Analysis of Fake Currency Circulation in India

&

Detection of Fake Currency Using Statistical Image Processing and Machine Learning

Project Report Submitted in Partial fulfilment of the requirement for the award of Degree of

MASTER OF BUSINESS ADMINISTRATION

MBA

Submitted by

SHABHARISH

Reg. No.:2314512769

Under the guidance of

ASHITHA

CENTRE FOR DISTANCE AND ONLINE EDUCATION

MANIPAL UNIVERSITY JAIPUR

July - 2025

BONAFIDE CERTIFICATE

This is to certify that Shabharish, a student of Master of Business Administration, Reg. No. 2314512769, has successfully completed the project titled "Analysis of Fake Currency Circulation in India & Detection of Fake Currency Using Statistical Image Processing and Machine Learning" under my supervision as a part of the requirements for the MBA program at centre for distance and online education, Manipal University Jaipur during the academic year 2024-2025.

This project report embodies the original work of the student, conducted with due diligence, and adheres to the standards expected by the institution. It has not been submitted to any other institution for any degree, diploma, or certificate.

ASHITHA

Test Lead, Wipro Limited

Date: 11-06-2025

Place: Bangalore, Karnataka

DECLARATION BY THE STUDENT

I, Shabharish, a student of Master of Business Administration (MBA), Reg. No. 2314512769, hereby declare that the project report titled "Analysis of Fake Currency Circulation in India & Detection of Fake Currency Using Statistical Image Processing and Machine Learning" submitted to Centre for Distance and Online Education, Manipal University Jaipur is a record of my original work carried out under the guidance of Ashitha. Test Lead, Wipro Limited.

I affirm that this project is the result of my own independent effort, and to the best of my knowledge, it does not contain any material previously published or written by any other person or material which has been accepted for the award of any other degree or diploma at any other educational institution, except where due acknowledgment has been made in the text.

I also declare that I have adhered to all the guidelines and standards required for academic honesty and have cited all sources wherever used.

SHABHARISH

Registration Number: 2314512769

Date: 11-06-2025

Place: Udupi, Karnataka

Analysis of Fake Currency Circulation in India

&

Detection of Fake Currency Using Statistical Image Processing and Machine Learning

ABSTRACT

Counterfeit currency is a persistent and growing concern in India, posing a serious threat to the nation's economic stability, internal security, and public trust in the financial system. The circulation of fake notes contributes to inflationary pressures, facilitates unlawful activities, and results in significant financial losses to both government institutions and private stakeholders. As counterfeiters adopt increasingly sophisticated printing technologies, the detection of fake currency has become more challenging, rendering traditional verification methods – such as manual inspection and expensive detection devices are inefficient and impractical for widespread implementation.

To address this multifaceted issue, this project adopts a dual approach. The first component involves an analytical study of counterfeit currency circulation patterns across various Indian states over a defined period. This analysis leverages data from credible sources, including government records, law enforcement reports, and financial institution disclosures. The goal is to identify key trends, and vulnerable regions that contribute to the distribution of fake currency. The insights gained from this investigation are used to understand the broader socio-economic impacts of counterfeit money and to inform targeted policy interventions.

The second part of the project focuses on developing a low-cost, automated system for detecting fake notes using image processing and machine learning. A Python-based tool was built using the Banknote Authentication Dataset, where features like variance, skewness, kurtosis, and entropy were extracted from scanned note images to train machine learning models. These models showed high accuracy in identifying real and fake notes. The project demonstrates that integrating such intelligent systems can significantly improve the speed, reliability, and affordability of currency verification, making them suitable for use in banks, retail settings, and mobile platforms. Future improvements could include deep learning integration and real-time image input for even better performance.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER-1

INTRODUCTION

The integrity of a nation's currency is vital to its economic stability, public confidence, and national security. Counterfeit currency refers to fake or forged money that is illegally produced and circulated to look like genuine legal tender. In India, the circulation of counterfeit currency has emerged as a significant challenge, affecting both macroeconomic indicators and grassroots financial systems. The increasing sophistication of fake notes, made possible by advancements in printing technologies and organized counterfeiting networks, has exposed vulnerabilities in traditional detection mechanisms. These issues not only cause monetary losses but also contribute to the funding of illegal and anti-national activities.

Recognizing the severity of this threat, this project seeks to explore the issue from both analytical and technological perspectives. It focuses on understanding the spread and impact of fake currency within India, while simultaneously proposing a practical and cost-effective solution for detecting counterfeit notes. By combining data analysis with machine learning and image processing techniques, the project aims to contribute meaningful insights and tools to support financial institutions, law enforcement agencies, and policymakers in combating currency fraud more effectively.

1.1. Background of the Study:

India has faced persistent challenges related to counterfeit currency for decades. Fake notes are often introduced into the economy through illegal cross-border networks and domestic counterfeiting operations. These fake notes not only disrupt the supply of genuine currency but also damage consumer trust, burden financial institutions, and undermine policy measures such as demonetization or cash flow control. In recent years, reports from the Reserve Bank of India (RBI), National Crime Records Bureau (NCRB), and various state governments have highlighted an upward trend in the detection and seizure of counterfeit notes, particularly in high-denomination currency.

In India, counterfeit currency appears in various forms, ranging from simple imitations to highly sophisticated forgeries, depending on the techniques and tools used by counterfeiters. The most basic type includes photocopied notes, which are created using standard printers or copiers. These are usually of poor quality, lacking texture and essential security features, making them easy to detect. Hand-drawn notes, produced with pens or pencils, are crude in appearance and commonly found in rural or low-awareness areas.

A more advanced form of counterfeit currency involves notes produced using printing presses, which closely imitate real currency by including features like watermarks and holograms, making them difficult for the average person to detect. With ongoing technological progress, counterfeiters now use digital or electronic printing to create high-resolution fake notes that may include microprinting, colour-shifting ink, and other sophisticated features. Some groups also counterfeit foreign currencies like US dollars or Euros for international scams or illegal trade. These evolving techniques show how fake currency threats are becoming more complex, emphasizing the need for smarter and more vigilant detection systems.

Traditional methods of identifying fake currency – such as watermark checks, ultraviolet light scanning, and manual inspection – are time consuming, costly, and prone to human error. Moreover, they are impractical for widespread deployment in high-volume settings like retail, transportation, or rural banking. This highlights a pressing need for automated, scalable, and affordable detection solutions. At the same time, Technological advancements in image processing and machine learning have created new opportunities for improving fraud detection, especially in identifying counterfeit currency. By analyzing statistical image features such as kurtosis, skewness, entropy, and variance, it is possible to detect subtle differences between real and fake notes. These features, when used with supervised machine learning algorithms, can help build accurate and efficient models for classifying currency.

Our proposed system focuses on analyzing the physical features of currency notes using image processing to extract key indicators like kurtosis, skewness, and entropy. These features help detect patterns that differentiate real notes from fake ones. To make the solution accessible, we developed a user-friendly web application that allows users to upload note images and instantly verify their authenticity using a trained machine learning model, providing a quick, affordable, and convenient method for counterfeit detection.

This study, therefore, builds on both the socio-economic context and the technological potential to deliver a comprehensive view of the counterfeit currency problem in India. It analyses state-wise trends and patterns in fake currency circulation, while also developing a Python-based detection model that leverages statistical image processing and machine learning to accurately classify banknotes. The ultimate goal is to support smarter decision-making, improve detection infrastructure, and contribute to India's financial security framework.

1.2. Research Objectives:

The primary objective of this project is to address the growing problem of counterfeit currency circulation in India by providing both an analytical understanding of its spread and a practical technological solution for its detection. With the rise in fake notes and the limitations of traditional detection methods, there is a need for an automated, cost-effective, and scalable approach to identify counterfeit currency.

This project aims to:

- ✓ Analyze the temporal trends of counterfeit currency circulation in India over a defined time period using historical data.
- ✓ Visualize the state-wise distribution of fake currency to identify regional patterns and potential hotspots of circulation.
- ✓ Develop a Python-based automated detection system that uses image processing and statistical analysis to distinguish between genuine and counterfeit currency notes.
- ✓ Extract and evaluate key statistical image features such as kurtosis, skewness, entropy, and variance for effective classification of currency notes.
- ✓ Apply machine learning algorithms for training and testing models that accurately classify notes as genuine or counterfeit.
- ✓ Provide a user-friendly and portable tool, in the form of a web application, that enables individuals and institutions to verify the authenticity of currency notes quickly and efficiently.

1.3. Scope of the Project:

The study on counterfeit currency in India has a dual focus:

Phase I – Analysis of Fake Currency Circulation in India:

- Analyses the detection and seizure of counterfeit notes across India between 2014–15 and 2024–25.
- Covers year-wise and denomination-wise patterns in counterfeit currency detected by banks.
- Explores state-wise and Union Territory-wise distribution based on NCRB reports from 2016–2022.
- Identifies geographical hotspots, high-risk denominations, and key periods such as the spike during demonetization.
- Overall, Provide a comprehensive analysis of counterfeit currency trends in India.

Phase II – Detection of Fake Currency Using Image Processing and Machine Learning:

- Uses machine learning and image processing to develop a prototype system for classifying fake notes which is scalable, easy to use, efficient which achieve good accuracy with less human errors.
- Employs the Banknote Authentication Dataset and Python-based tools to extract statistical features like variance, kurtosis, skewness and entropy.
- Demonstrates how counterfeit detection can be automated using real note images and classification models.
- Implements technologies such as Python, Django, HTML, CSS, JavaScript, and data visualization libraries to build and evaluate the system.
- Support authorities and financial institutions with insights and practical tools to counter the spread of fake currency.

CHAPTER-2

LITERATURE REVIEW

N.R.Deepak, Nikhat Yasmeen, Nida S, et al. "A Review on Fake currency detection using feature extraction."[1] Fake currency detection is a global issue affecting many economies, including those of the U.S. and India. This study focuses on identifying counterfeit Indian currency based on its physical features, such as the security thread, intaglio printing (RBI logo), and other distinctive security marks. In this project, the authors propose an effective method for extracting and recognising the properties of Indian rupee notes is presented. The study also includes detection and identification of counterfeit cash.

Mr. Ratnesh K. Choudhary, Ms. Prachi Borate et al. in their 2024 study "Literature Survey on Revolutionizing Fake Currency Detection: CNN-Based Approach for Indian Rupee Notes,"[2] present an effective methodology for detecting counterfeit Indian rupee notes. Their research addresses the escalating issue of counterfeit currency in India by leveraging advanced digital image processing and machine learning techniques. The study incorporates key processes such as preprocessing, segmentation, feature extraction, and clustering to identify fraudulent notes.

Gaikwad, Mayadevi et al.[3] conducted an experiment utilizing pattern matching to distinguish authentic currency notes from counterfeit ones. Each denomination was associated with a unique template; a match between the input note and the corresponding template indicated authenticity, while a mismatch suggested counterfeiting. The input images underwent preprocessing, which included noise reduction and the application of a feature extraction technique to identify the denomination. Subsequently, pattern matching was performed between the original and suspected counterfeit notes to verify authenticity.

Kumar and Chauhan et al(2020), in their study "A Study on Indian Fake Currency Detection,"[4] examine the issue of counterfeit currency in India and assess methods for its detection. They highlight the economic and security risks posed by fake notes and review traditional techniques like manual checks and UV scanning. Emphasizing the drawbacks of manual methods, the study advocates for modern solutions such as image processing and machine learning to enhance accuracy and efficiency. The authors stress the need for adopting advanced technologies, especially in banking and retail, to effectively combat counterfeit currency circulation.

Sharma and Sharma P (2018), in their study "An Overview of Counterfeit Currency in India,"[5] highlight the growing threat of fake currency and its impact on the Indian economy. They discuss how counterfeit money supports illegal activities like terrorism and smuggling, and how advancements in printing technology have made detection more challenging. The paper emphasizes the roles of the RBI, law enforcement, and public awareness in combating this issue. It concludes by recommending a multi-pronged strategy involving technology, enforcement, and education – supporting the use of modern tools like image processing and machine learning for effective counterfeit detection.

Syeda Aimen Naseem et al.[6] proposed a novel technique for identifying counterfeit banknotes using image processing methods implemented in MATLAB. Their approach focused on extracting key security features of the banknote, such as the watermark, security thread, and serial number. By analyzing standard RGB images, the algorithm was able to verify the authenticity of currency notes based on these visual elements, offering an efficient and practical solution for counterfeit detection.

Sharma A (2017), in the paper "Combating Counterfeit Currency in India: Issues and Challenges,"[7] explores the complex nature of counterfeit currency as both an economic and security threat. The study analyses the systemic challenges faced by Indian authorities, including weak enforcement, gaps in cross-border monitoring, and the increasing sophistication of counterfeiters. It emphasizes the need for stronger regulatory mechanisms, inter-agency coordination, and technological upgrades in detection systems. The paper advocates for the integration of digital tools and improved public awareness as essential components in the fight against fake currency, aligning well with modern data-driven and AI-based detection approaches.

Aakash S. Patel et al. [8] focused on applying machine learning algorithms in the field of image processing for fake currency detection. Their approach involved training the system using a pre-compiled dataset containing images of both genuine and counterfeit currency notes. The algorithm analyses this dataset to extract key features, enabling the system to accurately classify new input images of similar format as either real or fake.

Vidhi Roy and Mannadiar et al. [9] utilized digital image processing techniques to identify genuine currency. Their method included steps like image acquisition, grayscale conversion, edge detection, image segmentation, and feature extraction. These processes are critical for accurately analyzing and verifying the authenticity of banknotes using digital tools.

Debang S. Gujarathi, Sushii V. Nikam, and Prathmesh P. Gogte[10] proposed a simple and user-friendly image processing-based method for authenticating Indian currency notes, particularly denominations of ₹100, ₹500, and ₹1000. Their technique is designed to help individuals who may lack technical knowledge about currency features, making counterfeit detection more accessible to the general public.

CHAPTER-3

RESEARCH METHODOLOGY

This project is conducted in two integrated phases to address the issue of counterfeit currency in India. The first phase focuses on analyzing the circulation trends of fake currency, while the second phase involves developing a machine learning-based system to detect counterfeit notes using image processing techniques.

PHASE I

ANALYSIS OF FAKE CURRENCY CIRCULATION IN INDIA

In this phase of the project, historical data on the circulation of counterfeit currency in India was collected from reputable and authoritative sources, including the Reserve Bank of India (RBI), the National Crime Records Bureau (NCRB), and various government reports. The compiled dataset included information on the number of counterfeit notes detected each year, their denominations, and the geographical distribution of incidents across different states and Union Territories. This data formed the foundation for understanding the scope and scale of Fake Indian Currency Notes (FICNs) in the country. Before analysis, the raw data underwent a cleaning process to remove inconsistencies, duplicate entries, and missing values. It was then standardized for uniformity in state names, date formats, and currency denominations to ensure accurate comparison and analysis.

Following data preparation, **Exploratory Data Analysis** (EDA) was conducted to uncover meaningful patterns and trends in the dataset. EDA focused on identifying how counterfeit currency activity varied across different years, regions, and denominations. For instance, peaks in seizure volumes were correlated with national events such as demonetization, while state-wise distributions helped highlight areas with consistently high counterfeit activity. This initial exploration allowed for deeper insights into the nature of FICN circulation and its evolution over time, as well as potential systemic weaknesses in currency security and enforcement.

To present these findings effectively, the study utilized a combination of visualization tools and techniques, including Tableau and IBM Cognos Analytics. These platforms were used to create interactive tree maps, heat maps, line charts, and Column graphs that visually depicted the intensity and progression of counterfeit note circulation. Visualizations enabled the identification of regional hotspots, such as Gujarat and Delhi, and highlighted peak periods, like the sharp spike observed in 2022. This visual approach not only enhanced the interpretability of the data but also made it easier to pinpoint where policy interventions or improved enforcement measures were most needed.

The research follows a **descriptive design**, as it seeks to systematically examine and explain the distribution and trends of FICN seizures rather than test a hypothesis or manipulate variables. The approach is primarily **quantitative**, relying on numerical data such as the count and value of fake notes detected by banks and law enforcement agencies across various regions. However, to add depth and context, the study also includes qualitative elements – such as expert commentary from credible sources. This blend of methods makes the study partially mixed-methods, although the core analysis remains **statistical**. Year-wise and state-wise data were compared using absolute values and percentage contributions, revealing the most affected areas and denominations. Analytical tools like Microsoft Excel and IBM Cognos played a central role in processing this data and generating insights that can inform future anti-counterfeiting strategies.

Despite a thorough analysis, the study is limited by its reliance on secondary data, which may not capture unreported or undetected counterfeit activity. Due to time constraints, no primary data (e.g., interviews with enforcement personnel) was collected. Additionally, differences in reporting standards across states/UTs and the lack of real-time data may affect the accuracy of comparisons. However, validity and reliability were ensured by sourcing data from trusted agencies like the RBI and NCRB, applying consistent methods, and cross-verifying findings with national events and expert insights.

3.I.1. Data Collection Method:

In this project, I have used **Secondary data**. Secondary data refers to information that has been previously collected, processed, and made available by other sources, rather than being directly gathered by the researcher for the current study.

Data Used	Source
Number of Counterfeit Notes Detected (April-March) Denomination-wise Counterfeit Notes Detected in the Banking System (April-March)	Reserve Bank of India: Annual Report – Currency Management
Seizure of Fake Indian Currency Note (FICN)	National Crime Record Bureau: 'Crime in India' publication.

Table: 1. Dataset used and its Sources

3.I.2. Tools Used for Analysis and Visualization:

Microsoft Excel: Microsoft Excel was used for the initial stages of data cleaning, preparation, and basic analysis. It helped organize large datasets, remove duplicates, fill in missing values, and standardize formats such as currency, state names, and dates. Excel's built-in functions and pivot tables allowed for quick computation of totals, percentages, and year-on-year comparisons of FICN seizures across states and denominations.

IBM Cognos Analytics: IBM Cognos Analytics was employed for advanced data visualization and statistical reporting. It enabled the creation of interactive dashboards and visual summaries such as column-line charts to display trends in the number and value of counterfeit notes detected over time. The platform also supported drill-down analysis, helping to explore data patterns in more detail by region, denomination, and year.

Tableau Public: Tableau Public was used to create engaging and intuitive visualizations like tree maps and heat maps. These visuals made it easier to identify regional hotspots of counterfeit activity and analyze the contribution of individual states to the national total. Tableau's user-friendly interface allowed for the seamless presentation of complex data trends in a format that is easy to interpret for both technical and non-technical audiences.

CHAPTER-4. I

DATA ANALYSIS AND INTERPRETATION

In India, fake currency notes are identified and seized by various law enforcement agencies, as well as detected by the Reserve Bank of India (RBI) and other commercial banks during their routine transactions. These institutions play a crucial role in curbing the circulation of counterfeit notes by flagging suspicious currency and initiating necessary actions.

In the following sections of this project, a detailed overview of Fake Indian Currency Notes (FICN) detected by banks and seized by law enforcement agencies is presented. This includes a comprehensive analysis of state-wise and year-wise trends, providing valuable insights into the patterns and intensity of counterfeit currency circulation across the country over time.

The data pictured in Table: 2 shows how many fake Indian currency notes were detected by Indian banks over the last 10 years, along with their total value in rupees.

Table: 2 Total FICN Detected by Banks and Its Value in last 10 Years		
Year	**Total Notes**	**Total value (Rupees)**
2014-15	5,94,446	28,66,94,200
2015-16	6,32,926	29,64,17,117
2016-17	7,62,072	43,46,75,590
2017-18	5,22,783	23,34,91,963
2018-19	3,17,384	8,23,59,960
2019-20	2,96,695	7,48,03,617
2020-21	2,08,625	5,45,00,111
2021-22	2,30,971	8,25,93,563
2022-23	2,25,769	7,98,71,130
2023-24	2,22,639	10,80,73,993
2024-25	2,17,396	7,81,27,810

Table: 2 Total FICN Detected by Banks and Its Value in last 10 Years

The Column-line chart in the Figure:1, Reflects the data shown in the Table:2 for better visual understand. The pink bars show the total value of fake notes each year, while the blue line shows the total number of fake notes found. The highest point was in 2016-17, when banks detected more than 7.6 lakh fake notes worth nearly ₹43.4 crore. This big spike happened because there were so many fake ₹500 and ₹1000 notes in circulation just before the government carried out demonetization.

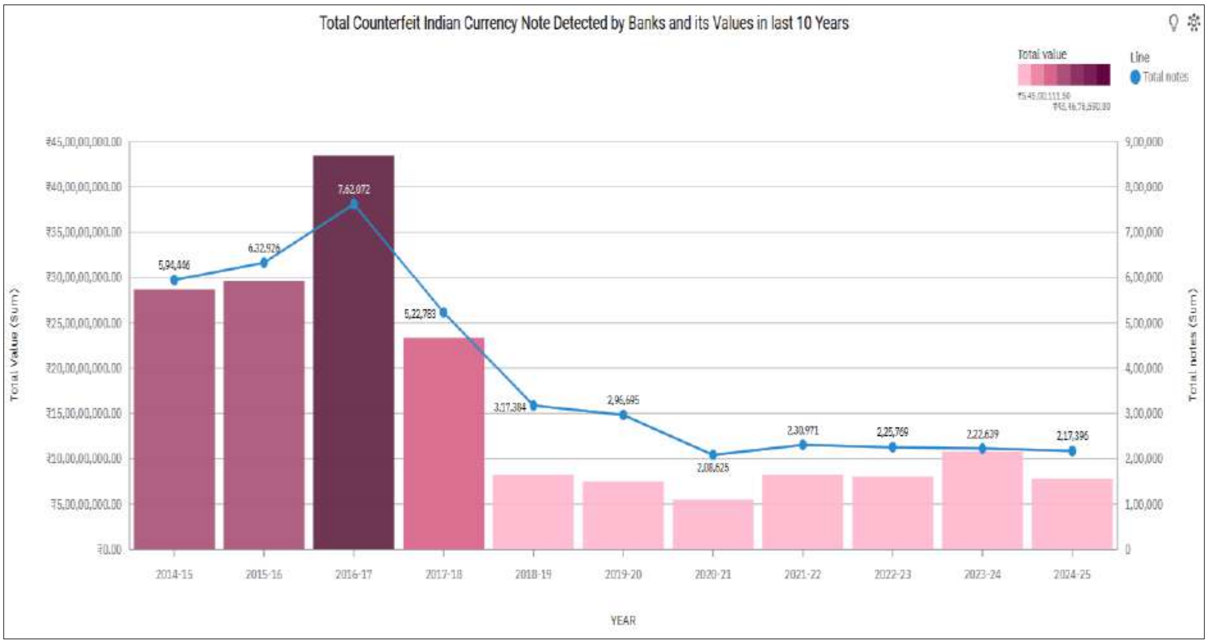

Figure:1. Counterfeit Indian Currency Notes Detected by Banks in last 10 Years

After demonetization in 2016, when old ₹500 and ₹1000 notes were banned, the number and value of fake notes dropped sharply. From 2017-18 onwards, the chart shows that both the number of fake notes and their value kept going down, with some small ups and downs. This shows that removing the old high-value notes really helped reduce fake currency. Even when new notes like ₹200 and ₹2000 were introduced, criminals continued to target them, but the scale of counterfeiting was much lower than before.

It's also important to know that this data only includes fake notes detected by Indian banks; including Reserve Bank of India. It does not count fake currency seized by the police or other enforcement agencies. So, the actual total might be even higher. In 2024-25, banks and the Reserve Bank found about 2.17 lakh fake notes worth around ₹8 crore. This means that while demonetization helped control the problem, counterfeit currency is still a challenge, and banks need to stay watchful to catch fake notes and protect the economy.

Table:3 presents denomination-wise fake Indian currency notes detected each year from 2014-15 to 2024-25, and whether they were caught by the Reserve Bank or other banks. It helps us understand which notes are most targeted by counterfeiters. The data present in the table only contains the details of counterfeit notes detected at the banks and does not include counterfeit notes seized by the police and other enforcement agencies.

Table:3a. Denomination-wise FICN detected by Banks					
Denomination (₹)	**Year**				
	2014 - 15	**2015 - 16**	**2016 - 17**	**2017 - 18**	**2018 - 19**
2 & 5	0	2	80	1	0
10	268	134	523	287	345
20	106	96	324	437	818
50	7,160	6,453	9,222	23,447	36,875
100	1,81,799	2,21,447	1,77,195	2,39,182	2,21,218
200	0	0	0	79	12,728
500	2,73,923	2,61,695	3,17,766	1,37,810	22,836
1000	1,31,190	1,43,099	2,56,324	1,03,611	717
2000	0	0	638	17,929	21,847
Detection at the Reserve Bank	26,128	31,765	32,432	1,88,693	17,781
Detection at Other Banks	5,68,318	6,01,161	7,29,640	3,34,090	2,99,603
Total	5,94,446	6,32,926	7,62,072	5,22,783	3,17,384

Table:3a. Denomination-wise FICN detected by Banks

Table:3b. Denomination-wise FICN detected by Banks						
Denomination (₹)	Year					
	2019 - 20	2020 - 21	2021 - 22	2022-23	2023-24	2024-25
2 & 5	22	9	1	3	1	3
10	844	304	354	313	235	159
20	510	267	311	337	297	253
50	47454	24802	17696	17755	15366	12015
100	168739	110736	92237	78699	66310	51069
200	31969	24245	27074	27258	28672	32660
500	30065	39462	79683	91116	85722	117727
1000	72	2	11	482	1	2
2000	17020	8798	13604	9806	26035	3508
Detection at the Reserve Bank	13530	8107	15878	10465	17613	10255
Detection at Other Banks	283165	200518	215093	215304	205026	207141
Total	296695	208625	230971	225769	222639	217396

Table:3b. Denomination-wise FICN detected by Banks

In recent years, the number of fake notes in India has shown some clear trends. Before demonetization in 2016, big notes like ₹500 and ₹1000 had the highest number of fake copies. For example, in 2016-17 alone, fake ₹500 notes crossed 3 lakh and fake ₹1000 notes were over 2.5 lakh, with a combined value of more than ₹41 crore. But after these old notes were banned in 2016, their fake numbers dropped sharply because they were no longer in circulation.

After that, new high-value notes like ₹200 and ₹2000 started being targeted by counterfeiters. Fake ₹2000 notes rose to over 26,000 by 2023-24. However, in FY25, there was a big dip in fake ₹2000 notes – dropping by about 86% from over 26,000 to just 3,508. This drop helped reduce the overall value of fake currency found by banks and the Reserve Bank. This happened because ₹2000 notes were withdrawn from circulation in May 2023, though they are still legal to use.

At the same time, fake ₹500 notes went up again from about 85,722 in FY24 to over 1.17 lakh in FY25, with their total fake value rising from around ₹4.3 crore to ₹5.9 crore. The ₹200 fake notes also increased by nearly 14% to over 32,000, showing that counterfeiters are shifting focus to other popular notes. ₹100 notes also remain among the most faked, with over 51,000 fake notes found because they are widely used in daily life. Small denominations like ₹10, ₹20, and ₹50 continue to have very low fake numbers every year.

Most fake notes, about 95% are caught by other banks during daily transactions, not directly by the Reserve Bank, which shows how important regular banks are in stopping fake currency from spreading. To improve security, a new Currency Research and Development Centre (CRDC) has been set up to test and upgrade the security features of Indian notes and develop better designs. Experts say criminals have become smarter at copying notes with better features that even fool sorting machines, so banks and the RBI must take stronger actions to tackle fake currency in the country.

The line chart in Figure:2 is a visual way to see what the Table:3 shows about fake currency. It clearly shows that fake ₹500 and ₹1000 notes were very high in 2016-17, just before demonetization, and then dropped sharply when the government banned old high-value notes. This proves how the policy directly reduced fake notes for those denominations.

After demonetization, new lines appear for ₹200 and ₹2000 notes. The chart shows that the ₹2000 note started getting faked more after 2017, reaching around 26,000 fake notes in 2023-24. The ₹200 note also shows a steady rise, which means counterfeiters quickly shifted to targeting new high-value notes. This trend highlights that whenever new notes come into circulation, they can also become a target for fake currency makers.

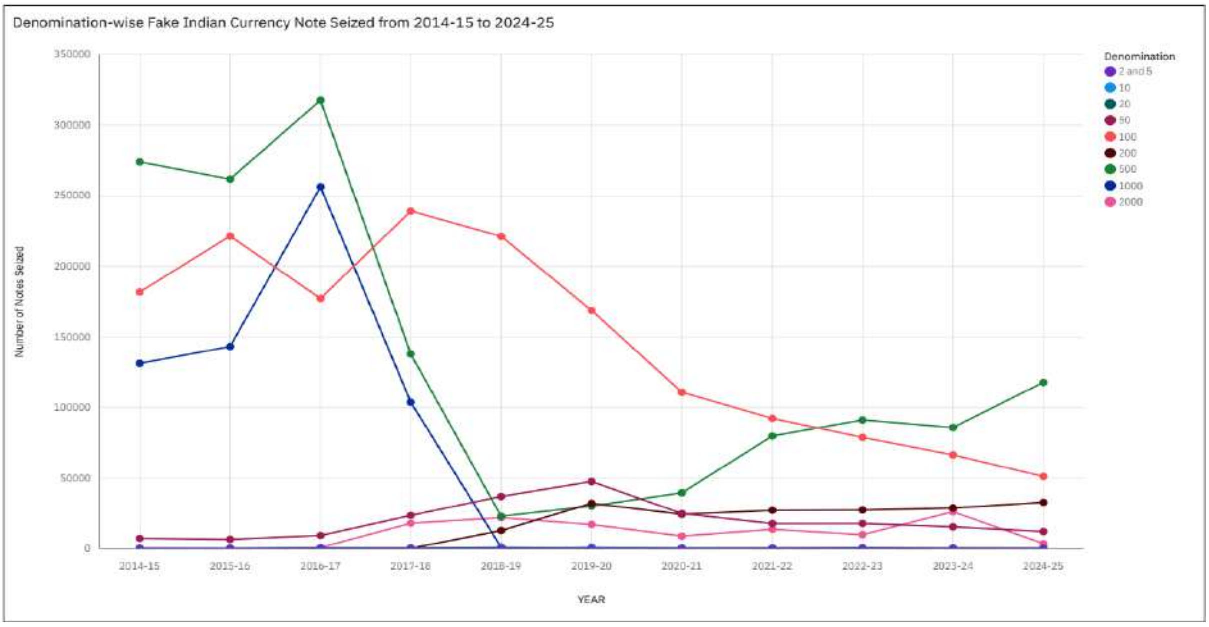

Figure: 2. Denomination-wise FICN Seized

Meanwhile, the line for ₹100 notes stays steady throughout the years, showing that fake ₹100 notes are always found because they are used so widely in daily life. In contrast, the lines for small notes like ₹2, ₹5, ₹10, and ₹20 stay almost flat at the bottom, proving they are hardly ever faked. Overall, the chart proves that total fake notes have dropped since demonetization, but counterfeiting still exists as criminals adapt to new currency notes.

As per the article published in Times of India on June 15, 2025. Former president of the Bank Employees Federation of India, C J Nandakumar, has raised concerns over the significant rise in fake ₹500 currency notes detected in the banking system during FY25. He warned that the growing circulation of counterfeit notes shows that criminals are becoming more advanced in designing fake banknotes that even escape detection by modern sorting machines.

“Criminals have become sophisticated in producing fake notes with security features that can bypass the systems banks use to detect counterfeits,” Nandakumar said. He stressed that while the Reserve Bank of India (RBI) has been issuing guidelines to tackle fake currency, stronger and more effective actions are needed. “The regulator must also initiate more stringent measures and closely supervise to curb the menace of Fake Indian Currency Notes (FICNs) in the country,” he added.

Table:4. State-wise and Year-wise FICN Seizure values (2016 – 2022) in Rupees								
STATE/UT	**YEAR**							**Total**
	2016	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	
Andhra Pradesh	92,80,000	1,21,79,954	1,11,28,450	3,70,85,600	1,44,50,550	1,47,21,300	23,26,140	10,11,71,994
Arunachal Pradesh	65,000	0	0	0	0	21,00,500	74000	22,39,500
Assam	8,00,050	89,00,510	28,96,280	12,17,850	645500	82,23,850	5652400	2,83,36,440
Bihar	37,36,800	28,13,750	9,56,750	8,43,500	111300	4,01,390	3917200	127,80,690
Chhattisgarh	0	12,40,070	19,68,200	9,97,650	2327560	1,69,600	1275130	79,78,210
Goa	17,000	74,500	0	0	0	26,000	0	1,17,500
Gujarat	2,37,24,050	9,00,88,850	1,23,28,672	3,77,44,010	8796490	1,01,42,780	3368750980	3,55,15,75,832
Haryana	1,95,900	2,87,450	4,63,000	1,03,200	1581500	13,55,600	85132650	8,91,19,300
Himachal Pradesh	28,500	3,88,000	3,30,200	0	0	9,500	2200	7,58,400
Jharkhand	7,06,000	0	0	0	0	3,60,900	0	10,66,900
Karnataka	80,09,136	52,98,880	1,71,08,300	4,78,26,150	2267150	90,88,950	87683560	17,72,82,126
Kerala	20,57,200	1,30,63,540	4,21,0740	83,43,700	2696750	1,95,03,000	472390	5,03,47,320
Madhya Pradesh	16,26,890	24,33,710	9,53,810	17,42,100	202200	82,60,500	489930	1,57,09,140
Maharashtra	47,99,700	52,39,650	1,15,31,970	1,92,18,450	836123400	1,63,09,750	1,79,46,000	91,11,68,920
Manipur	40,500	4,000	62,800	0	0	11,22,000	14,06,000	26,35,300
Meghalaya	38,000	0	0	0	14000	1,10,000	47,000	2,09,000
Mizoram	3,72,900	71,13,500	73,70,200	67,42,000	0	11,95,000	53,70,700	2,81,64,300
Nagaland	97,000	1,400	1,04,500	0	0	0	0	2,02,900
Odisha	2,74,700	1,50,550	6,200	0	0	0	0	4,31,450
Punjab	42,39,750	43,32,200	6,14,600	60,30,300	9580200	35,29,100	37,17,950	3,20,44,100
Rajasthan	10,35,100	10,24,100	39,66,600	61,65,650	27,34,950	21,74,940	4,10,09,800	5,81,11,140
Sikkim	0	0	0	0	0	0	0	0
Tamil Nadu	33,42,540	46,95,150	2,84,91,710	94,59,860	1,00,37,300	6,13,03,170	2,11,6910	11,94,46,640
Telangana	76,00,905	40,17,700	32,61,400	81,900	0	67,49,310	2,21,21,750	4,38,32,965
Tripura	29,200	0	8,500	26,600	4,820	91,000	1,21,500	2,81,620
Uttar Pradesh	50,13,700	2,86,49,860	1,33,28,860	77,67,810	38,79,260	44,71,900	59,84,250	6,90,95,640
Uttarakhand	6,66,400	5,36,200	1,41,200	10,200	0	3,76,100	7,71,100	25,01,200
West Bengal	2,32,95,800	1,93,66,070	2,10,95,600	3,17,43,450	2,46,27,250	1,12,31,500	77,56,940	13,91,16,610
A & N Islands	0	0	0	0	1,000	0	0	1,000
Chandigarh	14,99,000	0	0	0	0	40,000	0	15,39,000
D & N Haveli & Daman & Diu	0	0	0	0	0	0	0	0
Delhi	5,65,21,460	6,78,96,250	3,63,22,950	3,01,05,950	4,16,000	2,05,42,070	16,09,61,130	37,27,65,810
Jammu & Kashmir & Ladakh	1,30,100	12,11,450	8,85,500	4,82,500	12,83,300	3,17,100	20,500	43,30,450
Lakshadweep	0	0	0	10,800	0	0	0	10,800
Puducherry	6,900	12,000	0	1,900	0	850	2,42,500	2,64,150
NIA + CBI	0	0	0	1,58,000	0	1,600	12,98,100	14,57,700
STATE TOTAL	10,10,92,721	21,18,99,594	14,23,28,542	22,31,49,980	92,00,80,180	18,30,27,640	3,66,41,46,480	5,44,57,25,137
UT TOTAL	5,81,57,460	6,91,19,700	3,72,08,450	3,06,01,150	17,00,300	2,09,00,020	16,12,24,130	37,89,11,210
INDIA TOTAL	15,92,50,181	28,10,19,294	17,95,36,992	25,39,09,130	92,17,80,480	20,39,29,260	3,82,66,68,710	58,26,094,047

Table:4. State-wise and Year-wise FICN Seizure values (2016 – 2022)

The data in the Table:4 shows a detailed analysis of Fake Indian Currency Notes (FICN) seized across Indian states and Union Territories (UTs) from 2016 to 2022. The analysis is based on data published by the National Crime Records Bureau (NCRB) in its report 'Crime in India' and visualized using a heat map and tree map. The aim is to understand year-wise trends and state-wise distribution of FICN seizures, identify high-risk regions, and examine potential patterns or anomalies in counterfeit currency circulation.

During this 7-year period, between 2016 and 2022. India recorded a total FICN seizure of ₹5,82.60 crore, with ₹5,44.5 crore coming from states and ₹37.8. crore from UTs. Gujarat reported the highest seizure value in the country at ₹355.16 crore, significantly higher than any other state. Other top-ranking states include Maharashtra (₹91.11 crore), Delhi (₹37.2 crore), Karnataka (₹17.7 crore), West Bengal (₹13.9 crore), and Tamil Nadu (₹11.94 crore), all of which indicate major areas of counterfeit circulation or successful enforcement activity. This thing can be seen in the Figure:3.

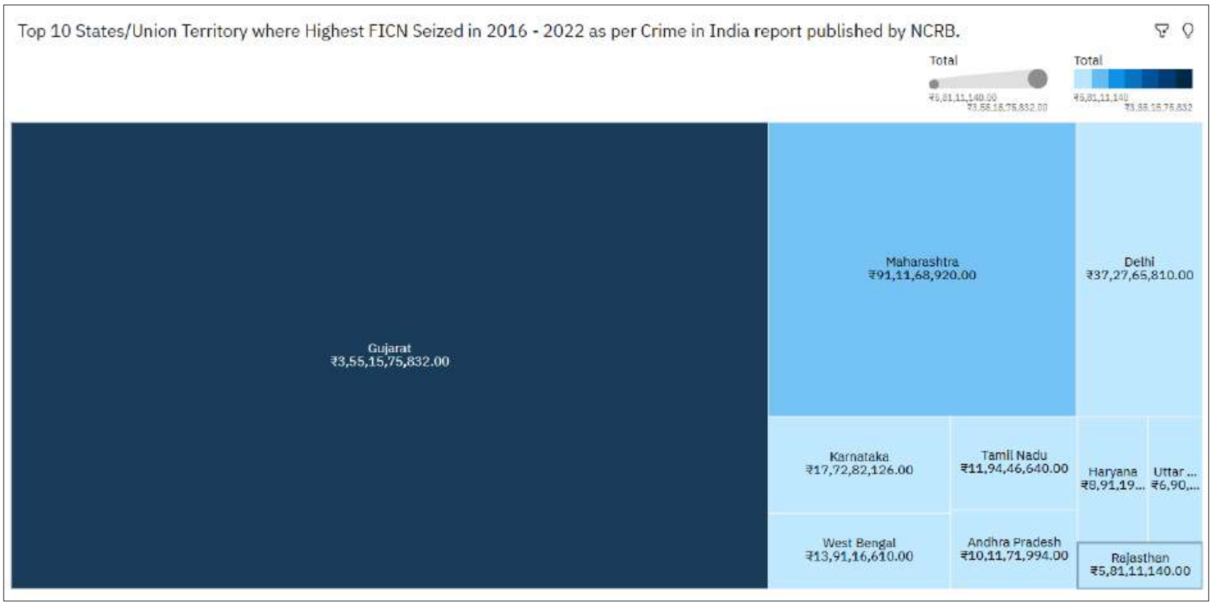

Figure: 3. Top 10 States/UT where highest FICN Seized (2016 – 2022)

The tree map in the Figure:3 visualizes the top 10 States/Union Territories in India with the highest total value of Fake Indian Currency Notes (FICN) seized from 2016 to 2022, based on NCRB data. Gujarat stands out overwhelmingly with seizures worth ₹355.16 crore, making it the largest contributor by far. Maharashtra follows with ₹91.17 crore, and Delhi ranks third with ₹37.28 crore. The chart highlights the significant disparity between Gujarat and the rest, indicating either a concentrated counterfeit network or major enforcement breakthroughs in the state.

When we analyze year-wise trends, we see relatively moderate values from 2016 to 2019, followed by a sharp spike in 2020 when seizures shot up to ₹92.1 crore. This could reflect heightened enforcement, changes in counterfeit operations, or broader availability of counterfeit notes post-demonetization. There was a drop in 2021, with ₹20.39 crore seized, but 2022 witnessed a massive surge to ₹3,82.66 crore, accounting for more than 65% of the total counterfeit currency seized in all seven years. Gujarat alone contributed ₹336.87 crore in 2022, helping explain this sharp national increase.

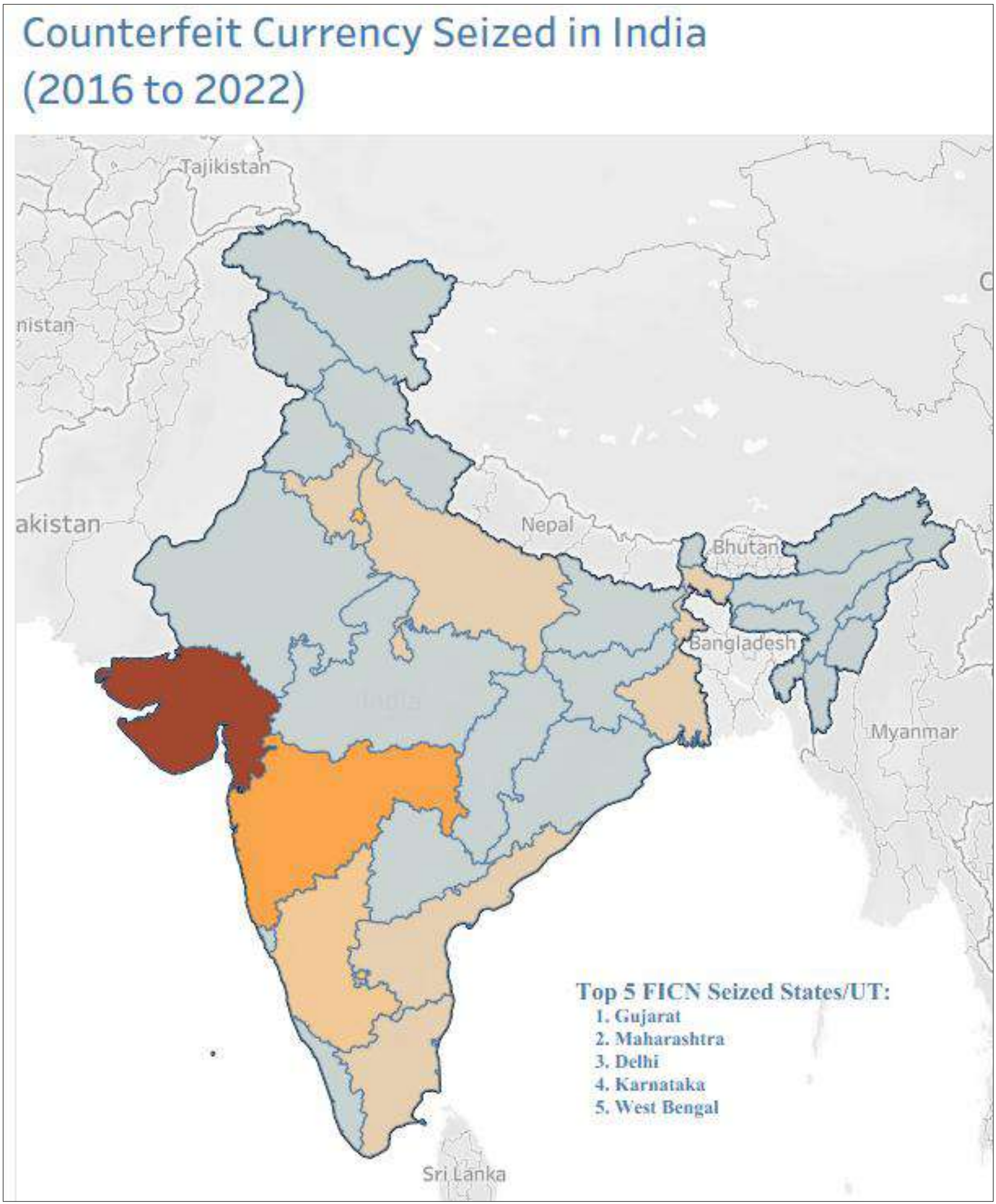

Figure: 4. Counterfeit Currency Seized in India (2016-22)

Most smaller states and UTs, such as Sikkim, Goa, Odisha, Puducherry, Lakshadweep, and the Andaman & Nicobar Islands, showed either very low or zero reported seizures. However, Delhi, a Union Territory and national capital, accounted for ₹37.27 crore – nearly the entire UT total, making it a major hotspot for FICN activity. Its high value may reflect its economic significance, urban complexity, and central role in inter-state transactions. Overall, the table reveals both geographical concentration and temporal spikes in FICN activity, highlighting the need for targeted policy measures and inter-state collaboration to counter this threat.

Table:5. Top 15 State/UT with Highest Value of FICN seized (2016 – 2022)		
Sl. No.	**STATE/UT**	**Total value of FICN seized**
1	Gujarat	3551575832
2	Maharashtra	911168920
3	Delhi	372765810
4	Karnataka	177282126
5	West Bengal	139116610
6	Tamil Nadu	119446640
7	Andhra Pradesh	101171994
8	Haryana	89119300
9	Uttar Pradesh	69095640
10	Rajasthan	58111140
11	Kerala	50347320
12	Telangana	43832965
13	Punjab	32044100
14	Assam	28336440
15	Mizoram	28164300

Table: 5. Top 15 State/UT with Highest Value of FICN seized (2016 – 2022)

The map in the Figure:4, visually represents the state-wise intensity of Fake Indian Currency Notes (FICN) seizures across India from 2016 to 2022, with darker shades indicating higher volumes of counterfeit currency recovered. Gujarat stands out prominently with the darkest shade, highlighting its top position with the highest total FICN seizure of over ₹355 crore during the seven-year period. Other states like Maharashtra, Delhi, Karnataka, and West Bengal also feature among the top five and are shaded in progressively lighter yet still intense tones, reflecting substantial counterfeit seizures ranging from ₹13 crore to ₹91 crore. These states, due to their size, economic activity, and transit routes, may experience more circulation of counterfeit currency or have stronger enforcement and detection systems.

The data also brings attention to regional patterns. Border states such as West Bengal, Punjab, and Assam show consistently high seizure figures, which may be attributed to cross-border smuggling from neighbouring countries – a known route for counterfeit inflow. On the other hand, smaller states and Union Territories, such as Sikkim, Lakshadweep, Andaman & Nicobar Islands, and Daman & Diu, report either minimal or no FICN seizures. This could be due to lower levels of economic activity, less circulation of high-denomination currency, or limited law enforcement capabilities. Notably, Union Territories as a group saw a significant rise in 2022, with Delhi alone contributing the majority of the ₹16 crore seized, underlining its importance as a central hub in the counterfeit currency network.

CHAPTER: 5.I.

FINDING AND DISCUSSION

The analysis of counterfeit currency circulation in India between FY2014–15 and FY2024–25 reveals several notable trends. The most significant spike in counterfeit note detection occurred in FY2016–17, when over 7.6 lakh fake notes valued at approximately ₹43 crore were seized, largely due to the widespread circulation of fake ₹500 and ₹1000 notes prior to demonetization. Following this policy intervention, there was a sharp decline in both the number and value of fake notes, demonstrating demonetization's immediate deterrent effect. However, counterfeiters quickly adapted, shifting their focus to newly introduced denominations like ₹200 and ₹2000. The rise in fake ₹2000 notes continued up to FY2023–24 but declined sharply in FY2024–25 due to the RBI's decision to withdraw ₹2000 notes from circulation.

Denomination-wise, ₹100 notes consistently appeared among the most counterfeited, likely because they are widely used in everyday transactions, making them an easy target. Lower-value notes such as ₹10, ₹20, and ₹50 showed relatively minimal forgery, reflecting limited profitability for counterfeiters. An important operational insight is that commercial banks detected over 95% of all fake notes, underscoring their frontline role in counterfeit detection, while the Reserve Bank of India (RBI) played a smaller but significant role in spotting high-quality fakes during central processing.

At the state level, Gujarat recorded the highest seizure value of ₹355.16 crore between 2016 and 2022 – far exceeding all other states. Other major contributors to counterfeit seizures included Maharashtra, Delhi, Karnataka, and West Bengal. A massive surge in FICN was seen in 2022, with seizures reaching ₹3,826 crore nationally, accounting for nearly 65% of the total seven-year figure. This unprecedented increase was primarily driven by Gujarat's data that year, possibly due to enhanced enforcement or the exposure of a large counterfeit network.

Geographic visualizations such as heat maps and tree maps further revealed that counterfeit activity was concentrated in economically active and border states, such as West Bengal, Punjab, and Assam, possibly due to smuggling from neighbouring countries. Conversely, smaller states and Union Territories like Sikkim or Daman & Diu reported negligible seizures, while Delhi emerged as a notable hotspot despite being a UT, with over ₹37 crore in seizures, highlighting its strategic importance in counterfeit distribution networks.

PHASE II

DETECTION OF FAKE CURRENCY USING IMAGE PROCESSING AND MACHINE LEARNING

In the second phase of the project, the focus is on detecting counterfeit currency using image processing and machine learning techniques. The analysis is based on the Banknote Authentication Dataset, which includes statistical features – such as variance, skewness, kurtosis, and entropy – extracted from images of both genuine and counterfeit banknote-like specimens.

The approach used in our proposed system is based upon physical appearance of the currency. Image processing algorithms have been adopted to extract the features such as kurtosis, skew and entropy which will identify the pattern in the currency note which will determine the originality of the note. A Python-based system is developed to automate this detection process by using these statistical features to train and evaluate a range of classification models. The dataset is split into training and testing subsets in a 70:30 ratio, and model performance is assessed using standard metrics. Finally, the most accurate model is deployed in a user-friendly Python application that allows users to input either note images or feature data and receive real-time classification results, determining whether a banknote is genuine or counterfeit.

The model in our project was trained using the Banknote Authentication Dataset, which we collected as a secondary data and it was originally collected by Helene Doerksen from the University of Applied Sciences, Ostwestfalen-Lippe, Germany, in August 2012. As a result, our Python-based application is currently unable to accurately detect the authenticity of currency notes introduced after 2012. This limitation can be addressed by updating the model with a more recent and comprehensive banknote authentication dataset.

3.II.1. Research Design Flowchart:

In the context of our Detection of Fake Currency Using Image Processing and Machine Learning project, a Data Flow Diagram (DFD) serves as a valuable graphical tool to visualize how information – such as an uploaded currency note image – flows through the system and undergoes a series of transformations to produce a final result. It represents the logical flow of data from the moment a user submits a note to the point where the system classifies it as either real or fake.

DFDs are extremely useful for understanding how our system functions and play a key role during the analysis and design phase of the project. To handle the complexity of the application, the DFD can be organized hierarchically using levelled DFDs, which break down the system into smaller, more manageable components. This layered approach makes it easier to analyze, explain, and refine each part of the currency detection process. The basic structure of a DFD, sometimes referred to as a data flow graph or bubble chart, allows us to illustrate each major step in the process.

Level-0 DFD:

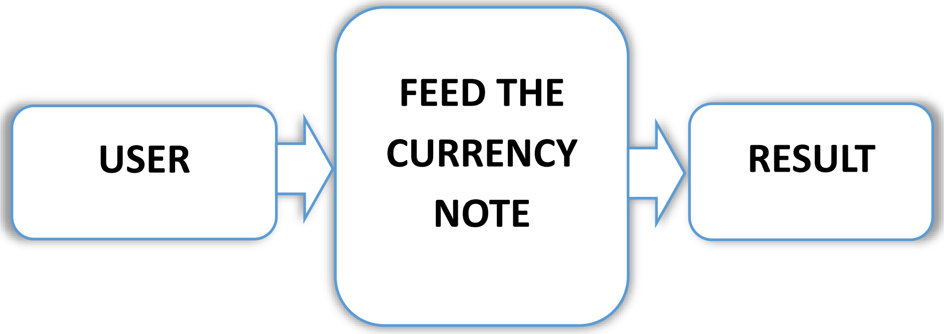

Figure: 5. Data Flow Diagram Level-0

The Level-0 DFD, also known as the context-level diagram, presents a high-level overview of the fake currency detection system. It shows the interaction between the user and the system in the most simplified form. The user feeds the currency note into the system, and in return, the system processes the input and gives the output – identifying whether the note is real or fake. This level hides the internal workings and focuses only on the primary data exchange. We can see detailed working process in Level-1 Data Flow Diagram in later part of this research.

3.II.2. Data Collection Method:

In this project, I used **Secondary Data** from various online sources which is mentioned below.

Data Used	Source
Banknote-authentication dataset	OpenML
Various Real & Counterfeit currency notes images	Kaggele

Table:6. List of Collected Data and their Sources

The Banknote Authentication dataset is used to differentiate between genuine and counterfeit banknotes. The data was derived from images of both real and forged banknote-like specimens. For digitization, an industrial camera typically used for print inspection was employed, capturing images at a resolution of 400 x 400 pixels. Owing to the lens type and the distance from the objects, high-resolution grayscale images (approximately 660 DPI) were obtained. Features were then extracted from these images using the Wavelet Transform technique.

3.II.3. Technologies Used:

- Python
- Django
- HTML
- CSS
- JavaScript

Python:

Python is a simple, high-level, and general-purpose programming language that is easy to learn and widely used. Created by Guido van Rossum, it is an interpreted and dynamically typed language, meaning we don't need to declare variable types. Python supports multiple programming styles, including object-oriented, procedural, and functional programming. Its clear syntax and flexibility make it ideal for scripting, rapid application development, and building a wide range of applications. Python is used in almost every technical field, including data science, data mining, desktop and console-based applications, mobile apps, software development, artificial intelligence, web development, enterprise applications, 3D CAD, and machine learning. Since there's no need for a separate compilation step, development and debugging in Python are fast and efficient.

Python Libraries and modules used:

Module/Library	Purpose
django.contrib.auth	Handles user login, logout, session tracking, and password hashing. Essential for secure user authentication.
django.shortcuts	Provides helper functions like render() to load templates with data and redirect() to change views after actions like login.
django.conf	Allows access to project-level configurations in settings.py, such as paths, debug mode, and media/static URLs.
pathlib	Offers object-oriented path operations, improving readability and platform compatibility over os.path.
os	Enables file and directory manipulation, accessing environment variables, and building dynamic file paths.
glob	Finds all files matching a pattern (e.g., .jpg, .csv) and is useful for working with folders containing multiple files.
cv2 (OpenCV)	Reads, displays, processes images (e.g., edge detection, blurring), used here to prepare images for ML input.
numpy	Performs mathematical and statistical calculations on image arrays (e.g., variance, mean). Key for image analysis.
PIL.Image (Pillow)	Opens and converts image files, often used to process uploaded images from users before analysis.
pyautogui	Automates mouse/keyboard actions
pandas	Used for reading, cleaning, and manipulating data (e.g., from CSVs). Handles the Banknote Authentication dataset.
matplotlib.pyplot	Generates charts and visual plots (e.g., displaying uploaded note and processed image in the result page).
seaborn	Built on matplotlib, creates statistical visualizations like pair plots and count plots, aiding in EDA.
sklearn.model_selection	Contains train_test_split() to divide dataset into training and testing subsets for fair evaluation of ML model.
sklearn.preprocessing	StandardScaler normalizes data to have mean=0 and std=1; MinMaxScaler scales features to a defined range.
sklearn.linear_model	Implements machine learning models like LogisticRegression, which is used here to classify currency as real or fake.

sklearn.metrics	Evaluates ML model performance using tools like confusion_matrix, which shows true/false positives and negatives.
scipy.stats	Provides statistical measures such as kurtosis, skew, and entropy of image data for ML feature extraction.
statistics	Offers basic statistical operations (mean, median, mode); imported but not used, so can be removed.
base64	Converts binary data (e.g., image files) into text format (Base64) for web transmission and embedding into HTML.
io, StringIO	Allows in-memory stream handling; StringIO is used to convert matplotlib plots into SVG format for web display.

Table:7. List of Python Libraries and modules

Django:

Django is a popular web application framework written in Python, based on the MVT (Model-View-Template) design pattern. It is well-known for its rapid development capabilities, allowing developers to build web applications quickly after gathering client requirements. Django is designed to handle much of the configuration automatically, so developers can focus more on writing the application itself. Its tagline, “The web framework for perfectionists with deadlines,” reflects its focus on speed and efficiency.

Django is a powerful Python-based web framework known for its rapid development, security, and scalability. It includes built-in tools like user authentication, admin panels, and support for RSS feeds and site maps. Django is versatile, allowing developers to build various applications such as content management systems, social networks, and scientific tools. As an open-source framework, it’s free to use and backed by a strong, supportive community.

HTML:

HTML stands for HyperText Markup Language and is used to create web pages and web applications. “HyperText” means text that contains links to other web pages, allowing users to navigate between them easily. A “markup language” is a type of computer language used to format and organize text in a document, helping to make it more interactive by adding elements like images, tables, and links. A web page is a document written in HTML that is displayed by a web browser and can be either static or dynamic. HTML is simple to learn and use, with many formatting tags that help create well-structured and visually appealing pages. It allows links, images, videos, and sound to be added, making web pages more engaging. HTML is platform-independent, meaning it works on different operating systems like Windows, Linux, or Mac. It is also case-insensitive, so tags can be written in either uppercase or lowercase.

CSS:

CSS stands for Cascading Style Sheets and is used to control the look and formatting of web pages written in HTML or other markup languages. It adds styling features like colours, fonts, layouts, and spacing to web pages, making them more visually appealing. CSS is often used with HTML and JavaScript to create modern, interactive websites and user interfaces, including for mobile apps. One of the main benefits of CSS is that it allows you to change the design of an entire website by editing just one file, saving a lot of time and effort. Before CSS, styles had to be written on every individual HTML page, which was time-consuming. CSS also offers more design options than HTML alone. It helps web pages load faster by reducing repeated code and makes it easier to maintain and update websites, since changes in one CSS file can update styles across all pages instantly.

JavaScript:

JavaScript is a lightweight, object-oriented programming language used to make web pages interactive. It is an interpreted language, meaning it runs directly in the browser without needing to be compiled. First introduced in 1995 for the Netscape Navigator browser, JavaScript is now supported by all major web browsers. It allows users to build modern web applications that can update content without reloading the entire page. Despite its name, JavaScript is not related to the Java programming language – the name was just a marketing choice at the time. JavaScript is also used beyond web browsers in databases like CouchDB and MongoDB. It is case-sensitive, follows a syntax similar to the C language, and supports object-oriented programming using prototypes. JavaScript works on different operating systems like Windows and macOS and gives users control over browser behaviour. Common uses of JavaScript include form validation, dynamic drop-down menus, showing dates and times, and creating pop-up messages and clocks on websites.

3.II.4. Requirement Analysis:

This section outlines the essential requirements for implementing the system. The goal of the requirement analysis is to identify the necessary resources while keeping them minimal and efficient. To ensure smooth performance of all features, the system should meet the below mentioned hardware and software requirements.

Hardware Specification	
RAM (Random Access Memory)	< 4 GB
Storage	< 512 GB
Processor	< 2 GHz

Table:8. Hardware Specification

Software Specification	
Operation System	Windows 10 and above
Programming Language	Python
IDE (Integrated Development Environment)	Visual Studio
Web Browser to test	

Table:9. Software Specification

CHAPTER-4. II

DATA ANALYSIS AND INTERPRETATION

4.II.1. Research Implementation Flowchart:

The Level-1 Data Flow Diagram expands on the Level-0 (Figure:5) by breaking down the internal processes involved in the system. The Level-1 Data Flow Diagram (DFD) shown in the figure:6, illustrates the internal process flow of the fake currency detection system in a clear and simplified manner. The process begins with the user input, where a user uploads or feeds an image of a currency note into the system. This serves as the entry point for the application, initiating the detection pipeline.

Level-1 DFD:

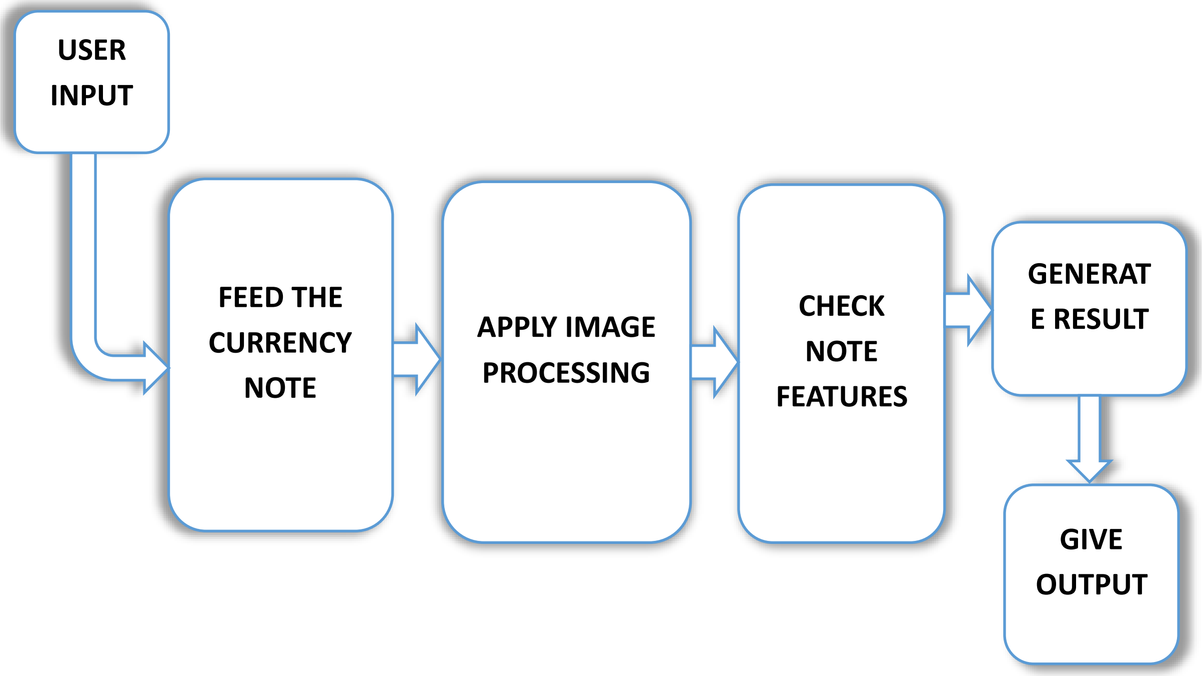

Figure:6. Data Flow Diagram Level-1

Once the currency note is fed into the system, image processing techniques are applied to enhance and prepare the image for analysis. This stage involves converting the image into a usable format and extracting statistical features such as variance, skewness, kurtosis, and entropy. These features are essential in detecting the texture and design characteristics that help distinguish fake notes from genuine ones.

- **Variance**: Variance measures how much the data points in a dataset differ from the average (mean) value. In image or data analysis, higher variance means the values are more spread out, while lower variance means they are closer together.
- **Kurtosis**: Kurtosis tells us how sharp or flat the peak of the data distribution is. A high kurtosis indicates more extreme values (heavy tails), while low kurtosis means the data is more evenly distributed with fewer outliers.
- **Skewness**: Skewness shows whether the data is tilted to one side. If the skewness is positive, the data leans to the right (more low values), and if it's negative, it leans to the left (more high values). A perfectly balanced dataset has zero skewness.
- **Entropy**: Entropy measures the randomness or complexity in data. In image processing or signal analysis, higher entropy means more disorder or detail in the image, while lower entropy indicates a simpler or more uniform pattern.

Feature	What It Measures	Project Purpose
Variance	Spread of pixel values	Identifies uniformity or contrast in textures
Skewness	Asymmetry in distribution	Detects unusual shading or inconsistent printing
Kurtosis	Sharpness of distribution	Captures edge clarity and presence of details/noise
Entropy	Randomness or information	Measures complexity or simplicity in the note design

Table:10. List of Features and their Purpose

The next phase is feature checking, where the system evaluates the extracted features and uses a trained machine learning model to classify the currency note. Based on the model's prediction, a result is generated, which is then displayed to the user. This final output indicates whether the uploaded currency note is real or fake, thus completing the detection process. This flow ensures a logical, efficient, and automated method for identifying counterfeit notes.

4.II.2. Python Coding:

```python
from django.contrib.auth import authenticate, login
from django.shortcuts import render, redirect
import pickle
from django.conf import settings
import os
from pathlib import Path
import cv2
import numpy as np

import pathlib
from PIL import Image
import os, os.path
import glob
import base64
from io import StringIO
import io
import cv2
import base64
import numpy as np
from PIL import Image
import matplotlib.pyplot as plt
import pyautogui as pag

import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import StandardScaler
from sklearn.linear_model import LogisticRegression
from sklearn.metrics import confusion_matrix

import cv2
from scipy.stats import kurtosis, skew,entropy
import numpy as np
from scipy import ndimage
import statistics
import base64

BASE_DIR = Path(__file__).resolve().parent.parent

def index(request):

    if request.method == "POST":

        data = pd.read_csv('banknote_authentication.txt', header=None)
        data.columns = ['var', 'skew', 'curt', 'entr', 'auth']
        print(data.head())

        sns.pairplot(data, hue='auth')
        sns.countplot(x=data['auth'])
        target_count = data.auth.value_counts()

        nb_to_delete = target_count[0] - target_count[1]
        data = data.sample(frac=1, random_state=42).sort_values(by='auth')
        data = data[nb_to_delete:]

        x = data.loc[:, data.columns != 'auth']
        y = data.loc[:, data.columns == 'auth']
        x_train, x_test, y_train, y_test = train_test_split(x, y, test_size=0.3, random_state=42)

        scalar = StandardScaler()
        scalar.fit(x_train)
        x_train = scalar.transform(x_train)
        x_test = scalar.transform(x_test)

        clf = LogisticRegression(solver='lbfgs', random_state=42, multi_class='auto')
        clf.fit(x_train, y_train.values.ravel())
```

```python
        y_pred = np.array(clf.predict(x_test))
        conf_mat = pd.DataFrame(confusion_matrix(y_test, y_pred),
                                columns=["Pred.Negative", "Pred.Positive"],
                                index=['Act.Negative', "Act.Positive"])
        tn, fp, fn, tp = confusion_matrix(y_test, y_pred).ravel()
        accuracy = round((tn+tp)/(tn+fp+fn+tp), 4)



        try:
            my_uploaded_file = request.FILES['my_uploaded_file'].read()
            my_uploaded_file_base64 = base64.b64encode(my_uploaded_file)

            print('loaded')

            def stringToImage(base64_string):
                imgdata = base64.b64decode(base64_string)
                image = Image.open(io.BytesIO(imgdata))
                return image

            def stringToEdgeImage(base64_string):
                imgdata = base64.b64decode(base64_string)
                image = Image.open(io.BytesIO(imgdata))
                #img_gray = cv2.cvtColor(np.array(image), cv2.COLOR_BGR2GRAY)
                img_blur = cv2.GaussianBlur(np.array(image), (3,3), 0)
                sobelxy = cv2.Sobel(src=img_blur, ddepth=cv2.CV_64F, dx=1, dy=0, ksize=5)
                return np.array(sobelxy)

            ######
            opencvImage = cv2.cvtColor(np.array(stringToImage(my_uploaded_file_base64)), cv2.COLOR_RGB2BGR)
            norm_image = cv2.normalize(opencvImage, None, alpha=0, beta=1, norm_type=cv2.NORM_MINMAX, dtype=cv2.CV_32F)

            img_blur = cv2.GaussianBlur(norm_image, (3,3), 0)
            sobelxy = cv2.Sobel(src=img_blur, ddepth=cv2.CV_64F, dx=1, dy=1, ksize=5)
            #sobelxy = cv2.imshow('sobelxy', sobelxy)

            var = np.var(norm_image,axis=None)
            sk = skew(norm_image, axis=None)
            kur = kurtosis(norm_image, axis=None)
            ent = entropy(norm_image, axis=None)
            ent = ent/100



            from sklearn.preprocessing import MinMaxScaler
            scaler = MinMaxScaler(feature_range=(0, 1))
            result = clf.predict(np.array([[-0.91318,-2.0113,-0.19565,0.066365]]))
            result = clf.predict(np.array([[var,sk,kur,ent]]))
            print(result)

            out = ""
            if result[0] ==0:
                out = "Real Currency"
            else:
                out = "Fake Currency"

            ######

            fig = plt.figure(figsize=(3, 3))
            plt.axis('off')
            plt.imshow(stringToImage(my_uploaded_file_base64))

            imagedata = StringIO()
            fig.savefig(imagedata, format='svg')
            imagedata.seek(0)
            imagedata.getvalue()


            fig2 = plt.figure(figsize=(3, 3))
            plt.axis('off')
            plt.imshow(stringToEdgeImage(my_uploaded_file_base64))

            imagedata2 = StringIO()
            fig2.savefig(imagedata2, format='svg')
            imagedata2.seek(0)
            imagedata2.getvalue()
```

```
                if my_uploaded_file_base64 != None:
                    return render(request, "result.html",{'original_image':imagedata.getvalue(),
                        'edge_image':imagedata2.getvalue(),
                        'variance':"{:.2f}".format(var),
                        'skew':"{:.2f}".format(sk),
                        'kurtosis':"{:.2f}".format(kur),
                        'entropy':"{:.2f}".format(ent),
                        'accuracy':accuracy,
                        'result':result,
                        'out':out})
            except:
                print("Notes picture not loaded")
        return render(request, "index.html")

def result(request):
    return render(request, "result.html")
```

4.II.3. HTML Coding:

Code for Index page:

```
File  Edit  View  Git  Project  Debug  Test  Analyze  Tools  Extensions  Window  Help  Search  mysite
Select Startup Item...  Python 3.12 (64-bit)
index.html  views.py

<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-KyZXEAg3QhqLMpG8r+8fhAXLRk2vvoC2f3B09zVXn8C

    <title>Home</title>
  {% load static %}
  </head>

  <nav class="navbar navbar-dark bg-dark justify-content-center">
    <div class="container">
      <a class="navbar-brand" href="/">
      <img src="{% static 'myapp/icon1l.png' %}" alt="5" width="48" height="48">
        Fake Currency Identifier
      </a>
    </div>
      </nav>

  {% load static %}
  <body background="{% static 'myapp/bg1.png' %}" style="background-size: cover;background-repeat: no-repeat;background-attachment: fixed;">
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/js/bootstrap.bundle.min.js" integrity="sha384-U1DAWAznBHeqEIlVSCgzq+c9gqGAJn5c/t99JyeKa9xxaYpSvHU5aw
    <br><br>

     <section class="vh-100 gradient-custom">
      <div class="container py-4 h-90">
        <div class="row d-flex justify-content-center align-items-center h-100">
          <div class="col-12 col-md-8 col-lg-6 col-xl-5">
            <div class="card bg-dark text-white" style="border-radius: 1rem;">
              <div class="card-body p-3 text-center">

                <div class="mb-md-5 mt-md-4 pb-5">

                  <h2 class="fw-bold mb-1 text-uppercase">Select Notes</h2>
                  <p class="text-white-50 mb-5">Please select note picture by click on the below button:</p>

                  <form name="voterform" method="POST" enctype="multipart/form-data">
                    {% csrf_token %}


                  <div class="form-outline form-white mb-4">
                    <input type="file" id="my_uploaded_file" name="my_uploaded_file" accept="image/*">
                  </div>
                  <br>

                  <button class="btn btn-outline-light btn-lg px-5" name="login" type="submit">Check Now</button>

                  </form>
                </div>
              </div>
            </div>
          </div>
        </div>
      </div>
    </section>



  </body>
</html>
```

Code for Result page:

```html
<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-KyZXEAg3QhqLMpG8r+8fhAXLRk2vvoC2f3B09zVXn8C

    <title>Result Page</title>
  </head>
  {% load static %}
  <body>
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/js/bootstrap.bundle.min.js" integrity="sha384-U1DAWAznBHeqEIlVSCgzq+c9gqGAJn5c/t99JyeKa9xxaYpSvHU5aw

  <nav class="navbar navbar-dark bg-dark justify-content-center">
    <div class="container">
      <a class="navbar-brand" href="">
      <img src="{% static 'myapp/icon11.png' %}" alt="S" width="48" height="48">
       Fake Currency Identifier
      </a>
    </div>
      </nav>

<div class="row row-cols-1 row-cols-md-2 g-4 text-center" style="padding:50px;">
  <div class="col">
      <div class="card shadow-lg p-3 mb-5 rounded" style="background-color: white;">
      <div class="card-body">
        <h3 class="card-title">Uploaded Image Before Image Processing</h3>
        <p class="card-text">{{ original_image|safe }}</p>
      </div>
    </div>
  </div>
  <div class="col">
    <div class="card shadow-lg p-3 mb-5 rounded" style="background-color: white;">
      <div class="card-body">
        <h3 class="card-title">Edged Image After Image Processing</h3>
        <p class="card-text">{{ edge_image|safe }}</p>
      </div>
    </div>
  </div>
</div>

<div class="row row-cols-2 row-cols-md-4 g-4 text-center" style="padding:30px;">
  <div class="col">
      <div class="card shadow-lg p-3 mb-5 rounded" style="background-color: lightgray;">
          <div class="card-body">
              <h3 class="card-title">VARIANCE</h3>
              <p class="card-text">{{ variance|safe }}</p>
          </div>
      </div>
  </div>
  <div class="col">
    <div class="card shadow-lg p-3 mb-5 rounded" style="background-color: lightgray;">
      <div class="card-body">
        <h3 class="card-title">SKEWNESS</h3>
        <p class="card-text">{{ skew|safe }}</p>
      </div>
    </div>
  </div>
  <div class="col">
    <div class="card shadow-lg p-3 mb-5 rounded" style="background-color: lightgray;">
      <div class="card-body">
        <h3 class="card-title">KURTOSIS</h3>
        <p class="card-text">{{ kurtosis|safe }}</p>
      </div>
    </div>
  </div>
    <div class="col">
    <div class="card shadow-lg p-3 mb-5 rounded" style="background-color: lightgray;">
      <div class="card-body">
        <h3 class="card-title">ENTROPY</h3>
        <p class="card-text">{{ entropy|safe }}</p>
      </div>
    </div>
  </div>
</div>

<div class="row row-cols-2 row-cols-md-2 g-4 text-center" style="padding:30px;">
  <div class="col">
    <div class="card shadow-lg p-3 mb-5 rounded" style="background-color: lightgray;">
      <div class="card-body">
        <h3 class="card-title">ACCURACY</h3>
        <p class="card-text">{{ accuracy|safe }}</p>
      </div>
    </div>
  </div>
  <div class="col">
    <div class="card shadow-lg p-3 mb-5 rounded" style="background-color: lightgray;">
      <div class="card-body">
        <h3 class="card-title">RESULT : {{ result|safe }}</h3>
        <p class="card-text">{{ out|safe }}</p>
      </div>
    </div>
  </div>
</div>


  </body>
</html>
```

4.II.4. Output 1: Real Currency

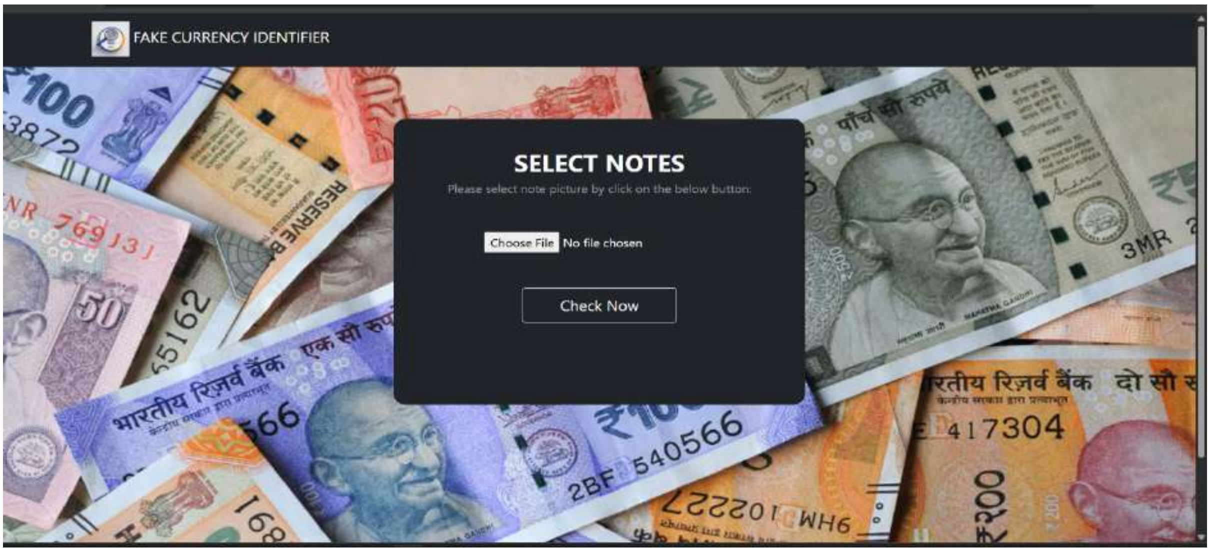

Figure:7. Output 1: Index page

Figure:8. Output 1: Uploaded image

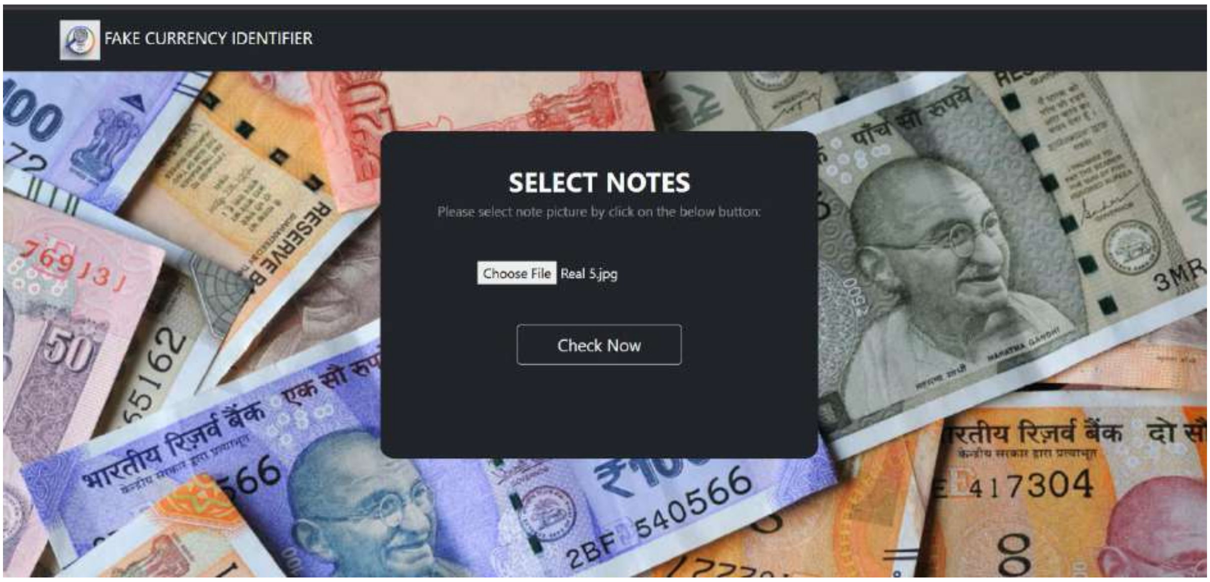

Figure:9. Output 1: Index page after uploading image

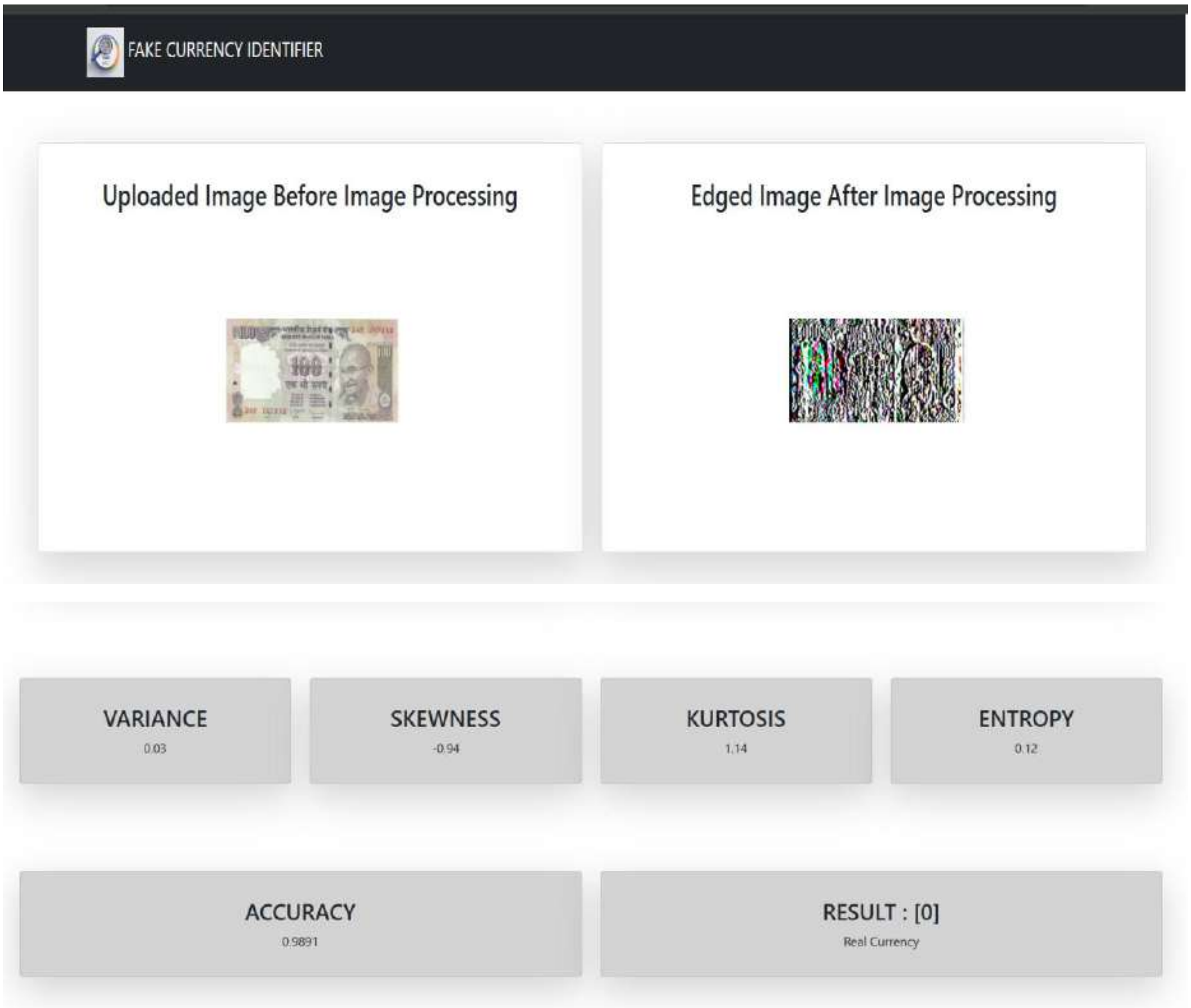

Figure:10. Output 1: Result page

4.II.5. Output 2: Fake Currency

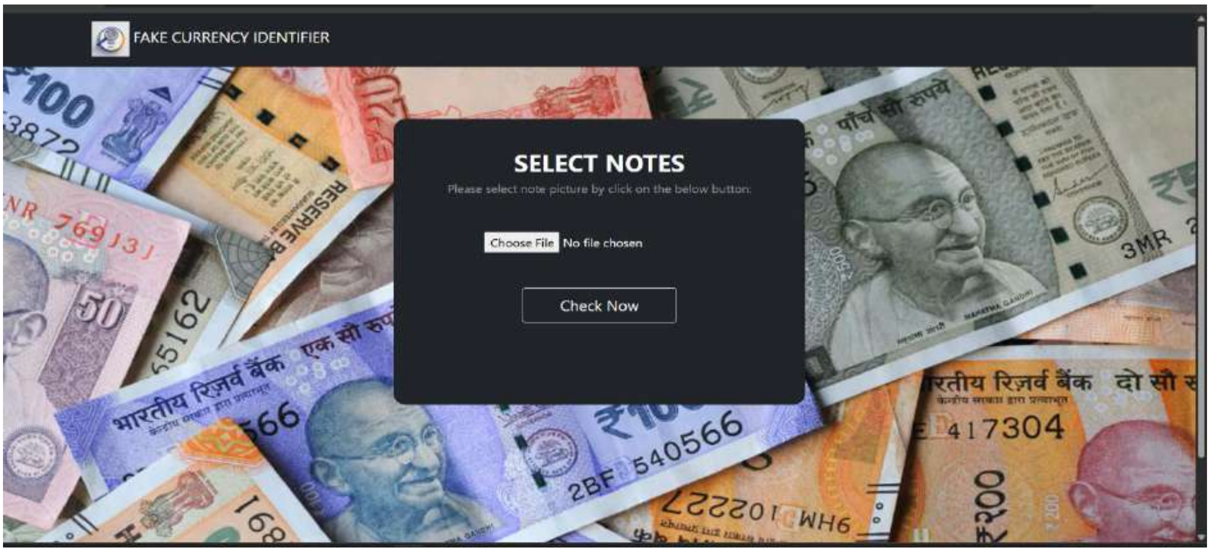

Figure:11. Output 2: Index page

Figure:12. Output 2: Uploaded image

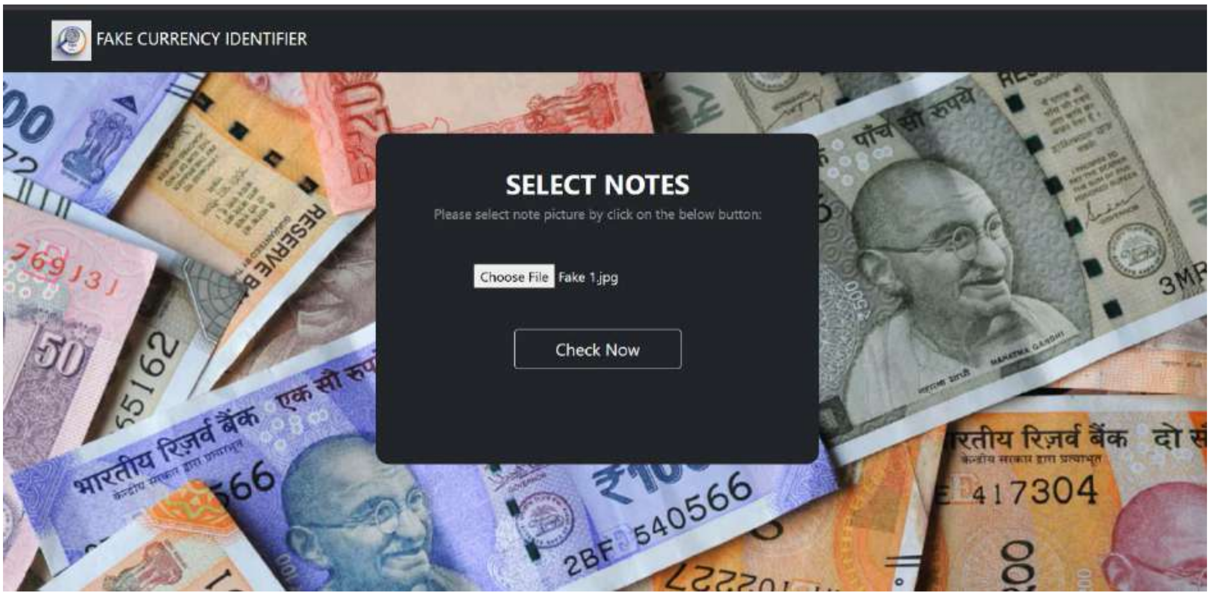

Figure:13. Output 2: Index page after uploading image

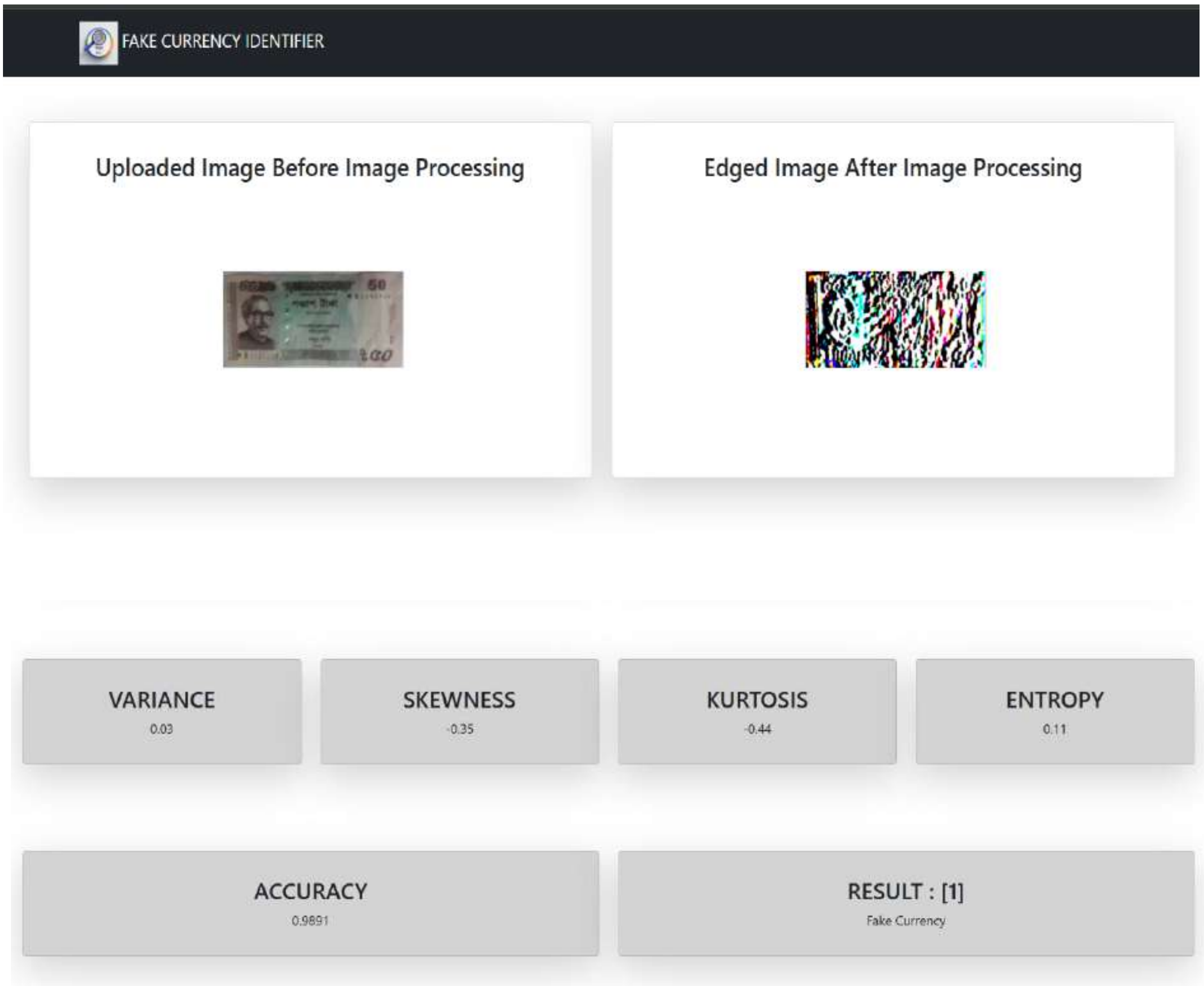

Figure:14. Output 2: Result page

CHAPTER-5. II

FINDINGS AND DISCUSSION

The implementation of the fake currency detection system using image processing and machine learning yielded highly promising results. Based on the uploaded outputs, the system was able to effectively distinguish between real and fake currency notes using key statistical features such as variance, skewness, kurtosis, and entropy extracted from note images. The processed images demonstrate clear edge enhancement, which highlights significant differences in texture and pattern details crucial for classification.

For instance, in one of the samples identified as fake currency, the features showed low kurtosis (-0.44) and negative skewness (-0.35), indicating a lack of detail and asymmetrical image data, common in counterfeit notes. On the other hand, the real currency sample displayed positive kurtosis (1.14) and higher negative skewness (-0.94), suggesting more refined image features and symmetrical distribution – consistent with original banknote designs. The entropy value was slightly higher for the genuine note, indicating richer information content.

The system achieved a remarkable accuracy of 98.91%, validating the effectiveness of the machine learning model in distinguishing between real and fake currency. These results highlight the model's potential as a reliable, real-time solution for counterfeit detection, particularly in automated kiosks, ATMs, or point-of-sale devices. Moreover, by providing transparent metrics along with visual and textual outputs, the system ensures clarity and confidence in its classification.

Overall, Phase II of this project demonstrates that combining image processing with statistical analysis and machine learning can deliver accurate, efficient, and user-friendly solutions to tackle the critical issue of counterfeit currency detection in India.

CHAPTER-6

CONCLUSION

The first phase of the study presents a comprehensive analysis of counterfeit currency trends in India over the past decade. It reveals that circulation of Fake Indian Currency Notes (FICN) is heavily influenced by policy decisions, regional enforcement efforts, and geographic factors. The 2016 demonetization exercise had a notable but short-lived effect, as counterfeiters rapidly shifted focus to newly introduced denominations like ₹500 and ₹2000. The consistent targeting of commonly used denominations such as ₹100 and ₹500 emphasizes the need for frequent updates to currency design and embedded security features to stay ahead of forgery techniques.

Additionally, the state-wise analysis uncovers major disparities in the detection and seizure of counterfeit currency, pointing to uneven enforcement capabilities and potential vulnerabilities along certain smuggling routes, particularly in border regions. These insights highlight the importance of strengthening inter-state coordination and enhancing detection infrastructure in high-risk zones. The findings serve as valuable input for policymakers, law enforcement agencies, and financial institutions in crafting region-specific countermeasures and improving the effectiveness of currency control strategies.

The second phase of the project successfully demonstrates the development of a highly accurate and cost-effective fake currency detection system using image processing and machine learning. By extracting key statistical features like variance, skewness, kurtosis, and entropy from scanned banknote images, the system achieves a classification accuracy of 98.91%. This Python-based application not only meets the primary objectives of the study but also proves its practical applicability in real-world scenarios. It can be deployed in retail outlets, banks, or public services to support quick and automated verification, thereby offering a scalable technological solution to reduce the risks of counterfeit currency circulation

CHAPTER-7

RECOMMENDATION

- **Strengthen Currency Design and Security:** Periodic updates to currency security features can help stay ahead of counterfeiters, especially for high-circulation denominations like ₹100 and ₹500.
- **Increase Awareness Among the Public:** Launch nationwide campaigns to educate people about identifying fake notes through visible security features.
- **Improve Cross-border Surveillance:** Deploy more resources at international borders to detect smuggling routes, especially in states like West Bengal, Punjab, and Assam.
- **Encourage Inter-agency Collaboration:** Improve coordination between the RBI, law enforcement, and intelligence agencies for faster detection, tracking, and dismantling of counterfeit networks.
- **Establish Specialized Anti-Counterfeit Units:** Set up dedicated task forces in states with high FICN activity for targeted operations and quicker response.
- **Enhance Detection Technology at Banks**: Invest in advanced currency sorting and scanning systems at commercial banks to improve detection rates.
- **Expanding Dataset**: Expand the dataset to include a wider variety of banknotes, counterfeit techniques, lighting conditions, and printing styles. Collaborate with financial institutions and government bodies for access to real-time and authentic data samples.
- **Real-time Implementation**: Optimize the algorithm for real-time deployment on edge devices (e.g., Raspberry Pi, embedded systems), enabling the system to be used in fast-paced environments such as retail counters or cash deposit machines.
- **Cross-validation and Pilot Testing**: Conduct pilot testing in partnership with banks or cash-intensive sectors to validate the system's performance under real-world conditions and refine it based on user feedback.
- **Enhancing Dataset**: As the current model is trained on pre-2012 data, it is essential to retrain and fine-tune the algorithm using updated datasets that include recent Indian currency notes, especially the new ₹500 and ₹2000 denominations, to ensure continued relevance and accuracy.

CHAPTER-8

LIMITATIONS

The first phase of the study is based entirely on secondary data from credible sources like the Reserve Bank of India (RBI) and the National Crime Records Bureau (NCRB). While these sources provide valuable insights, they may not account for all cases of counterfeit currency, especially those that go undetected or unreported. Additionally, discrepancies in data reporting standards across different states may affect the consistency and comparability of the results. The absence of real-time tracking data further limits the ability to capture ongoing counterfeit activity.

The second phase, which involves the development of a detection system, also has its constraints. The model was trained using a dataset based on pre-2012 currency notes, reducing its effectiveness when applied to newer denominations like the revised ₹500 and ₹2000 notes. Moreover, the study employed basic machine learning algorithms, while more advanced techniques such as Convolutional Neural Networks (CNNs) could potentially improve accuracy, particularly when dealing with complex forgery patterns or poor-quality images. The dataset sourced from OpenML and Kaggle may not reflect the most recent counterfeiting methods, thus impacting real-world applicability.

Time limitations were a significant constraint in both phases of the study. Due to these constraints, primary data collection methods such as field surveys or expert interviews with law enforcement and bank personnel could not be conducted. This limits the qualitative depth of the research and the opportunity to validate findings with first-hand insights from practitioners involved in counterfeit detection and currency regulation.

BIBLIOGRAPHY/REFERENCES

[1]. N R, Deepak, Nikhat Yasmeen, Nida S, “A Review on Fake currency detection using feature extraction” (February23,2022).
https://ssrn.com/abstract=4041599

[2]. Mr. Ratnesh K. Choudhary, Ms. Prachi Borate, Mr. Pravin Jaiswal, Ms. Shweta Gupta, & Mr. Vibhanshu Mandaogade. (2024). Literature Survey on Revolutionizing Fake Currency Detection: CNN-Based Approach for Indian Rupee Notes. *Journal of Image Processing and Intelligent Remote Sensing*, *4*(5), 15–24. https://doi.org/10.55529/jipirs.45.15.24

[3]. Gaikwad, Mayadevi A., Vaijinath V. Bhosle, and Vaibhav D. Patil. "Automatic Indian New Fake Currency Detection." International Journal of Engineering Research & Technology (IJERT) 6.11 (2017).

[4]. Kumar, Devid & Chauhan, Surendra. (2020). A STUDY ON INDIAN FAKE CURRENCY DETECTION. 8. 568-573.

[5]. Sharma, N., & Sharma, P. (2018). "An overview of counterfeit currency in India." International Journal of Management, Technology and Engineering, 8(1), 165-172

[6]. Naseem, Syeda Aimen, et al. "Counterfeit Recognition of Pakistani Currency." KIET, Journal of Computing and Information Sciences 6.1 (2023): 123-147.

[7]. Sharma, A. (2017). "Combating Counterfeit Currency in India: Issues and Challenges." Journal of Money Laundering Control, 20(3), 351-363.

[8]. Aakash S Patel, “Indian Paper Currency Detection” International Journal for Scientific Research and Development (IJSRD), vol 7, issue 06, ISSN: 2321-0613 (June 2019)

[9]. Vidhi Roy, Gangey Mishra, Rahul Mannadiar, Sushant Patil “Fake currency detection using image processing” (ICCSP). IEEE, 2019.

[10]. Devang S., Gujarathi, Sushii V. Nikam, currency recognition system for using image processing, “International journal of advance scientific research and engineering trends” volume 2.7 (2017).

[11]. Reserve Bank of India (RBI). (2021). “Detection and Reporting of Counterfeit Notes.” Retrieved from
https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10473

[12]. https://archive.ics.uci.edu/dataset/267/banknote+authentication

[13]. National Crime Record Bureau: ‘Crime in India’ publication.
https://www.ncrb.gov.in/crime-in-india.html

[14]. https://timesofindia.indiatimes.com/business/india-business/rs-2000-denomination-fake-currency-notes-dip-but-rs-500-counterfeit-notes-spike-in-fy25/articleshow/121837098.cms
[15]. https://timesofindia.indiatimes.com/business/india-business/fake-currency-note-detections-drop-for-third-year/articleshow/121494643.cms
[16]. https://www.data.gov.in/resource/denomination-wise-data-regarding-annual-percentage-increase-fake-currency-notes
[17]. https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=12814
[18]. Reserve Bank of India - Annual Report
https://rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1438
[19]. Directorate of Revenue Intelligence (DRI). (2021).
"Counterfeit Currency Notes." Retrieved from:
http://www.dri.nic.in/Content.aspx?pid=72
[20]. Indian Banks' Association (IBA). (2021).
"Guidelines for Detection of Counterfeit Notes." Retrieved from https://www.iba.org.in/Documents/Guidelines-For-Detection-Of-CounterfeitNotes.pdf
[21]. OpenML
https://www.openml.org/data/download/1586223/php50jXam