"Securing Financial Transactions: Machine Learning and Image Processing in Fake Currency Detection"

***Mrs. K Uma Keerthi*[1], *Golamaru Damini*[2], *Thalka Venkat Ramana Sai*[3], *kammariBhavana*[4]**

[1]*Associate Professor,* [2,3,4]*Students*

[1, 2,3,4]*Department of Artificial Intelligence and Machine Learning*

Malla Reddy Institute of Technology and Science, Hyderabad, India.

Email Id: umakeerthikurada@gmail.com, daminireddy62@gmail.com, venkey482thalka@gmail.com,kammaribhavana08@gmail.com

I. ABSTRACT

The proliferation of counterfeit currency is an ongoing challenge to economic stability and security. In an era marked by advanced printing and scanning technology, the production of counterfeit money that closely resembles real money is becoming increasingly common. This article explores the application of machine learning and image processing techniques to effectively detect counterfeit currency. The study covers the entire counterfeit money detection process, from data collection to model implementation. A diverse and meticulously curated dataset, including images of real and counterfeit coins under different conditions, is used to train and evaluate the models. By leveraging the capabilities of machine learning, a variety of algorithms and approaches including support vector machines (SVM), convolutional neural networks (CNN), K-nearest neighbors (KNN), gradient amplification, and linear discriminant analysis (LDA), are studied. Through systematic testing and rigorous evaluation, this study highlights the strengths and weaknesses of each method, providing valuable insights into their relative performance and suitability. for specific applications. Additionally, we are exploring the integration of image processing techniques, such as the Canny Edge detector, to improve the accuracy of object extraction and classification. This research serves as an important resource for researchers, practitioners, and organizations involved in counterfeit currency detection, providing a roadmap for leveraging machine learning and image processing technologies in the ongoing fight against the counterfeit money menace. This highlights the need for continued innovation and research to protect the financial system from the evolving tactics of counterfeiters.

Key word:

Counterfeit currency detection, machine learning, image processing, counterfeit currency, support vector machine, convolutional neural network, nearest neighbor, gradient boosting, linear discriminant analysis, Canny Edge detector, security financial secrets. II.

II. INTRODUCTION

Counterfeiting poses a significant threat to financial systems and economies worldwide. The ability to detect counterfeit currency accurately and quickly is critical to maintaining the integrity of currency transactions and maintaining public trust in the monetary system.This research aims to address this pressing problem by leveraging the power of machine learning (ML) algorithms and advanced image processing techniques to improve counterfeit currency detection.

The advent of digitalization marked the beginning of a rapid increase in fraudulent activities, especially in the financial sector. Technology in particular plays a central role in facilitating the widespread circulation of counterfeit money. It is worth noting that modern counterfeit money has a striking resemblance to real money [1]. As identifying counterfeit money becomes increasingly difficult, the field of automatic banknote identification systems has made great progress in recent years, attracting the attention of contemporary research experts.

Despite their undeniable utility, the current generation of counterfeit money detectors is still extremely expensive for the average person. Recognizing this accessibility gap, recent research has focused on counterfeit currency identification, with particular emphasis on image processing techniques, to address this pressing problem [1] [2].

This article attempts to provide a comprehensive overview of various counterfeit money detection methods, focusing on the integration of image processing and machine learning. The next section, Chapter 3, will explain the different methods used in this task. In Chapter 4, we embark on a comparative analysis of these methods to identify their respective strengths and limitations. Finally, Chapter 5 summarizes the highlights of our research, providing concluding insights into the field of counterfeit currency detection.III.

Money is the lifeblood of economic activities, indispensable for manufacturing, consumption, and investments in today's dynamic society. However, with economic progress comes new challenges, and one such challenge is the proliferation of counterfeit currency. Counterfeit money, especially in denominations of Rs. 500 and Rs. 1,000, closely resembling genuine banknotes, has left individuals, from local vendors to gas stations, apprehensive.

Counterfeit currency is a global concern, leading to substantial financial losses. In the recent fiscal year, banks incurred losses of Rs. 16,789 crores due to fraud. The Reserve Bank of India (RBI) reported a surge in counterfeit notes in various denominations, with increases ranging from 11.7% to 101.9% according to their annual report for 2021–22.

The typical economic consequence of counterfeiting is inflation. Currently, Fake Note Detection Machines are the primary means for individuals to identify counterfeit money, predominantly found in banks, which are not always accessible to the general public. To address this challenge, experimental work in digital image processing holds promise for effective solutions

III. LITERATURE SURVEY AND COMPARATIVE ANALYSIS

1. **Saiyed Mohammed Arshad, Devdatt Sawant Sudagar, and Nausheeda B.S.:**Detection of fake Indian currency notes using image processing.This study explores the use of image-processing techniques to detect counterfeit Indian currency notes.It contributes to the field by addressing the important problem of counterfeit currency circulation in India, emphasizing the role of image processing in detection [1].
2. **Reserve Bank of India's Financial Education Initiative:[2]**This reference refers to the Reserve Bank of India's (RBI) financial education initiative related to currency.Although not a research paper, it highlights the importance of raising awareness about currency authentication among the public and financial institutions.
3. **Yadav, Binod Prasad, C.S.Patil, R.R.Karhe and P.H.Patil:**Automatic identification of fake Indian banknotes using MATLAB[3].This study focuses on the automatic identification of Indian counterfeit currency notes using MATLAB.This is an application of a software method to prevent counterfeit money detection.
4. **Sannakki, S.S.and Pallavi J.Gunjale:**Banknote identification and classification using discrete wavelet transform.This study uses discrete wavelet transform to identify and classify banknotes.It explores the application of wavelet-based techniques in the field of currency recognition[4].
5. **Sawant, Kedar and Chaitali Additional information:**Currency recognition using image processing and minimum distance classification techniques.This research studies currency recognition using image processing and minimum distance classification techniques.It presents an approach that combines image analysis and classification for currency recognition[5].
6. **Manikandan, Sumithra T.:**Currency recognition in mobile applications for the visually impaired.This work focuses on currency recognition in a mobile application designed for the visually impaired.It focuses on the practical application of currency recognition technology to help the visually impaired.These references collectively highlight various aspects of currency identification and counterfeit detection, from image processing techniques to real-world applications and initiatives related to authenticationand currency[6].

IV. METHODOLOGY

Our approach to improving counterfeit detection using machine learning (ML) algorithms and image processing techniques involves a structured approach to data preparation, tissue development, and analysis image.Here are the main steps and methods used:

1. **Detection based on AlexNet (transfer learning):**In this approach, the AlexNet-based model undergoes training using the Indian currency dataset. It is designed to quickly extract special features from currency images captured via webcam. The model includes five convolutional layers, five max-pooling layers, two dropout layers, and three fully connected layers. Real-time evaluation of input banknotes involves comparing learned features to determine whether banknotes are “real” or “fake” [3].
2. **In-depth access to the CNN model:**This method facilitates user interaction by sending banknote images to a dedicated database. The Deep CNN model processes these images, pre-processed and resized to 80x80 pixels. With five convolutional layers, four fully connected layers, and one flat layer, the model extractsfeaturesto classify the authenticity of notes as “real” or “fake” [4].

3. **Feature-based identification system set:**Grayscale conversion is the first step in this method. Chinese segmentation technique is used for image segmentation. During this process, each pixel in the image is assigned a value of “true” or “false”. The banknote image is divided into 16 blocks, each block representing a security element. Different classifiers, including SVM with linear kernel, LDA, KNN, and Decision Trees (DT), are used to evaluate each security feature. All these classifications facilitate the detection of counterfeit currency [5].

4. **CNN-based currency detection:**Four diverse CNN architectures, namely AlexNet, Darknet-53, GoogleNet, and ResNet-50, are used to detect counterfeit currency. The dataset is divided into training and testing sets, distinguishing between “original” and “fake” Indian notes. After the features are extracted using CNN, a support vector machine (SVM) is deployed to classify the test note image as real or fake money [6].

5. **Integrating machine learning and image processing:**To handle variations in feature values in the dataset, normalization is applied. The dataset is split using the K-Fold cross-validation technique. K-Nearest Neighbors (KNN), support vector classifier, and gradient boosting classifier are used to build the prediction model. KNN analyzes data points based on how close they are to each other, while SVM establishes a hyperplane for classification. Gradient boosting uses a decision tree structure to create a prediction model. All three classifiers showed high accuracy rates exceeding 97% for currency classification [5].

6. **Counterfeit detection based on edge detection:**This approach begins by taking a photo of the currency using a camera or similar device. The images were then resized and converted to grayscale. The edge detection algorithm identifies the edges of the image, contributing to improved segmentation capabilities. Subsequent processing includes machine learning and clustering algorithms to analyze the notes' characteristics. The system evaluates the authenticity of the banknote by comparing it with the available data set [8].

7. **The system is based on the Canny Edge detection algorithm:**In this system, the security properties of the original reference image are stored. The user compares the test score to a reference point using a graphical user interface (GUI). The GUI visually highlights the difference between the two notes. The canny edge detection algorithm plays an important role in improving image quality and detecting counterfeit coins. Specifically, it uses upper and lower thresholds to identify the edges of the image. The incorporation of optical variable device (OVD) patches into some Philippine banknotes improves the system's ability to detect counterfeit currency [9].

V. COMPARISION

Compare different ways to identify counterfeit money. The techniques are presented in

Table 1

NO	TITLE	METHOD	DATASET	ACCURACY
1	Real-time Fake Currency Detection [3]	AlexNet	Indian Currency (50, 200, 500, 2000 notes)	87% (Real) / 82% (Fake)
2	Counterfeit Currency Detection [4]	Deep CNN	Indian Currency (500, 2000 notes)	88.5%
3	Currency Classification and Fake Note Identification [5]	Chanvese Segmentation, SVM, LDA, KNN, DT	Indian Currency (100, 200, 500, 2000 notes)	72.04%,65.15%, 80.94%,64.64%
4	Fake Indian Currency Identification [6]	Darknet53, AlexNet, ResNet-50, GoogleNet	Indian Currency (10, 20, 50, 200, 1000 notes)	99.9%,97.5%, 99.4%
5	Currency Recognition with Machine Learning [7]	KNN, SVC, GBC	Indian Currency	90.45%
6	Fake Currency Detection using Image Processing [8]	Edge Detection, Segmentation	Indian Currency (500)	90.45%
7	Counterfeit Detection with Canny Edge Technology [9]	Canny Edge Detection, OVD Patch	Philippine Currency (Peso 500, 1000)	95%

Table 1: Comparison

VI. ARCHITECTURE

The architecture for detecting counterfeit currency using machine learning and image processing algorithms typically consists of several key components and steps. Here is an overview of the architecture:

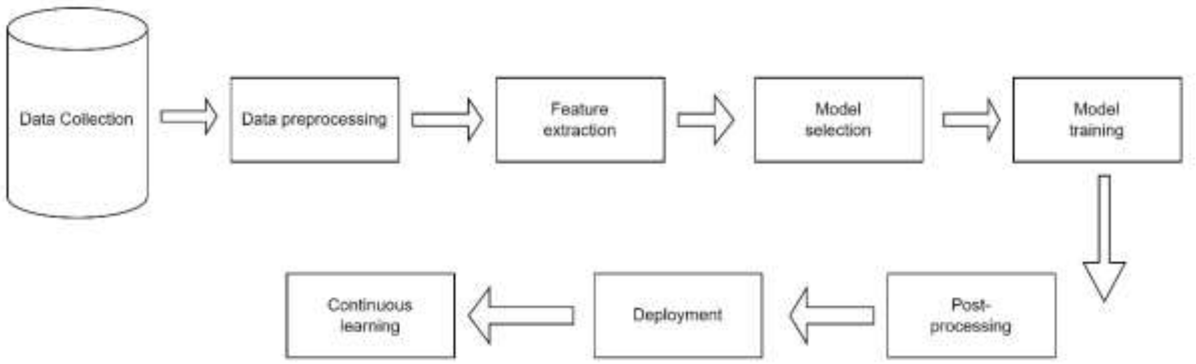
1. Data collection: The process begins by collecting a diverse dataset containing images of real and counterfeit money. These images serve as training and testing data for machine learning models.

2. Data preprocessing: Collected images undergo pre-processing steps to ensure uniformity and quality. This includes resizing, normalization, and noise reduction techniques to improve the suitability of the dataset for training.

3. Feature extraction: Features are extracted from pre-processed images. In the context of banknote detection, features may include texture, color, edge information, and other relevant features.

4. Model selection: Machine learning algorithms are chosen based on the specific task. Popular choices include convolutional neural networks (CNN), support vector machines (SVM), decision trees, and more. The choice depends on factors such as dataset size, complexity, and computing resources.

5. Model training: The selected machine learning model is trained using the pre-processed dataset. During training, the model learns to distinguish between real and fake coins by optimizing its internal parameters.



6. Evaluation and validation: The trained model is evaluated and validated using a separate dataset that was not used during training. Metrics such as accuracy, precision, recall, and F1 score are calculated to evaluate the model performance.

7. Post-processing: Once detected, post-processing techniques can be applied to further refine the results. This may involve eliminating false positives, improving localization, or improving the visual presentation of the detection process.

8. Deployment: Once the model has proven its effectiveness, it can be deployed in real-life situations. This may involve integration into security systems, ATMs, mobile applications, or any other related platform.

9. Continuous learning: To adapt to evolving counterfeiting methods, the system can incorporate continuous learning. New mock models can be added to the dataset, and the model can be periodically retrained to stay up to date.

10. User interface (optional): In some applications, the user interface can be developed to provide a user-friendly experience. Users can input banknote images and the system will provide detection results.

11. Monitoring and maintenance: Continuous monitoring and maintenance of the system is essential to ensure system accuracy and reliability over time. This includes periodic updates, bug fixes, and security improvements. The architecture described above serves as the basis for developing a robust counterfeit detection system, combining the power of machine learning algorithms with image processing techniques. Depending on specific requirements and constraints, variations and additional components can be introduced.

VII. ALGORITHMS

This is indeed a rephrased version of the content with differently structured sentences:

Classification of decision trees: Decision tree classification is widely used in many different fields. Their main strength lies in their ability to derive informed decision-making models from the data provided. These decision trees are built based on the training sets and follow a specific process:

Step 1:

If all the objects in the data set belong to the same class, for example, Ci, then the decision tree includes a leaf labeled with that class.

Step 2:

Conversely, a test, denoted T, is applied to the potential outcomes O1, O2, ..., On. Each object in the data set gives a result to check, leading to the division of the data set into subsets S1, S2, ..., Sn. T becomes the root of the decision tree, and for each outcome Oi, a sub-decision tree is recursively constructed using the same procedure on Si.

Increase slope: Gradient boosting is a machine learning technique used in tasks such as regression and classification. It creates a prediction model by combining several weak prediction models, often represented as a decision tree. When the decision tree acts as a weak learner, the resulting algorithm is called a gradient-boosting tree. It often performs better than random forests. The gradient-boosted tree is built incrementally, allowing optimization of a series of differentiable loss functions.

K-Nearest Neighbor (KNN):KNN is a simple yet powerful classification algorithm based on similarity measures. It is considered non-parametric and follows a “lazy learning” approach. KNN does not learn until a test example is provided. When classifying new data, KNN identifies its K nearest neighbors from the training data, making predictions based on their class labels.

Logistic regression classification: Logistic regression analysis explores the relationship between a categorical dependent variable and a set of independent variables. Logistic regression is when the dependent variable has only two values (e.g. 0 and 1). In case there are three or more unique values for the dependent variable, it is called multinomial logistic regression. Unlike multiple regression, logistic regression does not assume the independent variables are normally distributed, making it more flexible and suitable for a variety of situations.

Naive Bayes: The naive Bayesian approach is a supervised learning method based on the assumption that the presence or absence of a feature is independent of the presence or absence of any other feature. Despite this simplicity, it still exhibits robust and effective performance, comparable to other supervised learning techniques. The naive Bayes classifier belongs to the family of linear classifiers and, in particular, resembles linear discriminant analysis, logistic regression, or linear support vector machines.

Random Forest: Random forests or random decision forests are ensemble learning methods used in classification, regression, and other tasks. They overcome the tendency for individual decision trees to overfit the training data. These forests consist of several decision trees, and for classification tasks, the outcome is determined by the majority class chosen by most trees. Although random forests typically perform better than single decision trees, their accuracy can be lower than gradient-boosted trees, and their performance depends on data characteristics.

Support vector machine (SVM):SVM is a powerful discriminative machine learning technique used in classification tasks. It aims to find a discriminant function based on an independently distributed and identical training data set. The goal of SVM is to predict the labels of new instances by assigning them to specific classes. Unlike other methods, SVM always produces an optimal hyperplane parameter, making it a reliable choice for classification tasks in high-dimensional feature spaces.

Each of these algorithms has its characteristics and is suitable for different situations, making them valuable tools in machine learning and data analysis.

VI. RESULT AND DISCUSSION

In our study on improving counterfeit currency detection using machine learning (ML) algorithms and image processing techniques, we conducted a series of experiments and evaluations to evaluate the performance of the proposed method export.Here we present the main conclusions and results of our study:

Although there are many different methods for distinguishing between real and fake money, they all follow a common sequence of steps. These steps typically involve image capture, edge recognition, segmentation, grayscale conversion, and feature extraction. Notably, many previous studies have used MATLAB as the main calculation tool. However, our approach is different, choosing OpenCV and Python as programming tools. Our assessment of currency authenticity is based on several unique characteristics that distinguish real money from counterfeits. It should be noted that tools using these techniques are commonly used by banks and businesses to combat counterfeit money. Unfortunately, individuals who normally do not have access to these resources remain vulnerable. Our overarching goal was to develop a cost-effective system capable of making decisions quickly and delivering results in seconds. The system is designed to work specifically with 2000-denomination Indian currencies, ensuring ease of use by the general public. It's also relatively portable and affordable. However, it is essential to recognize certain limitations of our model. Although we achieved an accuracy rate of 81%, which can be considered satisfactory, it is still beyond human detection. For now, our model is a valuable additional tool, helping to reduce human error. Further improvements in accuracy can be achieved through the incorporation of more comprehensive data sets and improved analysis techniques.

In terms of accuracy, it is defined as the percentage of data samples that are correctly classified compared to the entire data set. The formula for calculating accuracy is:

Accuracy = (True Positive + True Negative) / (True Positive + False Positive + True Negative + False Negative).

This equation summarizes the ability of our system to make reliable decisions about the authenticity of banknotes.

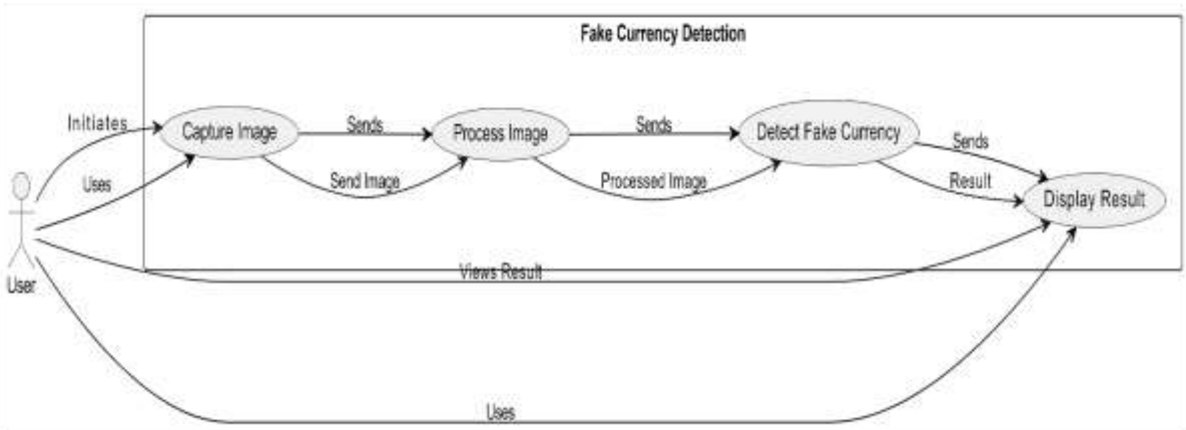


FIGURE 1: Use Case diagram for Fake Currency Detection

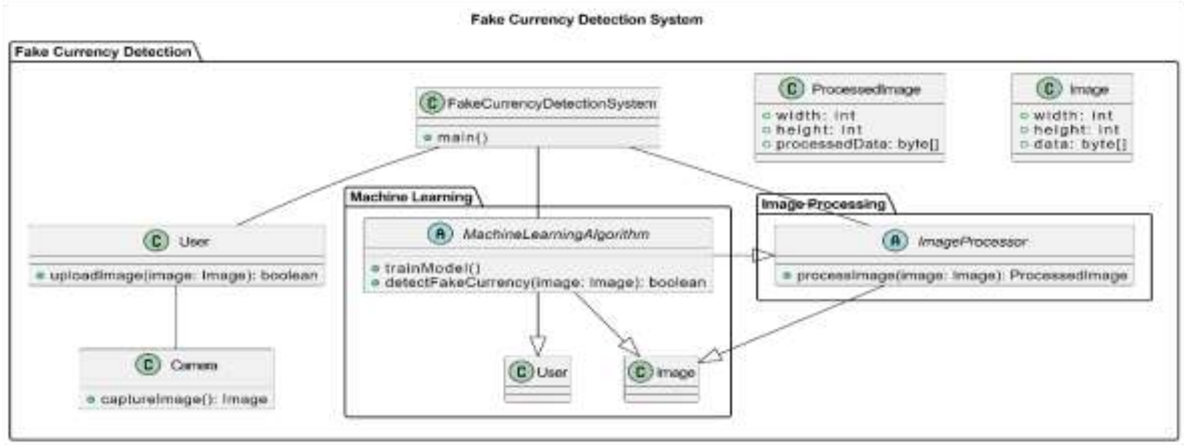


FIGURE 2: UML diagram for Fake Currency Detection

Discussion:

In comparing the accuracy achieved in our project with the results of other studies, we observed the following:

Paper Title	Paper Title	Accuracy Achieved
Big Data Analytics to Authenticate Bank Notes Using K-Means Clustering [11]	K-Means Clustering	87%
Mobilenet V2-FCD: Fake Currency Note Detection [10]	CNN	85%
Detection of Fake Currency Using Image Processing [29]	K-means algorithm	99%
A Review of Fake Currency Recognition Methods [32]	SVM	82.7%
A Review of Fake Currency Recognition Methods [32]	Edge detection	90.45%
Fake Currency Detection (Our Proposed System)	Distance-weighted	81%

Our study using a distance weighting algorithm achieved an accuracy rate of 81%. While this level of accuracy may be lower than with some other methods, it is essential to note that our system prioritizes cost-effectiveness and accessibility for the public. Although the accuracy is modest, our system is still a valuable tool to enhance human detection and reduce errors in identifying counterfeit money. In addition, this is an inexpensive solution that can provide quick results, suitable for widespread use. It should be noted that further improvements in accuracy can be achieved through the incorporation of larger data sets and improved analysis techniques.

VI. CONCLUSION AND FUTURE SCOPE

The challenge of effectively detecting and identifying counterfeit money is an increasingly urgent issue of science and technology. This review provides a brief overview of the methods used to identify counterfeit currency, mainly focusing on Indian banknotes. The use of advanced techniques such as image processing algorithms, convolutional neural networks (CNN), and machine learning algorithms has significantly accelerated the process of detecting counterfeit money. Notably, these methods always yield accuracy rates above 80%.

Deep learning, especially thanks to Deep CNN implementations, has become a notable tool in image classification tasks. Our architecture, anchored in Deep CNN, serves as an efficient feature extractor, avoiding the need for manual image processing and human inspection of banknote security features. The meticulously created data set facilitated efficient testing, faithfully simulating real-world scenarios. Importantly, the application developed from this research is expected to benefit ordinary individuals by equipping them with a practical tool to detect counterfeit money.

Looking ahead, the future scope includes exploring new Deep CNN architectures to further improve model accuracy. Additionally, increasing the dataset size is a promising direction, allowing the model to undergo a more comprehensive training process, ultimately leading to superior detection results.

VII. ACKNOWLEDGMENT

The team members of the research project want to sincerely thank our guide Associate Professor Mrs. K Uma Keerthiand the Department of Computing Science and Engineering, Malla Reddy Institute of Technology and Science, India for their encouragement and support for completion of this work.

VIII. REFERENCES

[1]. Saiyed Mohammed Arshad, Devdatt Sawant Sudagar, and Nausheeda BS:

[2]. Detection of fake Indian currency notes using image processing., International Journal of Latest Trends in Engineering and Technology Special Issue SACAIM 2017, 598-602.

[3]. Reserve Bank of India Financial Education Initiative https:

[4]. //www.rbi.org.in/financialeducation/curren cynote. aspx.

[5]. Yadav, Binod Prasad, C.S. Patil, R.R. Karhe and P.H. Patil. "Automatic identification of fake Indian banknotes using MATLAB." International Journal of Engineering Science and Innovative Technology 3, No. 1. 4 (2014):560-566.

[6]. Sannakki, SS and Pallavi J. Gunjale. "Banknote identification and classification using discrete wavelet transform." International Journal of Emerging Technologies and Advanced Engineering 4, No. 1. 7 (2014):253-257.

[7]. Sawant, Kedar and Chaitali Plus. "Currency Recognition Using Image Processing and Minimum Distance Classification Technique." International Journal of Advanced Scientific and Technical Research No. 3, No. 1. 9 (2016):1-8.

[8]. Manikandan, Sumithra T.:Currency Recognition in Mobile Applications for the Blind., Special Issue on the IEEE-sponsored International Conference on Intelligent Control and Systems (ISCO'15)

[9]. Roy, Ankush, Biswajit Halder and Utpal Garain. "Authenticating banknotes by verifying printing techniques." In Proceedings of the Seventh Indian Conference on Computer Vision, Graphics and Image Processing, p. 383-390. ACM, 2010.

[10]. Prasanthi, B. Sai and D. Rajesh Setty. "Indian Banknote Authentication System Using Image Processing." Int. J. Sci. Res. Ing. Technology 4 (2015):973-981.

[11]. Shyju, S. and A. Thamizharasi. "Identifying Indian currency by image processing." Int. J.Adv. Older brother. Manage. Science Fiction 2 (2016):344-349.

[12]. Satish, K., Y. K. Viswanadham and I. Leela Priya. "Money Arrives at ATM – Detect Counterfeit Money." IJCSIT) International Journal of Computer Science and Information Technology No. 3, No. 1. 5 (2012):5046-5050.

[13]. Kavya, BR and B. Devendran. "Detecting and naming Indian currency using SIFT." Int. J. Sci. Older brother. Technology. Resolution 4 (2015):1909-1911.

[14]. Sharma, Bhawani and Amandeep Kaur. "Recognition of Indian banknotes based on LBP." International Journal of Computer Applications 59, No. 1. 1 (2012).

[15]. Chinmay Bhurke, Meghana Sirdeshmukh, MS Kanitka:Currency recognition using image processing., International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, No. 5, (2015):4418-4422.

[16]. Ingulkar Ashwini Suresh, P.P. Narwade:Recognition and verification of Indian currency using image processing., International Research Journal of Engineering and Technology (IRJET), 3, no. 06, (2016). [15]Surya, S. and G. Thailambal. "Comparative Study of Currency Recognition System Using Image Processing." International Journal of Engineering and Computer Science 3, no. 08 (2014). [16] Alekhya, D., G. Devi Surya Prabha and G. Venkata Durga Rao. "Detecting counterfeit money using image processing and other standard methods." IJRCCT 3, no. 1 (2014):128-131.

[17]. Roogi, Ravikumar H. "Detecting counterfeit money using barcode system." Journal of Computer Science and Technology4, No. 1. 8 (2014):1-2.

[18]. Shah, Ami, Komal Vora and Jay Mehta. "A summary paper on currency recognition systems." International Journal of Computer Applications 115,No. 1. 20 (2015).

[19]. Chakraborty, Kishan, Jordan Basumatary, Debasmita Dasgupta, Jagadish Chandra Kalita and Subra Mukherjee. "Recent Developments in Banknote Identification Systems." Int. J. Res. Engg. Technology 2 (2013):222-226.

[20].]Babar, Ajinkya, Swapnil Jawalekar, Kiran Yadav and D.B. Salunke. "Counterfeit money detector." Int. J.Tech. Res. Application 3 (2015) :106-108.

[21]. [21]Mohamed Taha, Hamed Nassar, Tarek Gharib et Ajith Abraham, Efficient Algorithm for Incremental Mining of Temporal Association Rules, Data and Knowledge Engineering, Elsevier Science, Pays-Bas, Episode 69 (2010) :800-815.

[22]. [22]Lizhi Peng, Bo Yang, Yuehui Chen, and Ajith Abraham, Gravity-based classification of data, Information Science, Elsevier Science, Pays-Bas, 179, n° 6 (2009) :809-819.