International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-Jun-2026, ISSN (Online): 2395-566X

# Deep Learning and Image Processing-Based Bank Check Verification System

**Marella Maheswari[1], P ASHOKA[2]**
[1]Student, Department of CSE, MAM Women's Engineering College, kesanupalli (Narasaraopeta).
[2]Assistant Professor, Department of CSE, MAM Women's Engineering College, kesanupalli (Narasaraopeta)

**Abstract- Revolutionizing the verification of bank checks, this innovative technology simplifies the process by integrating deep learning, image processing, and an intuitive Django-based web interface. It streamlines the process with little human participation, making it easier than ever before. Our Convolutional neural network (CNN) trained on the IDRBT check dataset and executed in PyTorch has a 99.14% success rate in recognizing handwritten digits, as shown in the introductory article. Adaptive thresholding and Gaussian blurring are implemented in the source code to enhance the picture preparation. The optical character recognition (OCR) in MATLAB can recover machine-printed text with 97.7 percent accuracy, including IFSC codes and account numbers, when Pytesseract is used in the code for region-based text extraction. The approach uses SVM classification and SIFT feature extraction for real-time authenticity checks, allowing signature verification powered by SIFT and SVM to reach 98.1% accuracy. The web-based interface allows more users to upload photos of checks, train models, see datasets, and get immediate categorization results ("Genuine" or "Not Genuine"). The system complies with CTS-2010 standards for Indian banks and the extraction of critical details such as signatures, amounts, and check numbers is possible even if it supports formats from other countries. In order to automate the verification process and decrease processing time, operational expenditures, and fraud risks, it makes use of contour detection and region-based analysis. This scalable solution sets a new standard for secure, efficient financial transactions by combining the rigors approach from the paper with the actual code implementation. Future versions may support more than one language and format.**

**Keywords- Bank Check Verification, Automated Cheque Processing, Deep Learning, Convolutional Neural Network (CNN), Image Processing, Django Web Interface.**

## I. INTRODUCTION

Bank checks are still an important part of international money transfers, even if electronic payments are becoming more common. Even if online purchases are growing increasingly common, this is still true. However, these tests are tedious, costly, error-prone, and time-consuming to complete manually by humans. In addition, mistakes are possible. In addition, this comes with its own set of hazards. On top of that, it improves the odds of finding and fixing mistakes. Therefore, academics have been motivated to explore this potentially fruitful area of research due to the introduction of automated bank cherub processing systems. Attribution to one of the aforementioned factors is possible. Computer vision, image processing, pattern recognition, machine learning, and deep learning are some of the fundamental disciplines for automating bank check processing. Steps in the process include collecting photos, processing them, extracting them, and then recognizing them. By integrating image processing with deep learning methods, crucial features such as bank branch codes, check numbers, precise amounts, account numbers, and signature patterns may be located and validated. Machine learning algorithms could be able to spot fraudulent financial transactions with relative ease. Modern algorithms like the Generative Adversarial Network (GAN) can analyze scanned images of checks for different traits that might help detect likely counterfeit items in real time. Studies on truncation techniques have also used AI and machine learning.

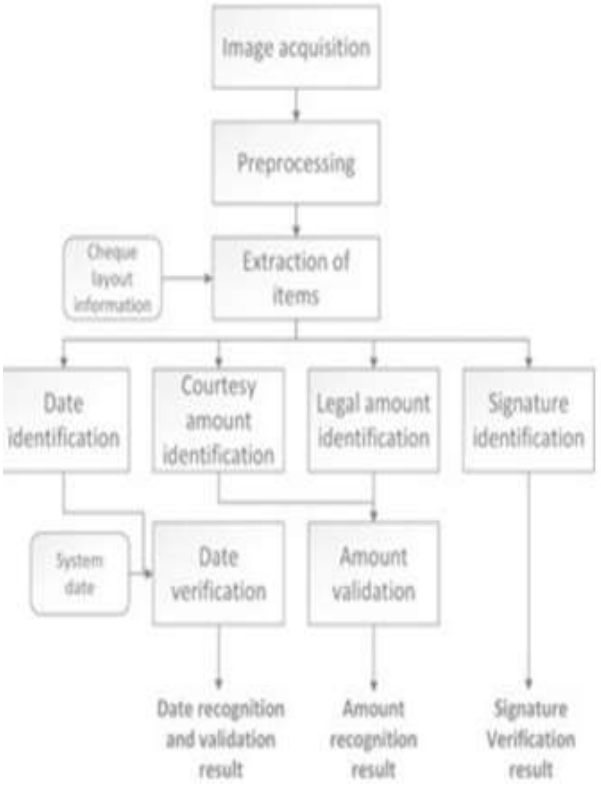
The Cheque Truncation System (CTS) uses a two-step verification mechanism to guarantee that checks have passed clearance. Verifying the authenticity of the check booklet should be your first step, as suggested by Deepak and colleagues (2010). The next step is to review the data presented in the brochure. This article highlights several novel methods for automated bank check verification, such as obtaining the issuer's signature, legal amounts, courtesy amounts, account numbers, check numbers, and IFSC codes. Bounding boxes are used to show the obtained features for validation reasons. Approaches for recognizing, authenticating, and confirming bank checks have been examined by several researchers [1, 2], however their success is poor. Optical character recognition (OCR) is a method that automatically identifies text in photographs, whether it is handwritten or machine-printed letters and numbers. Enhancement, compression, segmentation, and editing are all aspects of digital pictures that

are analyzed in image processing. Various steps are involved in processing images, such as acquiring, preprocessing, segmenting, interpreting, and recognizing. When it comes to pattern recognition in photos, CNNs with more layers really shine. Reducing the time and resources needed for banks' cheque clearing operations, Convolutional Neural Networks efficiently execute math on massive datasets. The study conducted with the help of MATLAB-2018a. Finding better ways to verify bank checks and using image processing and deep learning to make automated verification more accurate are the main goals of this study. Providing an overview of the main findings: Extracting data from scanned bank checks, including the date, account number, and check itself, by using image segmentation techniques.

Certain numerical values using a CNN and comparing them to the transformed data of legal amounts using the suggested approach. In comparison to previous methods, this study's curated bank cheque verification strategy was shown to be more efficient. Automating the process of verifying bank checks is suggested in the study via the use of image processing and deep learning. By using OCR, CNN, SIFT, and SVM technologies to extract critical data from check leaflets, the suggested model enhances accuracy and efficiency. Research that automates check clearing and speeds up processing is beneficial to the banking industry. An important part of this research is that it might make financial transactions more efficient, which would save money and time and lessen the likelihood of check fraud. By discussing the ongoing problems in the industry and offering a practical approach to studying them, this study offers a great foundation for further studies on the subject. It offers a thorough evaluation of many models along with their individual accuracy rates in payee name recognition, date recognition, digit identification, and signature detection.

## II. RELATEDWORKS

In order for a blank check to be authenticated, a number of steps must be followed precisely. After the IFSC code is authenticated, the system checks the check number to make sure it comes from the account holder's authorized set of cheque booklets.




The next step is to compare the customer's account balance with the amount and signature(s) of the check's issuer. Please complete these necessary verifications quickly and accurately since they are integral to the check clearing process, which includes all phases, including withdrawals and transfers. Several interrelated and vital processes make up the check clearance procedure. Information from the check booklet may be retrieved using a number of reliable and efficient techniques.

The accuracy of optical character recognition (OCR) makes it a useful tool for deciphering machine-printed text. While this is going on, CNNs powered by deep learning process both numerical data and handwritten text. In order to verify signatures, SIFT extracts features, and then SVM sorts them for efficiency gains. Since these methods work best with clean images, picture segmentation is essential for gleaning useful details. Section A: Acquiring Images Before the scanned image(s) could be immediately employed in image processing operations, they needed to undergo pre-processing steps. The purpose of these processes was to prepare the image(s) for further processing. Part B: Pre-processing Images a scanned copy of the check was used for our investigation. Preprocessing

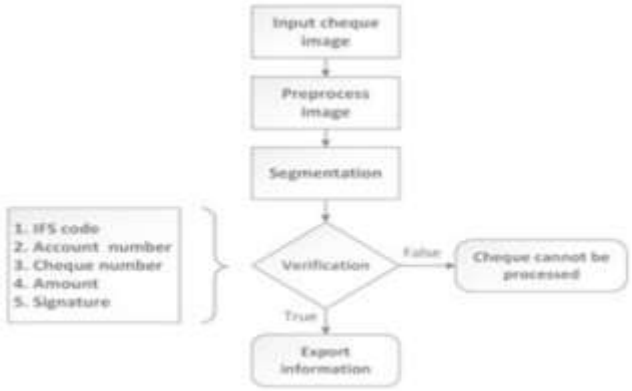
was necessary before the scanned photos could be used. Rotating the picture and then removing unnecessary background data are the initial steps in implementing this strategy. To rotate the scanned photo, we used the "Date Box," which is a common component of all bank checks. The precision of parameter identification was further enhanced when we eliminated extraneous information and background noise. The overall validity and reliability of the verification depends on these preprocessing processes.

## III. PROPOSEDMODEL

The date field, which is often seen on normal check books, was used to rotate the scanned photos. The date box's location was determined via contour extraction, which then served as a point of reference for rotation. • The date box's location in the image's centre quadrant served as the basis for the rotation angle, and the image's centre was used as the rotation point. • The noise in the scanned photos was eliminated by measuring the date box and then using length mapping to get the check's range. Figure 7: Block diagram depicting the process of verifying bank checks • A predetermined formula was used to convert the RGB picture to a monochrome grayscale image. •

The noise in the grayscale picture was removed using Gaussian filtering, which makes use of a 2D Gaussian function with a defined standard deviation. To enhance the image, morphological operations such as erosion and dilation were carried out. First, the equation for a 2-dimensional Gaussian function is G(x, y) = 1/2πσ2 × e − x 2+y 2/2σ2. A normal value arrangement is represented here by G(x, y). On the other hand, σ is used to represent the standard deviation of the arrangement. We made use of the binary image format to precisely and reliably extract outlines from the grayscale picture. To put it simply, after converting the image to binary format, we used the following procedure to discover the boundary points of the region: f(I, j − 1) = 0 f(i, j) = 1 f(i, j) > 1 f(i, j + 1) = 0 Two functions, f(i, j − 1) and f(i, j + 1), provide the pixel values of neighboring points for f(i, j), whereas the binary image function f(i, j) provides the pixel value of the necessary point in this equation. Division (C.)

The relevant portions of the check documents were located and crucial data was isolated using image segmentation. This enabled processing of the required data while still gaining access to the whole method. The proportions of RBI are used to segment both the contour extraction and the standard templates. It was possible to decipher typographic letters and numbers written by hand using a combination of transfer learning and optical character recognition. For the purpose of signature verification, SIFT extracted features and SVM assigned classes to them. Size, national, or bank standard deviation checks during semi-automatic segmentation required operator involvement.




The formula for 2-D Gaussian function is

$$G(x,y) = \frac{1}{2\pi\sigma^2} \times e^{-\frac{x^2+y^2}{2\sigma^2}} \quad (1)$$

In this case, the typical arrangement of the values is denoted by $G(x, y)$. In contrast, the arrangement's standard deviation is denoted by $\sigma$.

To accurately and precisely extract contours from the grayscale image, we utilized the binary image format. Put simply, we used the algorithm stated below to find the region's border points after converting the picture to binary representation :

$$\begin{cases} f(i,j-1) = 0 \\ f(i,j) = 1 \\ f(i,j) \geq 1 \\ f(i,j+1) = 0 \end{cases} \quad (2)$$

The binary image function $f(i, j)$ gives the pixel value of the needed point in this equation, whereas the functions $f(i, j - 1)$ and $f(i, j + 1)$ give the pixel values of the nearby points for$f(i, j)$.

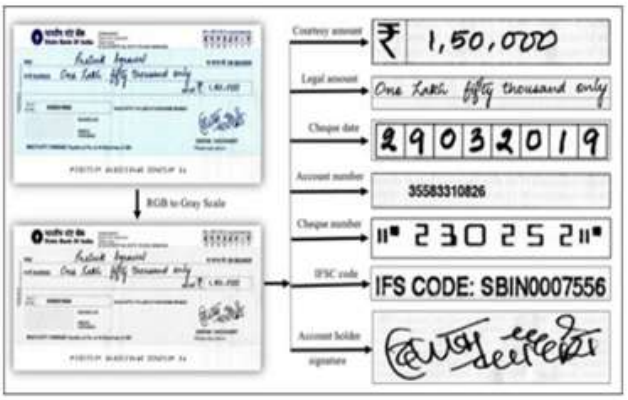



Fig. CNN architecture proposed for recognizing handwritten digits in courteous amount

D. A model for identifying courtesy amounts and legal matters using CNN For this research, we used a CNN to decipher the handwritten courtesy amount and turn it into a string. The CNN was constructed using MATLAB's Deep Learning Toolbox. It has two convolution layers with max pooling. For the purpose of training and assessment, MNIST was used for digit identification, whereas EMNIST was used for English letter recognition. We trained on 80% of these datasets and tested on 20%. Following the detection of characters and numbers by a CNN, we proceeded to sort numerical digits using the Indian Place Value (IPV) approach. To account for differences in the sequence of numbers written by hand, we used transfer learning. For the purpose of making a comparison to the permitted amount, we transformed the numerical value into text. A dictionary function was used to validate both string values. Consistent string checking was carried out. Checking the check's accuracy and legitimacy was done by comparing the legal number to the textual amount. Keep in mind that the CTS-2010 check dimensions for Indian banks are followed by this all-encompassing method. International checks with specific dimensions needed by various nations or banks may also be processed by it. Because it complies with international check requirements and employs standardized check measures, it may be considered semi-automatic.

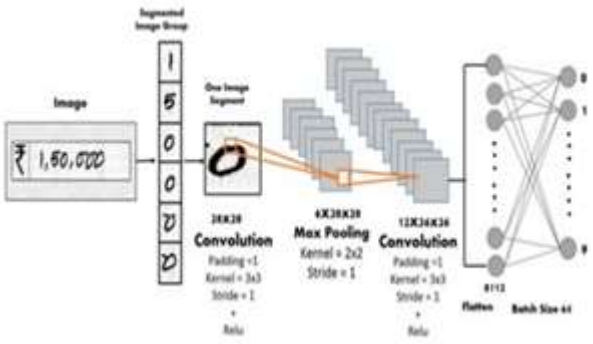



Fig. CNN architecture proposed for recognizing handwritten digits in courteous amount

Section E: Verifying Signatures Essential signature authentication was the subject of our research. The essential process of signature authenticity was investigated. Fifty different people had their scanned checks accompanied with 110 offline handwritten signatures. Out of the total, 80 were genuine and 30 were fake. After segmenting the signature images, we retrieved and normalized their properties. The effects of scaling, thinning, rotating, and cropping might be reduced with the use of normalization. Using Scale-Invariant Feature Transform (SIFT), we were able to recover outlines and features from normalized pictures. Reproducing visual regions at critical times while preserving their size and orientation is essential for SIFT to be functional. Scale-space extreme are generated by SSE, key points are located by KPL, orientation is assigned by OA, and key points are extracted by KDE.

The process is divided into four parts. SVM classifiers enhanced signature authentication using SIFT-derived features. The training and testing datasets were evenly split 80:20 between real and fake signatures. A support vector machine (SVM) uses a two-dimensional separating hyper plane to divide input into two categories. Optimal hyper plane-grouped data points for classification are generated by this approach. This meticulous method creates a strong framework for verifying and processing checks, guaranteeing their legitimacy and accuracy. This method is automated as it adheres to CTS-2010 standards for Indian banks and to specific dimensions determined by other nations' or banks' regulations for international cheques.

Honest and compassionate verification is guaranteed by this method. Figure 10: Sorting account holder signatures for validation of bank checks F. Results and analysis MATLAB was used to assess the precision and efficiency of a particular problem. We scanned 114 photos of bank cheques; 112 were from the IDRBT collection and 2 were done separately. The main parameter parts of the bank check booklet were used to train and test our system. Handwritten numbers were correctly detected 99.14% of the time by a Convolutional Neural Network. We trained character recognition networks with 850 iterations, achieving a mini-batch loss of 0.0077 and an accuracy of 99.94%. With the use of courtesy photographs, we were able to establish an IPV (English to Indian) conversion. Once the signature had been confirmed, we checked it against the authorized total.

Once the segmented image was standardized and features were extracted using SIFT, we used a Support Vector Machine (SVM) classifier to find and classify patterns. Our 98.1 percent accuracy is provided by the Support Vector Machine (SVM). Because of their distinct writing style, handwritten signatures continue to be a dependable technique for authenticity verification, even as forensics has advanced. Advantages and disadvantages of online and offline signature verification both exist. We were successful in our examination of system performance per module accuracy using sophisticated approaches.

## IV. RESULTSANDDISCUSSION

Shadows and spatial noise in low-quality duplicated photographs were not addressed by several studies [16]. Researchers used a local adaptive threshold to transform the grayscale picture to binary in order to capture word shapes. Interference between text and characters was minimized by the use of dual filtering. When compared to optical character recognition (OCR) systems, deep Convolutional de-noising auto-encoders performed 26.78% better, according to a small handful of researchers [17]. A Void Pantograph is necessary for the authentication of check images. An invisible pantograph was used in the first printing. It is essential for security printing toolkits since it stands out when printed. Automated void pantograph parameter tweaking was achieved by Aronoff et al. optimising the parameters of the void pantograph was automated by a group of researchers [18].

Fig. 4. Images of sample checks from various nations

There are plethoras of research that compare various languages' handwritten and machine-generated characters. In an experiment, the accuracy rate for classifying Arabic handwritten and machine-generated characters was 68%. Other studies used computer vision and image processing for object and edge detection. Offline recognition of handwritten digits using KNN and SVM classifiers reached 99% accuracy. Scratchy and non-scratchy handwriting were detected by CNNs. Grabbing and cutting images automatically. Real-world data is classified using DNNs. Cell picture segmentation with watershed and distance transform enhancements were used. A small group of researchers created a performance-based string matching method that allowed Rabin-Karp parallelization on Nvidia GPUs. The programme used the Quick Search, Horspool, and Brute Force algorithms [19, 20].

Generative AI takes a more holistic view of security by creating a real-time image of threats and their potential to cause havoc using data from multiple sources. Businesses can respond to possible assaults more quickly and efficiently with the help of automated threat detection. A comparison of the algorithms' accuracy is shown in Table 1.

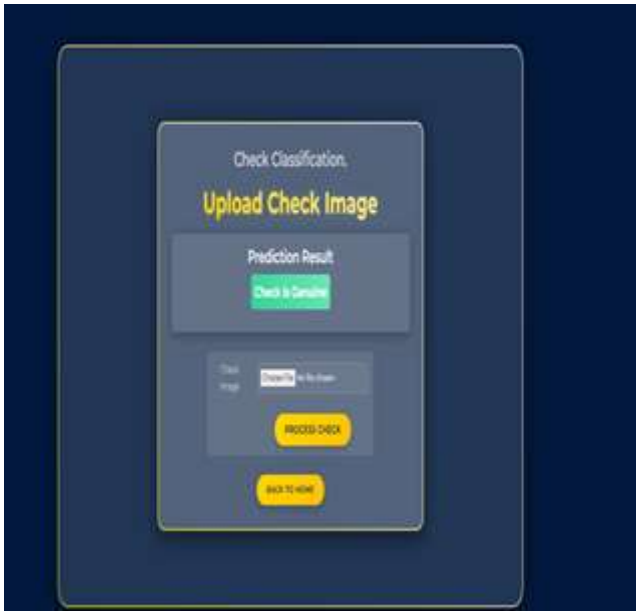
## V. TABLEI.COMPARISONOFACCURACY (IN %)


On top of that, businesses may head off potential threats before they ever happen because to generative AI's ability to spot behaviors that can indicate dangerous activity. With this technology, businesses can be more proactive with cyber security rather to just monitoring their networks. An organization's security and threat intelligence processes may be evaluated by conducting a performance study using generative AI. To do this, it is helpful to evaluate factors like detection latency, accuracy, scalability, and customizability. Lower detection latency allows an organisation to discover threats more rapidly.

**Evaluation of Genuine**

Solutions for threat intelligence and is playing an increasingly important role in bolstering cyber security. Possible security risks may be analyzed and evaluated using realistic threat models generated by generative AI. Generative AI models may use massive data sets to create several virtual representations of real-world dangers. Table 2 compares the false positive rate of various methods.

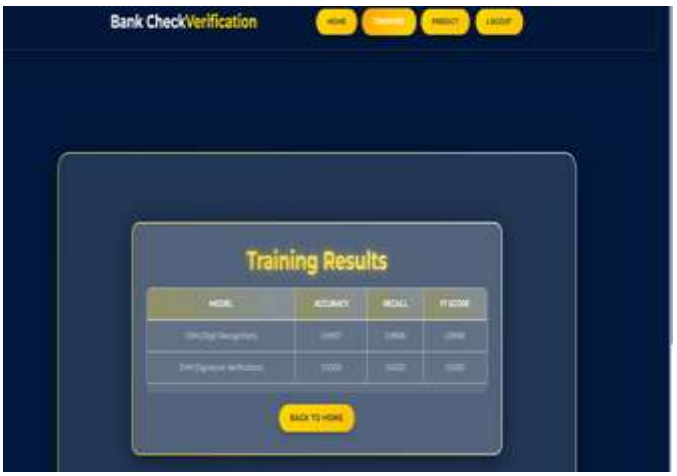

It is possible to use these simulations to build effective defenses by learning from different circumstances. Among the many possible applications of generative AI are the discovery and analysis of massive amounts of data, both organized and unstructured, and the detection and analysis of possible hostile or unexpected conduct. When conventional security measures fail to detect suspicious data patterns or outliers, generative AI models may learn from human actions to do so. Organizations would be able to address risks before they escalate if this leads to improved threat detection.




**Evaluation of Falsenegativerate**

Cyber security and threat intelligence are two areas where the use of artificial intelligence and machine learning is gaining traction. AI has shown to be an effective weapon in the fight against more complex threats, both in terms of detection and prevention. Specifically, there are a number of ways that generative AI is being used to enhance security systems.

Using generative AI, potential threats may be identified in real-time. The false negative rate of several algorithms is compared in Table 3.




This helps find malicious actions that other security systems may miss. It may also be used to analyze user behavior across many platforms and identify patterns that may indicate a security breach or criminal activity. One application of generative AI is to model potential attacks and their consequences in "what-if" scenarios or simulations, which may help designers build more secure systems. Generative AI can automate security operations to save time and money on system maintenance. Additionally, AI has the potential to detect and highlight suspicious behavior that humans may otherwise fail to notice. Finally, generative AI may be used to continually monitor and update security systems, allowing them to stay ahead of any attacks.

**Evaluation of Response time**

A kind of AI called as generative AI is capable of autonomously learning from datasets and creating new, unseen data. It may be used to improve cyber security processes and threat intelligence by seeing potential dangers before they happen. Rapid detection of data anomalies and alerting of security personnel to possible dangers are both made possible

by generative AI. Potential outcomes include enhanced general defence against cyber-attacks and accelerated response times. Various strategies for response time are compared in Table 4.


By mimicking real-world scenarios via simulations enabled by generative AI, security professionals may also practice responding to potential security attacks. This may help find potential vulnerabilities and make security measures more effective. Finally, new threats may be mitigated with the help of generative AI, which can detect and block harmful software and other threats. Looking in the big picture, generative AI might be a powerful tool for enhancing cyber security procedures and threat intelligence. The application of generative AI allows organizations to identify harmful threats more swiftly and react as effectively as possible. Companies may use this information to anticipate potential dangers and adjust their cyber defense measures accordingly. Furthermore, generative AI may help find existing system and network vulnerabilities and then patch or defend them as well as possible. Organizations may benefit from generative AI in cyber security and threat intelligence systems in several ways, including preventing, detecting, and responding to cyber assaults.

## VI. CONCLUSION

A full-fledged model for verifying bank cheques using OCR, CNN, SIFT, and SVM together. Automating the clearing of cheques increases both efficiency and precision. Machine-printed checks were optically scanned. To a 97.7 percent accuracy rate, the OCR was able to match typographic characters. Data from checks produced by machines was helpful. Using many datasets, a CNN model was able to detect handwritten numerical values. With rigors testing and training, accuracy was raised to 99.14%. Number recognition with CNNs improved from 99.05 percent. Checks need the use of handwriting digit detection. Remarkably, our CNN character recognition achieved a score of 99.94%. CNN enhanced verification by accurately identifying check characters. Signals were detected using SIFT and SVM. All except one of the signatures on the cheque were correct. In order to accurately verify signatures, SIFT discovered crucial features of signature pictures that SVM had recognised. Our strategy is beneficial to banks. Time is saved by automating the clearance of checks. Centralized monitoring of check transactions streamlines and confirms the process. The act of learning English itself has checks. The method's applicability might be broadened in future studies to include more languages. We employ OCR, CNN, SIFT, and SVM in our groundbreaking bank cheque verification system. In order to expedite the clearing of bank cheques, the system verifies signatures and identifies both machine-printed and handwritten data.

## REFERENCES

1. Dhanva K, Harikrishnan M, Babu PU (2018) Cheque image security enhancement in online banking. In: Second international conference on inventive communication and computational technologies (ICICCT), pp 1256–1260
2. Singh HK, Tigga AE (2012) Impact of information technology on indian banking services. In: 1st International conference on recent advances in information technology (RAIT), pp 662–665
3. Wang P, Shiau CR (1972) Machine recognition of printed Chinese characters via transformation algorithms. Pattern Recognit 5(4):303–321
4. Zramdini A, Ingold R (1998) Optical font recognition using typographical features. IEEE Trans Pattern Anal Mach Intell 20(8):877–882 [5] Zhu Y, Tan T, Wang Y (2002) Font recognition based on global texture analysis. IEEE Trans Pattern Anal Mach Intell 23(20):1192–1200
5. Saenthon A, Sukkhadamrongrak N (2014) Comparison the training methods of neural network for English and Thai character recognition. In: Signal and Information Processing Association Annual Summit and conference (APSIPA), pp 1–4

6. Ramanathan TT, Sharma D (2017) Multiple classifications using svm based multi knowledge-based system. In: International conference on advances in computing & communications, (ICACC'17), pp 307– 311.
7. Stewart S, Pinto L, Barrett B (2018) Segmentation and stitching improves handwriting recognition on datasets with few samples. In: 16th International Conference on Frontiers in Handwriting Recognition (ICFHR), pp 465–470
8. Kajale R, Das S, Medhekar P (2017) Supervised machine learning in intelligent character recognition of handwritten and printed nameplate. In: International conference on advances in computing, communication and control (ICAC3), pp 1–5
9. Feng W, Gao S (2010) A vehicle license plate recognition algorithm in night based on hsv. In: 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol 4, pp 53–56
10. Singh S, Kariveda T, Gupta JD, Bhattacharya K (2015) Handwritten words recognition for legal amounts of bank cheques in English script. In: Eighth IEEE International Conference on advances in Pattern Recognition (ICAPR), pp 1–5
11. Miah MBA, Yousuf MA, Mia MS, Miya MP (2015) Handwritten courtesy amount and signature recognition on bank cheque using neural network. Int J Comput Appl 118(5):21–20.
12. Jayadevan R, Pal U, Kimura F (2010) Recognition of words from legal amounts of Indian bank cheques. In: 12th International Conference on frontiers in Handwriting recognition. IEEE, pp 166–171
13. Raghavendra SP, Danti A (2009) A novel recognition of Indian bank cheques based on invariant geometrical features. In: International conference on trends in automation, communications and computing technology (I-TACT'15), pp 1–5
14. Shirai K, Akita M, Okamoto M, Tanikawa K, Akiyama T, Sakaguchi T (2012) Removal of background patterns and signatures for magnetic ink character recognition of checks. In: 10th IAPR international workshop on document analysis systems, pp 190–194
15. Lu H, Guo B, Liu J, Yan X (2017) A shadow removal method for tesseract text recognition. In: International Congress on image and Signal Processing Biomedical Engineering and Informatics (CISP-BMEI), pp 1–5.