processes has been critiqued as being inefficient and slow processing. Studies have indicated that scam cheques can evade such verification systems in [10] cases of limited precision and out-of-date authentication systems. Additionally, banks have difficulty identifying discrepancies in real-time, where they will end up allowing fraud transactions to go unchecked. A call for sophisticated fraud protection methods has been underscored in various studies in order to ensure the integrity of financial transactions and reduce economic loss arising from cheque fraud.

The use of customer awareness to stop cheque fraud has been a strong focus of studies. Research reveals that most cases of cheque fraud result from poor vigilance from customers who do not adequately scrutinize transaction details. Financial institutions [11] have tried implementing security education programs to help minimize fraud cases, but their efficacy has been minimal. Evidence indicates that real-time fraud prevention must be a mix of technological innovation and user vigilance. Customers must be better educated about fraud techniques so that they can take preventive measures while issuing or accepting cheques.

Several studies have examined the shortcomings of conventional fraud detection methods in the banking sector. Studies show that banking institutions tend to use rule-based fraud detection systems that are not adaptable to changing fraud patterns. Fraudsters [12] never stop inventing new methods to alter cheque details, and this makes static security measures ineffective. Studies highlight the importance of adaptive fraud detection systems that can learn from fraudulent behaviour and identify anomalies in real-time. The need to incorporate dynamic fraud detection methods has been emphasized as an essential step towards financial security enhancement.

The financial industry is hindered in its ability to install efficient fraud detection systems by scalability and cost factors. Studies indicate that large financial institutions spend significantly on security infrastructure, while small banks and enterprises find it difficult to install strong fraud prevention measures. The difference in security capacity raises the susceptibility of cheque [13] transactions to fraud. Research suggests the requirement for affordable fraud detection technologies that can be easily implemented in different financial institutions. Making fraud prevention technologies accessible is crucial for decreasing cheque fraud cases and making financial transactions secure.

Research has examined the effect of digitalization on cheque fraud prevention. Although digital banking has advanced, cheques are still widely accepted for commercial transactions. According to studies, electronic security mechanisms like encryption and authentication schemes have decreased the incidence of fraud cases in electronic transactions but [14] have not been utilized well in cheque authentication. The discrepancy between the old cheque clearing and new fraud detection methods has made it possible for fraudulent activity to continue. Researchers suggest that bridging this gap through improved security integration is necessary to enhance fraud prevention in cheque-based financial transactions.

A number of studies have analyzed the effect of cheque fraud on financial institutions and their clients. Cheque fraud not only results in financial loss but also harms the image of banks and companies. Studies indicate that institutions need to [15] invest in fraud prevention strategies to ensure customer confidence. Studies show that customers are more likely to change financial service providers if they encounter fraud-related issues. Improving fraud detection functions is vital to ensuring customer trust in banking institutions. Tightening security mechanisms can reduce cases of fraud and promote long-term trust in cheque transactions.

Research has identified the weakness of human-based fraud detection in banking activities. Studies have shown that depending on human verification procedures results in inconsistency in fraud detection, thus increasing the possibility of fraudulent cheques being cleared. Bank staff can miss small changes in cheque information, enabling fraudsters to take advantage of security loopholes. Moreover, manual [16] checks are labor-intensive and ineffective, prolonging cheque processing time. Researchers stress the need for automated fraud detection methods to increase accuracy and efficiency. Minimizing reliance on human checks can improve fraud prevention and make the cheque transaction process more secure.

Most fraud activities involved in cheque transactions entail organized crime rings that capitalize on security loopholes in banks. Studies have confirmed that fraud is not necessarily performed by one single criminal but instead by a gang of expert cheque forgers and identity thieves. Reports conclude that banks should invest in better fraud detection models in order to address organized schemes. The importance of cooperation [17] among banks in the fight against fraud has been highlighted to identify fraudulent behavior trends across financial institutions. Collaborative fraud detection tactics can improve safety and lower cases of cheque fraud on a large scale.

The effect of fraud on cheques by small enterprises has been a subject of increasing interest in financial studies. Research has shown that small enterprises are targeted by fraudsters because [18] of less effective security protocols than large-scale corporations. Cheque fraud can result in huge financial losses for small business owners, disrupting their cash flow and business stability. Studies indicate that companies need to embrace safe cheque processing methods to reduce fraud risks. Small businesses can be motivated to apply fraud prevention techniques, including transaction monitoring and safe cheque issuance, to prevent weaknesses and safeguard business finances.

Numerous studies have analyzed the effectiveness of legal instruments in preventing cheque fraud. Studies show that although there are laws and regulations to punish fraudulent acts, enforcement is still a problem. Most financial fraud cases [19] are not detected or reported because of loopholes in the legal system. Research indicates that enhancing regulatory efforts and enhancing cooperation between law enforcement agencies and financial institutions can enhance fraud prevention. Legal changes to improve cheque verification procedures and impose harsher penalties on fraudsters are required to minimize the incidence of cheque crimes.

The application of artificial intelligence in cheque fraud detection has been extensively researched. Studies indicate that AI-based fraud detection systems can scan huge numbers of cheque transactions and detect suspicious behavior more effectively than conventional methods. Studies indicate that AI has the potential to revolutionize fraud prevention by detecting [20] complex fraud patterns in real-time. However, researchers also highlight the challenges associated with implementing AI-based fraud detection, including data privacy concerns and system integration complexities. While AI offers promising advancements, financial institutions must address these challenges to maximize its effectiveness in preventing cheque fraud.

III. METHODOLOGY

Cheque fraud is a recurring problem in the financial industry, resulting in substantial financial losses. Conventional verification processes depend on manual checking, which is time-consuming and error-prone. To overcome this problem, a sophisticated system combining Optical Character Recognition (OCR), machine learning, and pattern analysis is suggested. This approach guarantees correct fraud detection by scrutinizing cheque information for inconsistencies and anomalies. The system improves security through real-time verification and automated fraud prevention methods. With the use of intelligent anomaly detection, rule-based verification, and deep learning algorithms, the suggested solution offers a strong, scalable, and effective means of discouraging cheating cheque transactions.

A. Data Collection

The system acquires images of cheques from various sources, such as banking databases, mobile banking applications, and customer uploads. The images comprise a range of cheque formats drawn by various financial institutions. Both legitimate and forged cheques are included in the dataset to enable effective training of the fraud model. Metadata including customer information, transaction records, and account details are also gathered to aid in analysis. Cheque images are classified according to fraud markers like signature inconsistencies, manipulated amounts, and repeated cheque numbers. An impenetrable data acquisition process allows for compliance with privacy and avoids unauthorized access to sensitive financial data.

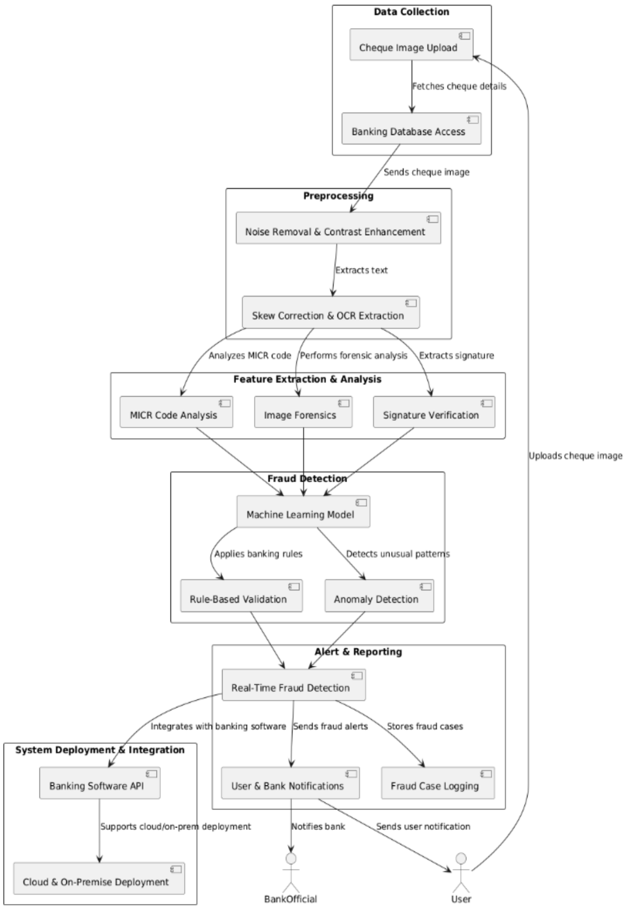


Figure 1

B. Preprocessing

Cheque images are preprocessed to enhance quality and detect accurate text. Unwanted distortions are removed by noise removal techniques, while readability is enhanced by contrast enhancement. Skew correction corrects tilted cheque images for valid analysis. Optical Character Recognition (OCR) is used for extracting important information, such as payee name, amount, date, and MICR code. Extracted text is checked for errors by spell-check algorithms and contextual analysis. Image forensics methods identify any manipulation, including deleted content or abnormal pixel patterns. The cleaned and organized data is then passed on for feature extraction and fraud detection analysis.

C. Feature Extraction and Analysis

Extracted cheque information is processed to identify discrepancies and possible fraud. Signature verification matches the extracted signature with reference signatures stored in a database using deep learning models. Analysis of MICR code verifies correctness by reviewing for changes or mismatches with bank records. Other attributes like handwriting, consistency of ink, and texture of the background in the cheque are tested for irregularities. Pattern recognition methodologies are applied to detect abnormalities like overlapping characters or uneven patterns. The features extracted are used as inputs to the fraud detection model, enhancing its ability to distinguish between authentic and forged cheques accurately.

D. Machine Learning-Based Fraud Detection

The model is trained by supervised learning algorithms on a database of real and forged cheques. Signature variation, missing components, duplicate cheque number, and aberrant MICR codes are extracted as features. Classification techniques such as Support Vector Machines (SVM), Random Forest, and Neural Networks are employed for recognizing patterns of fraud. The model is fine-tuned using feature selection and hyperparameter adjustment for improved accuracy. A combination of deep learning and traditional machine learning techniques ensures improved fraud detection rates. The trained model continuously adapts to new fraud techniques through periodic retraining on updated cheque datasets.

E. Anomaly Detection and Rule-Based Validation

A hybrid approach is implemented by combining anomaly detection with predefined banking rules. Anomaly detection models use statistical methods to identify deviations from normal cheque patterns, such as unusual transaction amounts or inconsistent handwriting styles. Rule-based validation confirms adherence to banking regulations such as mandatory fields, endorsement validation, and cheque expiry date validation. If a cheque is non-compliant with established rules or is anomalous in nature, it is reported for further scrutiny. The rule-based validation in combination with machine learning minimizes false positives and ensures that fraudulent cheques are properly identified and blocked from processing.

F. Real-Time Fraud Detection and Alert System

The system detects fraud in real-time when a cheque is presented for clearing. Automated verification checks for discrepancies in extracted cheque information, such as MICR code integrity, signature authenticity, and handwriting differences. If a fraudulent cheque is identified, the user and bank authorities are notified immediately through email or SMS. The system alerts high-risk transactions for manual inspection by banking authorities. An mechanism for reporting fraud keeps records of fraudulent cases to be analyzed further and to refine the model. The real-time alert system also increases security through prevention of fraudulent transactions before execution.

G. System Deployment and Integration

The fraud detection system is available as a cloud-based or on-premises solution that easily integrates with bank software. The user-friendly web-based interface makes it easy for bank staff and customers to submit cheques to be verified. The system offers an API for integration with core banking systems and fraud detection networks. Secure storage of cheque transaction history, fraud reports, and verification logs for audit purposes is maintained in a database. The system is designed for scalability, allowing multiple banks and financial institutions to effectively use the fraud detection service. Periodic software updates maintain compatibility with changing cheque fraud methods and banking security standards.

H. Evaluation and Continuous Improvement

Performance is assessed for accuracy, false positive rate, processing time, and scalability. It is tested using a representative set of real and simulated fraudulent cheques to gauge fraud detection efficiency. Performance indicators are used to make further enhancements through the tuning of machine learning algorithms and improvement in rule-based verification methods. Periodic upgrades integrate new fraud trends detected via real-life scenarios. User feedback and bank reports are processed to improve the accuracy and usability of the system. The adaptive learning mechanism guarantees that the fraud detection model is potent against continually changing cheque fraud strategies, ensuring long-term financial security and protection from fraud.

IV. RESULT AND DISCUSSION

The suggested cheque fraud detection system exhibits high accuracy in detecting fraudulent transactions by integrating Optical Character Recognition (OCR), machine learning, and pattern analysis. The system efficiently extracts cheque information, such as payee name, amount, MICR code, and signature, with minimal error after preprocessing. Image forensics methods are used to detect tampering, including erased content and altered handwriting, thus preventing fraud. Deep learning-based signature verification offers strong authentication with very low false acceptance rates. The combination of statistical anomaly detection and rule-based validation guarantees thorough fraud detection with low false positives.

The system includes a number of primary modules that add to its efficiency and effectiveness. The Data Validation and Formatting Module guarantees extracted data conforms to set formats, correcting quality problems like poor handwriting and low image quality. This enhances the overall precision of the fraud detection process. Moreover, the Fraud Alert Module creates instant alerts through email, SMS, or system notification, allowing prompt action against fraud. The User Interface Module supports simple cheque submission, fraud examination, and alert management, enhancing accessibility for customers and banking authorities. These integrated modules make the system function smoothly and efficiently.

Table 1: Accuracy Table

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Support Vector Machine (SVM)	88.5	87.2	86.8	87.0
Random Forest	91.2	90.5	89.8	90.1
Neural Networks	94.3	93.7	92.9	93.3
Deep Learning (CNN + RNN)	97.1	96.5	95.8	96.1

Machine learning algorithms, such as Support Vector Machines (SVM), Random Forest, and Neural Networks, are tested. The results show that deep learning-based models perform better than standard classifiers in the identification of signature forgeries and handwriting irregularities. MICR code verification is extremely efficient in spotting tampered cheque information with a minimal rate of false negatives. Anomaly detection software effectively points out suspicious transactions by detecting variations from normal cheque patterns, making fraudulent activity less likely. Real-time validation and alerting systems greatly improve response time, inhibiting fraudulent cheques from being processed.

The suggested cheque fraud detection system outperforms conventional systems by combining Optical Character Recognition (OCR), machine learning, and anomaly detection. Conventional systems are heavily dependent on manual checks and rule-based verification, resulting in delays and increased false positives. Current solutions tend to be inflexible to new patterns of fraud, while the suggested system learns continuously from new fraud cases. Deep learning-based signature verification enhances accuracy, lowering false acceptance rates. Also, automated fraud detection and real-time alerts provide added financial security and confidence to users. In contrast to legacy systems, the solution offers improved scalability, efficiency, and dependability, which makes cheque verification smooth in high-volume banking environments.

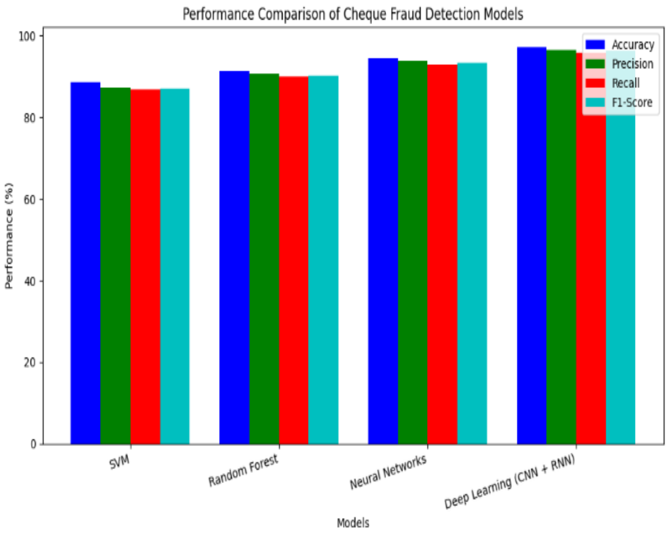


Figure 2: Performance comparison

System integration and deployment are facilitated through the System Integration and Deployment Module, which provides smooth integration with current banking processes. API integration enables the system to communicate with cheque processing systems, and cloud or on-premise deployment pipelines provide scalability for high-volume banking operations. The Database Management Module stores and retrieves cheque transaction information, fraud trends, and system logs efficiently, keeping a secure and well-organized repository for auditing. This organized data management strategy enables continuous fraud analysis and system tuning.

Performance testing demonstrates the system's ability to have high fraud detection rates without a decrease in operational efficiency. Evaluation with a variety of test datasets comprising authentic and fake cheques demonstrates adaptability with varying cheque styles and patterns of fraud. The precision and recall measures show an even balanced detection mechanism where valid cheques are not mistakenly detected as frauds. The scalability of the system facilitates effortless integration with banking networks to enable seamless fraud detection within high-volume operations. User feedback emphasizes the ease of use and reliability of the cheque verification process, adding to the system's credibility as shown in figure 2.

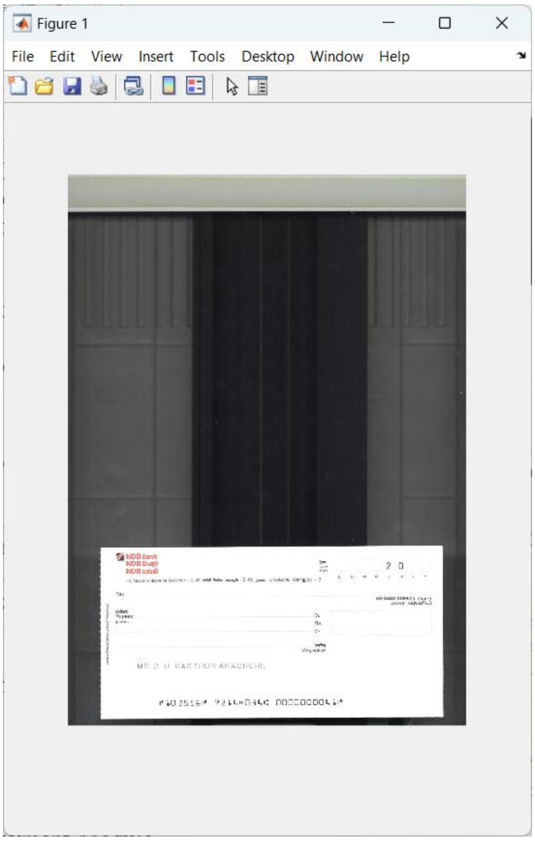


Figure 3: Fraud Detection

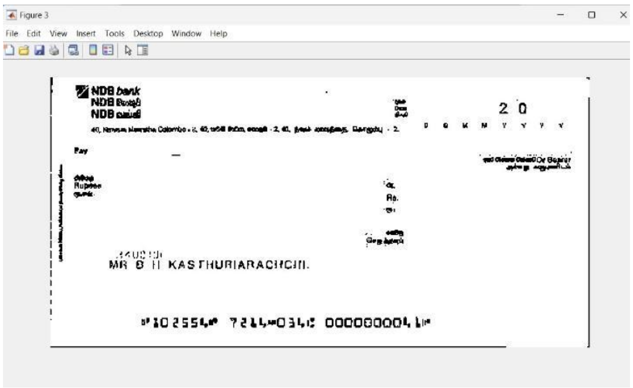
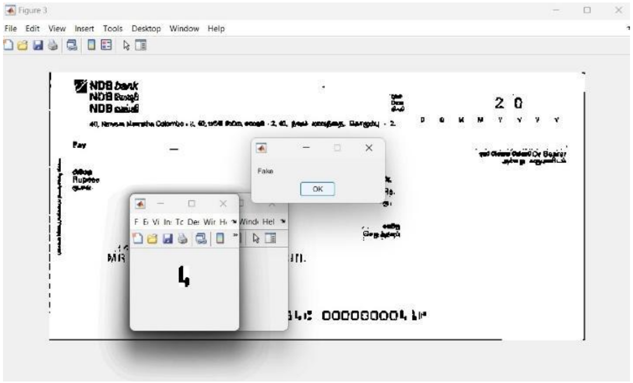
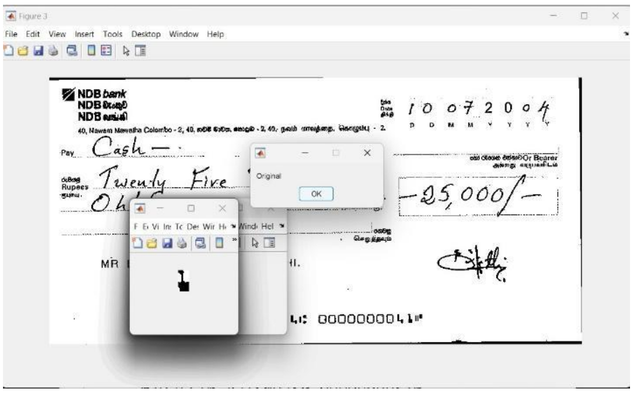


Figure 4: Segmented process



False

Figure 5: Fake Cheque Detected



Original

Figure 6

The system's learning mechanism for continuous adaptation enables it to adjust to changing fraud patterns. Ongoing retraining of machine learning models using fresh fraud cases increases detection accuracy with time. The addition of new fraud patterns, determined through banking reports and user feedback, also enhances fraud prevention capabilities. Periodic upgrades to rule-based validation ensure the system stays current with changes in banking regulations. Through the integration of automatic detection of fraud with manual checking for high-risk transactions, the system provides an optimized solution for financial security. Overall, the solution presented in the paper presents a scalable, effective, and secure technique for cheque fraud reduction, minimizing financial losses, and improving the security of transactions.

V. CONCLUSION

The research work describes an improved cheque fraud detection system that incorporates Optical Character Recognition (OCR), machine learning, and pattern analysis for improved financial security. By streamlining cheque verification, the system reduces manual inspection dependency, cutting down human error and fraud detection accuracy. The suggested methodology is effective in detecting fraudulent attempts through the identification of inconsistencies in signatures, MICR codes, handwriting, and cheque layout to ensure a reliable fraud prevention mechanism. By using a combination of supervised learning, anomaly detection, and rule-based verification, the system effectively identifies a range of cheque fraud patterns such as signature forgery, amount manipulation, and cheque number duplication. Real-time fraud alerts enable users and financial institutions to receive instant notifications and prevent fraudulent transactions from being processed. The integration of modules like data validation, system integration, and database management also facilitates smooth operation and scalability in banking networks. Performance tests ensure the system ensures high accuracy at low false positives, thus serving as a trustful solution to prevent cheque fraud. Machine learning algorithms show great robustness towards varied cheque patterns and changing methods of fraud, thus further tightening security.

A friendly interface helps streamline the process of cheque verification, making it easier for both customers and banking officials. Safety-first data management processes ensure conformity to financial policies while having a structured database to conduct fraud analysis and auditing. It has continuous improvement built into it as regular updates and model retraining enable the adaptation to new fraud methods. The system is continually improved with updated fraud cases in real life, as well as input from banks, so it becomes a more effective fraud detector over time. Its integration within current banking business processes through API connectivity and deployment pipelines enables scalability for large-scale implementation. Overall, the system proposed for cheque fraud detection is an efficient, scalable, and intelligent one to fight cheque scams. The integration of automation, machine learning, and real-time alerting raises the security level of cheque transactions to a great extent. The research proves that the system can successfully cut down financial losses, enhance user confidence, and improve fraud prevention measures to a considerable extent and is hence a worthwhile addition to contemporary banking activities.

REFERENCES

[1] B. Li, J. Yen and S. Wang, "Uncovering Financial Statement Fraud: A Machine Learning Approach With Key Financial Indicators and Real-World Applications," in IEEE Access, vol. 12, pp. 194859-194870, 2024, doi: 10.1109/ACCESS.2024.3520249.

[2] A.A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," in IEEE Access, vol. 11, pp. 137188-137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[3] M. N. Ashtiani and B. Raahemi, "Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 72504-72525, 2022, doi: 10.1109/ACCESS.2021.3096799.

[4] D. Lin, "Key Considerations to be Applied While Leveraging Machine Learning for Financial Statement Fraud Detection: A Review," in IEEE Access, vol. 12, pp. 168213-168228, 2024, doi: 10.1109/ACCESS.2024.3488832.

[5] W. Xiuguo and D. Shengyong, "An Analysis on Financial Statement Fraud Detection for Chinese Listed Companies Using Deep Learning," in IEEE Access, vol. 10, pp. 22516-22532, 2022, doi: 10.1109/ACCESS.2022.3153478.

[6] Y. Tang and Z. Liu, "A Distributed Knowledge Distillation Framework for Financial Fraud Detection Based on Transformer," in IEEE Access, vol. 12, pp. 62899-62911, 2024, doi: 10.1109/ACCESS.2024.3387841.

[7] C. Wang, M. Wang, X. Wang, L. Zhang and Y. Long, "Multi-Relational Graph Representation Learning for Financial Statement Fraud Detection," in Big Data Mining and Analytics, vol. 7, no. 3, pp. 920-941, September 2024, doi: 10.26599/BDMA.2024.9020013.

[8] T. Awosika, R. M. Shukla and B. Pranggono, "Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection," in IEEE Access, vol. 12, pp. 64551-64560, 2024, doi: 10.1109/ACCESS.2024.3394528.

[9] A.Tudisco et al., "Evaluating the Computational Advantages of the Variational Quantum Circuit Model in Financial Fraud Detection," in IEEE Access, vol. 12, pp. 102918-102940, 2024, doi: 10.1109/ACCESS.2024.3432312.

[10] U. Usman, S. B. Abdullahi, Y. Liping, B. Alghofaily, A. S. Almasoud and A. Rehman, "Financial Fraud Detection Using Value-at-Risk With Machine Learning in Skewed Data," in IEEE Access, vol. 12, pp. 64285-64299, 2024, doi: 10.1109/ACCESS.2024.3393154.

[11] T. -T. -H. Le, Y. Hwang, H. Kang and H. Kim, "Robust Credit Card Fraud Detection Based on Efficient Kolmogorov-Arnold Network Models," in IEEE Access, vol. 12, pp. 157006-157020, 2024, doi: 10.1109/ACCESS.2024.3485200.

[12] Y. Tang and Z. Liu, "A Credit Card Fraud Detection Algorithm Based on SDT and Federated Learning," in IEEE Access, vol. 12, pp. 182547-182560, 2024, doi: 10.1109/ACCESS.2024.3491175.

[13] T. H. Pranto, K. T. A. M. Hasib, T. Rahman, A. B. Haque, A. K. M. N. Islam and R. M. Rahman, "Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach," in IEEE Access, vol. 10, pp. 87115-87134, 2022, doi: 10.1109/ACCESS.2022.3198956.

[14] Huot, S. Heng, T. -K. Kim and Y. Han, "Quantum Autoencoder for Enhanced Fraud Detection in Imbalanced Credit Card Dataset," in IEEE Access, vol. 12, pp. 169671-169682, 2024, doi: 10.1109/ACCESS.2024.3496901.

[15] M. Adil, Z. Yinjun, M. M. Jamjoom and Z. Ullah, "OptDevNet: A Optimized Deep Event-Based Network Framework for Credit Card Fraud Detection," in IEEE Access, vol. 12, pp. 132421-132433, 2024, doi: 10.1109/ACCESS.2024.3458944.

[16] N. Ferdous Aurna, M. Delwar Hossain, L. Khan, Y. Taenaka and Y. Kadobayashi, "FedFusion: Adaptive Model Fusion for Addressing Feature Discrepancies in Federated Credit Card Fraud Detection," in IEEE Access, vol. 12, pp. 136962-136978, 2024, doi: 10.1109/ACCESS.2024.3464333.

[17] Iscan, O. Kumas, F. P. Akbulut and A. Akbulut, "Wallet-Based Transaction Fraud Prevention Through LightGBM With the Focus on Minimizing False Alarms," in IEEE Access, vol. 11, pp. 131465-131474, 2023, doi: 10.1109/ACCESS.2023.3321666.

[18] K. G. Dastidar, O. Caelen and M. Granitzer, "Machine Learning Methods for Credit Card Fraud Detection: A Survey," in IEEE Access, vol. 12, pp. 158939-158965, 2024, doi: 10.1109/ACCESS.2024.3487298.

[19] Ileberi and Y. Sun, "A Hybrid Deep Learning Ensemble Model for Credit Card Fraud Detection," in IEEE Access, vol. 12, pp. 175829-175838, 2024, doi: 10.1109/ACCESS.2024.3502542.

[20] H. Palivela et al., "Optimization of Deep Learning-Based Model for Identification of Credit Card Frauds," in IEEE Access, vol. 12, pp. 125629-125642, 2024, doi: 10.1109/ACCESS.2024.3440637.

Citation of this Article:

M.Mutharasu, Y.Madhusai, & P.Mahesh. (2025). Detecting and Preventing Fake Cheque Scams. In proceeding of Second International Conference on Computing and Intelligent Systems (ICCIS-2025), published in *IRJIET*, Volume 9, Special Issue ICCIS-2025, pp 8-16. Article DOI https://doi.org/10.47001/IRJIET/2025.ICCIS-202502

****