IJIRIS: International Journal of Innovative Research in Information Security
Volume 10, Issue 04, May 2024
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives

Enhancing Signature Forgery Detection System Using CNN-SVM

Sonika
Department of CSE
East Point College of Engineering and Technology,
Bangalore, INDIA
sonikareddy516@gmail.com
Sunil KK
Department of CSE
East Point College of Engineering and Technology,
Bangalore, INDIA
sunilkulali064@gmail.com
Sunil BA
Department of CSE
East Point College of Engineering and Technology,
Bangalore, INDIA
sunilsunilba@gmail.com
Vishwas V
Department of CSE
East Point College of Engineering and Technology,
Bangalore, INDIA
vishwas.v2020@gmail.com
Manimegalai A
Assistant Professor, Department of CSE
East Point College of Engineering and Technology,
Bangalore, INDIA
manimegalai.a@eastpoint.ac.in

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.10/Issue04/MYIS10112
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRIS/RS/Vol.10/Issue04/MYIS10112
Received: 07, April 2024 | Revised:16, April 2024 | Accepted: 27, April 2024 Published Online: 07, May 2024 Volume2024
Article ID MYIS10112 http://www.ijiris.com/volumes/Vol10/iss-04/33.MYIS10112.pdf
Article Citation: Sonika,Sunil,SunilV,Vishhwas,Manimegalai(2024). Enhancing Signature Forgery Detection System Using CNN-SVM. International Journal of Innovative Research in Information Security, Volume 10, Issue 04, Pages 288-293
doi:> https://doi.org/10.26562/ijiris.2024.v1004.33
BibTex key: Manimegalai@2024Enhancing

Copyright: ©2024 This is an open access article distributed under the terms of the Creative Commons Attribution License; which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract: Handwritten signatures are widely used as a means of personal identification and authentication. Many documents like bank cheques and legal transactions require signature verification. But considering a large number of documents, it is a very difficult and time-consuming task. Therefore, ensuring the necessity for a robust automatic signature verification tool that aims to reduce fraud in all related financial transaction sectors. The current visual verification depends mainly on the experience, mood, and working environment of the verifier which ultimately wastes both time and money. Moreover, it is difficult for the eyes of any experts to precisely verify the ratios between lines and angles of a genuine signature to a fraud signature. Therefore, we propose an automatic signature verification technique using the recent advances in image processing and machine learning.

INTRODUCTION

Signature verification and forgery detection systems are used to verify a person's identity by verifying a signature. These systems can be used both online and offline. Online signature verification and forgery detection systems are used to verify a person's identity by verifying a signature in an online environment. A reference signature is usually stored in a secure database and is used to compare a person's signature to ensure its authenticity. The system can also detect possible fake attempts by comparing the signature with a reference signature. Offline signature verification and forgery detection systems are used to verify a person's identity by verifying a signature in an offline environment. These systems use several methods to capture a person's signature and compare it to a reference signature. Both online and offline signature verification and forgery detection systems are important tools for authenticating a person's identity. These systems are used in a variety of industries, including banking, healthcare and government. They are also used to protect against fraud and identity theft.

LITERATURE SURVEY

[1] Automated bank cheque verification using image processing and deep learning methods Description: Our innovative tool utilizes image processing and deep learning methods to accurately verify key components of bank cheques, such as the branch code, cheque number, legal and courtesy amounts, account number, and signature patterns. Using the IDRBT cheque dataset and convolutional neural networks, we achieved a 99.14% accuracy for handwritten numeric character recognition and 97.7% accuracy for machine-printed script using MATLAB's OCR

[2] Deep Learning Recurrent Attention Optical Character Recognition Network with Data Augmentation for Cheque Data Extraction

Description: In this study, a recurrent attention optical character recognition network (RA_OCRN) was employed to extract legal information from images of bank cheques, aiming to improve accuracy in check verification processes. The research utilized deep learning for data pretreatment and augmentation, showcasing improved results compared to existing methods when tested on the Kaggle cheque detection dataset.

[3] Use of Digital Signature Verification System (DSVS) in Various Industries: Security to Protect against Counterfeiting : Research Description: The study proposes a method for handwritten signature verification, combining dynamic and static features to enhance authenticity and protect customer property in the banking industry. The traditional approach to signature verification relies on human judgment, which can lead to misunderstandings, insults, and financial losses.

[4] Signature Verification of Bank Cheque

Description: Signature verification is widely used for biometric identification, particularly in banking and financial transactions. Various methods such as Hopfield neural network, Back-propagation algorithm, Support vector machine, Hidden Markov Model, and Artificial Neural Network (ANN) have been utilized for this purpose.

[5] Signature Extraction and Recognition from Bank Cheque Image

Description: A three-layer signature verification system has been proposed for bank cheque images, utilizing writer-independent and offline verification. It employs graphometrical and FAST features extracted from signatures as inputs for classification algorithms.

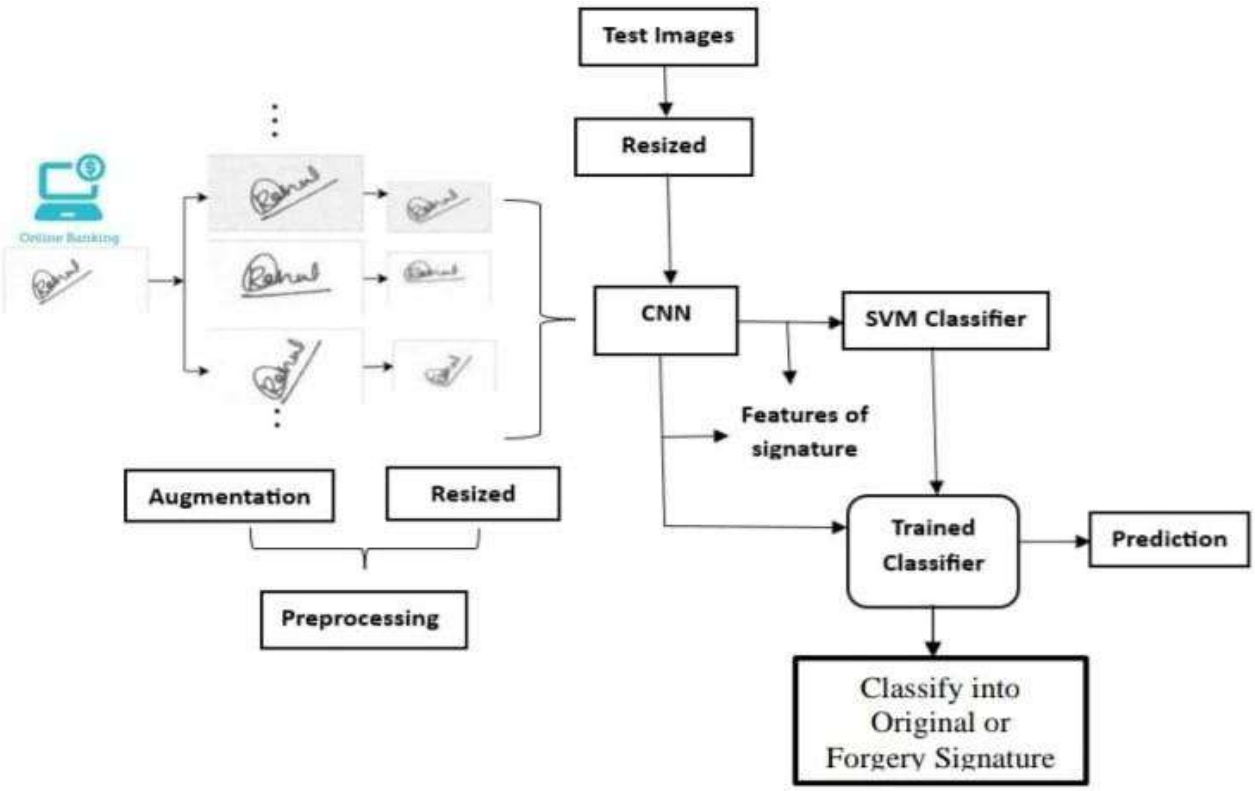
PROPOSED SYSTEM

After the images have been cropped by OCR technique, we will use the Connected Components Algorithm to extract the signature from the image.

Following are the Signature Verification Approaches:

- The OCR Approach: Identify the signatures and crop the images
- The Line Sweep Algorithm: Use OCR result images and do rectangle fitting across the signature.
- And verification of the signature done that belongs to fake or original using SVM and CNN models.

SYSTEM ARCHITECTURE



SYSTEM MODULES

The system modules of the project can be organized into several key components:

1. Data Augmentation

The following code is the implementation of the data augmentation process used to create images and increase the size of the dataset artificially. Here, Image Data Generator is used to produce new images. The rotation range is set to 360 as the images are spiral and can be rotated any number of degrees without changing the image's meaning. You can try other image transformations available under Image Data Generator class. But be careful while applying any augmentation as certain transformations may lower the CNN model's lower accuracy.

2. OCR Component:

Let's denote the OCR process as a function that takes an input image of a bank cheque and produces extracted textual information: OCR (image) Textual Information

Here, the OCR function analyzes the input image and outputs relevant textual details such as account numbers, payee names, and other relevant information

3 Line Sweep Component:

The Line Sweep technique involves systematically scanning and extracting features from signatures. Let's define the Line Sweep process as follows:

Line Sweep (signature)

Extracted Features

The Line Sweep function takes a signature image as input and performs a line-by-lines can, extracting features such as stroke directions, lengths, and angles. The output is a set of features that represent the signature's characteristics

4 CNN Model Architecture

- The model contains four Convolutional Layers with 128, 64, 32, and 32 filters, respectively.
- The convolutional layers contain filters with varying filter sizes.
- A MaxPool 2D layer follows each convolutional layer.
- Two Fully Connected layers follow the convolutional block.

5. Training the Model

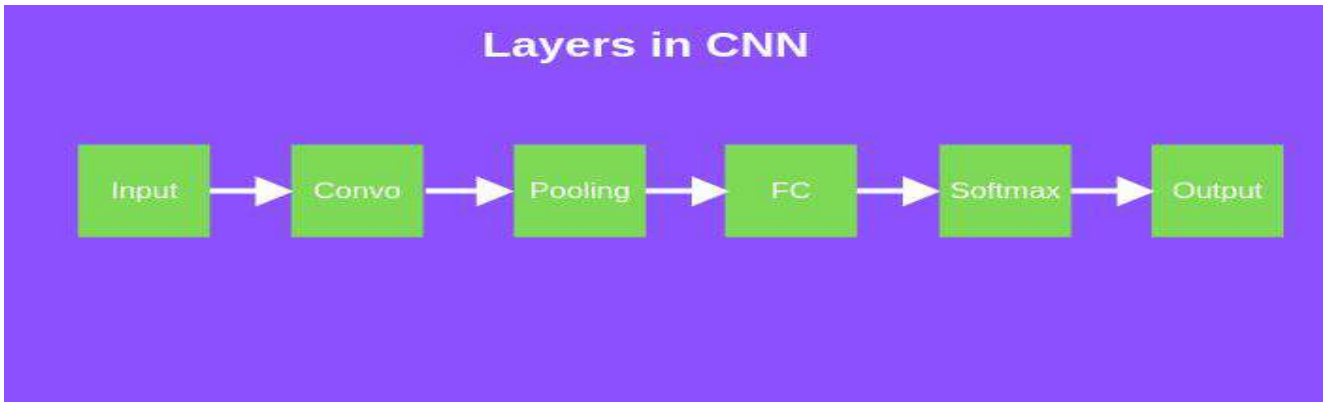
The model is trained with a learning rate of 3.15e-5 using Adam optimizer. The epochs and batch size are set to 70 and 128, respectively

6. Performance of the Model

The Loss and Accuracy Plots, Classification Report and Confusion Matrix, are used as performance metrics for the model.

SYSTEM IMPLEMENTATION

CNN Algorithm: CNN stands for Convolutional Neural Network, which is a class of deep neural networks primarily designed for processing structured grid-like data, such as images or video. CNNs have been particularly successful in tasks like image classification, object detection, and image segmentation.



Input Layer:

- The input layer represents the raw input data, typically an image or a set of images. Each image is represented as a grid of pixel values, with each pixel representing a feature.
- In order to prepare the input data for the Convolutional Neural Network (CNN), it is necessary to reshape the images into a single column format. For instance, if the images have dimensions of 28 x 28, totaling 784 pixels, they must be transformed into a column vector of size 784x1before being fed into the network.
- If there are "m" training examples, then the dimension of the input data will be (784, m). This reshaping ensures that each pixel value of the images is represented as a single input feature, facilitating the training process of the CNN.

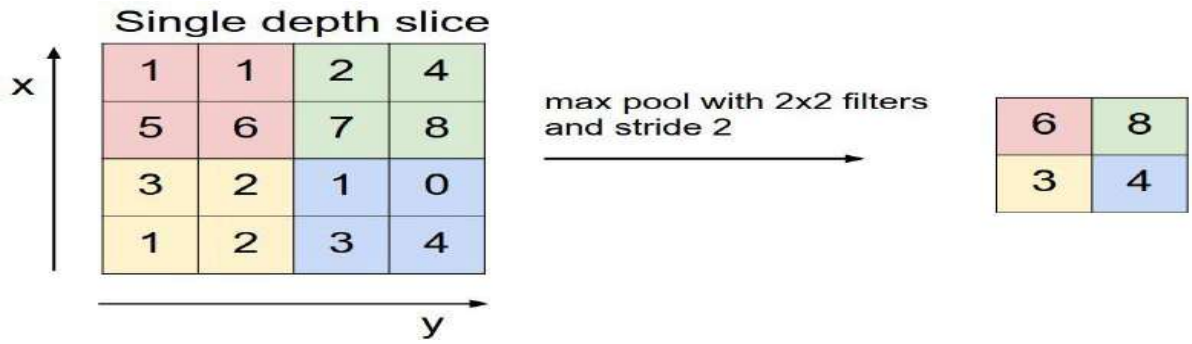
Convo Layer:

- In the convolutional layer, a set of learnable filters (also known as kernels) is applied to the input image through convolution operations.

- Convolution involves sliding each filter across the input image and computing the dot product between the filter and the local region of the input.
- The ReLU(Rectified Linear Unit) activation function is applied element-ise to the output of the convolution operation. ReLU introduces non-linearity, allowing the network to learn complex patterns and relationships in the data.

Pooling Layer:

- The pooling layer reduces the spatial dimensions of the feature maps generated by the convolutional layer while retaining the most important information.
- Common pooling operations include maxpooling, where the maximum value in each local region is retained, and average pooling, where the average value is computed.
- Pooling helps in reducing computation and controlling over fitting by providing translational in variance.



We have applied max pooling in single depth slice with Stride of 2. The 4x4- dimension input is reduced to 2x2 dimensions. There is no parameter in pooling layer but it has two hyper parameters — Filter (F) and Stride(S). In general, if we have input dimension W1xH1xD1, then W2 = (W1−F)/S+1H2 = (H1−F)/S+1D2=D1
Where W2, H2 and D2 are the width, height and depth of output.

Fully Connected Layer (FC):

- The fully connected layer receives the flattened output from the preceding layers and consists of densely connected neurons.
- Each neuron in the fully connected layer is connected to every neuron in the previous layer.
- The fully connected layer performs classification based on the learned features from the convolutional and pooling layers.

Soft Max / Logistic Layer:

- In classification tasks, a softmax or logistic layer is typically added after the fully connected layer.
- The softmax function converts the raw scores (logits) from the previous layer into class probabilities.
- Each output neuron represents the probability of the input belonging to a particular class.

Output Layer:

- The output layer receives the probabilities computed by the softmax or logistic layer.
- In binary classification tasks, a single output neuron with a sigmoid activation function is used to output the probability of the input belonging to one of the two classes (e.g.,0 or1).
- In multiclass classification tasks, multiple output neurons are used, each representing the probability of the input belonging to a specific class.

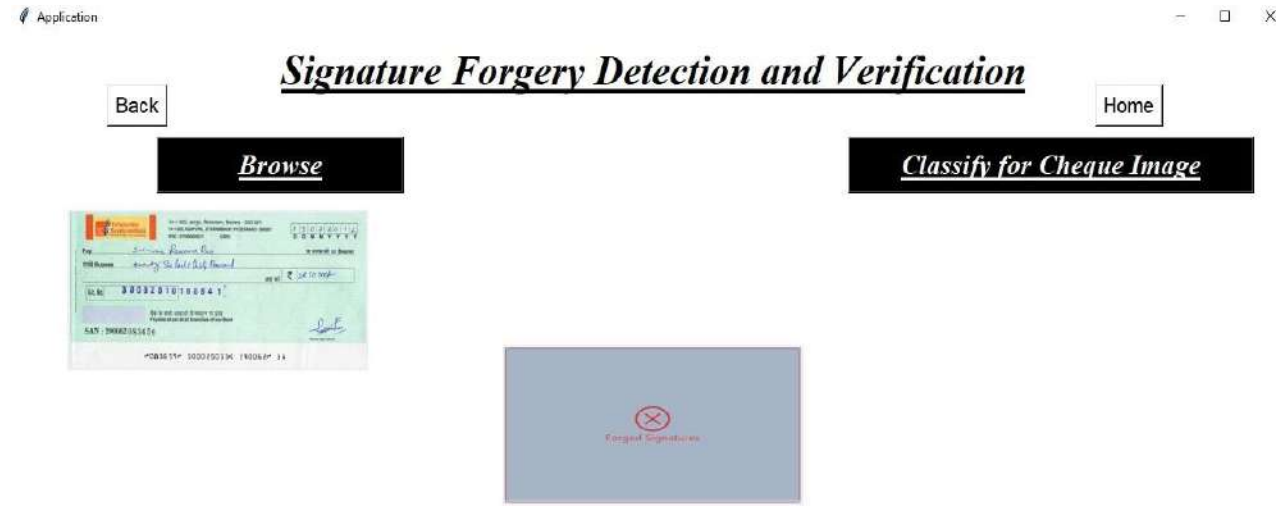
SCOPE OF FUTURE APPLICATION

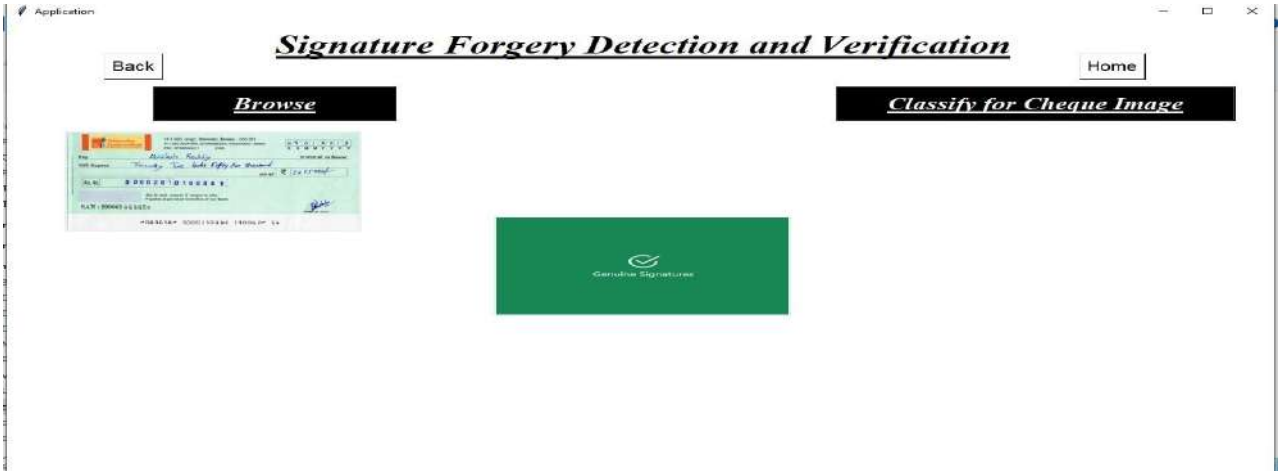
- Data collection and preprocessing: gathering a diverse datasets of genuine and forged signatures followed by preprocessing steps like normalization and augmentation.
- Model Architecture Selection: Designing a Convolutional Neural Network (CNN) architecture suitable for signature image classification, potentially in corporating techniques like transfer learning for improved performance.
- Training and Validation: Training the CNN model on the prepared dataset and validating its performance using appropriate evaluation metrics such as accuracy, precision, recall, and F1-score.
- SVM Integration: Integrating a Support Vector Machine (SVM) classifier to enhance the classification results obtained from the CNN model, possibly through techniques like ensembling or stacking.
- Hyper parameter Tuning: Optimizing hyper parameters for both CNN and SVM models to achieve the best possible performance.
- Evaluation and Testing: Evaluating the combined CNN-SVM system on an independent test set to assess its generalization ability and robustness.
- Deployment and Integration: Deploying the final model into a practical application environment, ensuring compatibility and usability with existing signature forgery detection systems.

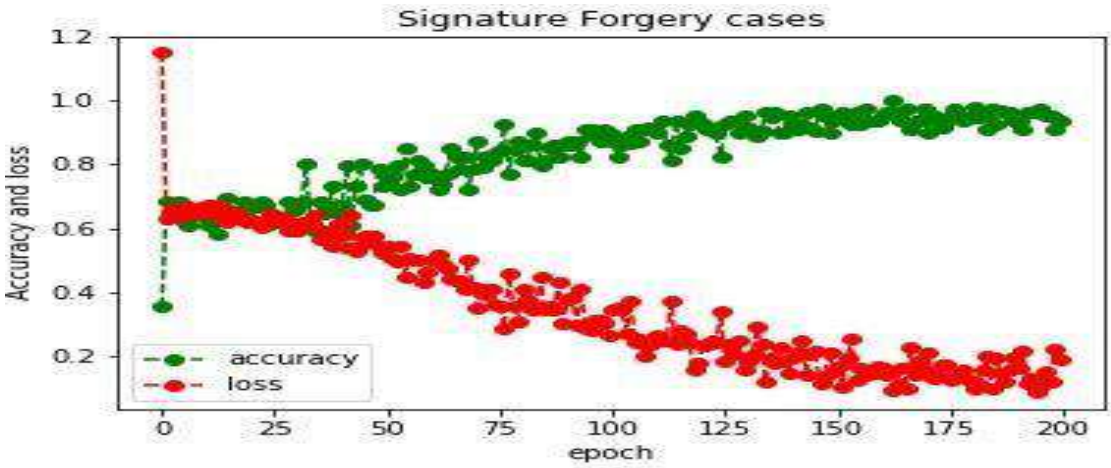
IJIRIS © 2014-24, AM Publications - All Rights Reserved

- Performance Comparison: Comparing the performance of the enhanced system with existing methods to demonstrate its effectiveness in improving signature forgery detection accuracy and reliability.
- Documentation and Reporting: Documenting the entire process, including methodology, results, and any challenges encountered, in a comprehensive report or research paper.
- Future Extensions: Discussing potential avenues for further improvement or extension of the system, such as in corporating additional features or exploring different machine learning algorithms.

RESULTS







CONCLUSION

This project represents a significant step forward in the field of signature verification and document authentication. The suggested system can make forecasts for forgery detection by learning from signatures. The project has provided valuable insights and contributions to the domain of signature verification. Wherever a signature is used as a form of authentication, including banks and educational organizations, the system can be used. Because they can solve some issues comparatively easily, neural networks have proven successful in a variety of applications. With the rapid development of technology, the old rules are becoming obsolete. As a result, new technologies are being developed to fight fraud and crime, and tools are updated as people discover vulnerabilities. Signature verification and forgery detection systems have been developed to deal with forged and rewritten signatures to provide clear and accurate disclosure of a person's identity and prevent any type of identity crime. When given access to examples of real and fake signatures of the same individuals whose signatures were previously seen during training, CNN and SVM does a great job of verifying signatures and it may give the result that signature is genuine or not.

REFERENCES

[1]. Prateek Agrawal, Deepak Chaudhary, Vishu Madaan, Anatoliy Zabrovskiy, Radu Prodan, DragiKimovski and Christian Timmerer. "Automated bank cheque verification using image processing and deep learning methods". (2021) Multimedia Tools and Applications.80.1-32.10.1007/s11042-020-09818-1.

[2]. Hitesh Chaitanyaswami, and Ashwin Dobariya. "Deep Learning Recurrent Attention Optical Character Recognition Network with Data Augmentation for Cheque Data Extraction." 2023 International Conference on Computer, Electronics &Electrical Engineering & their Applications (IC2E3) https://doi.org/10.1109/IC2E357697.2023.10262478

[3]. Dr.Thangavel V, "Use of Digital Signature Verification System (DSVS) in Various Industries: Security to Protect against Counterfeiting: Research". (April 24, 2023). SSRN: https://ssrn.com/abstract=4461014 or http://dx.doi.org/10.2139/ssrn.4461014

[4]. VijayaDhopte1,Prof.ShailaP.Kharde," Signature Verification of Bank Cheque "IJIRSETVolume10, Issue10, October 2021 https://doi:/10.15680/IJIRSET.2021.1010093

[5]. Bramara NeelimaK and SArulselvi " Signature Extraction and Recognition from Bank Cheque Image" IJITEE2019 https://doi:/10.35940/ijitee.B7766.129219