Detection of Counterfeit Bank Notes

Mrutunjay Singh*, Preetam Ozarde† and Konidena Abhiram‡
Department of Electronics and Communication Engineering
Visvesvarya National Institute of Technology, Nagpur
{*iammrutunjaysingh, †preetamozarde3, ‡helixpocus}@gmail.com

***Abstract*—Currency counterfeiting is a significant offense which has a profound impact on the assets and capital of the citizens thus having an adverse effect on the nation's finances. The schemes currently existing to combat the falsification of banknotes are complex, hardware-based and inaccessible to the common people. In this paper, a unique authentication system is proposed which is compact, mobile and devoid of any hardware components. Certain security features, such as security thread and latent image, embedded on the note are utilized to help ascertain its legitimacy. The methodology involves the extraction and encoding of these security features. Given the prominence of the security thread in certain image planes, a clustering algorithm, k-means is applied for classification. The latent image, segmented via template matching was encoded using HOG descriptor and classified with an SVM model. The result is illustrated with the aid of performance parameters and overall accuracy.**

***Keywords* - HOG descriptor, K-Means clustering, Latent Image, Security Thread, SVM Classifier.**

I. INTRODUCTION

There is a growing concern among governments about using bank notes as a primary form of currency. Fig.1 illustrates the various statistics associated with the detection of counterfeit banknotes. The annual RBI report during the year 2015-2016 indicated that 632,926 pieces of counterfeit notes were detected in the banking system that year, of which 95 percent were detected by commercial banks [11]. This resulted in extreme measures being taken by the government of India. On November of 2016, the circulation of all Rs. 500 banknotes of the legal tender was terminated. The government believed this act would have a positive effect on the economy and have a severe impact in diminishing the use of fabricated notes to fund illegitimate businesses and terrorism.

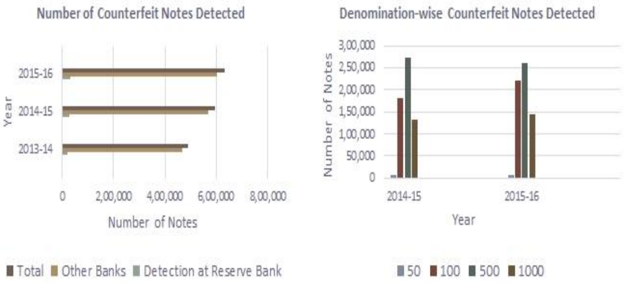

Fig. 1. Statistics on detected counterfeit banknotes [11]

The actual people who suffered from demonetization and the counterfeit currency are the common people. In the days following demonetization, the country was forced to endure acute cash shortages which inflicted further damage on the economy. The counterfeit notes reduce the value of real money in circulation. They also lead to a rise in the prices of various goods. Black marketing is also a cause of counterfeit currency. It is a part of a vicious circle of corruption that keeps eating away at both the economy and the trust of the people. Even though the demonetized currency was discarded the problem of counterfeit notes is not fully eradicated. The challenge of hunting down the counterfeiters is an arduous task due to their swift adaptation and proficiency in the use of advanced technology. Since most of the counterfeit notes were detected in commercial banks, an automated counterfeit currency detection tool would be helpful in preventing the use of such extreme measures in the future.

Various effective techniques have been developed based on certain properties of notes utilizing infrared spectroscopy [1], extraction of features when exposed to UV radiation [2] and exploitation of properties of light such as polarization and holographic techniques [3]. But the existing solutions to solve the counterfeit problem though effective are either computationally complex, hardware-based, expensive or most importantly inaccessible to the common people.

Hence we propose a cost-effective and robust automated counterfeit currency detection tool using image processing techniques which could be deployed for mobile applications. In this approach, we use a mobile camera to capture the image of the note whose authenticity is to be determined. The security thread and latent image embedded in the note are extracted. Certain image planes in which the security thread is conspicuous are isolated and a clustering algorithm, k-means is used for categorization [5][9]. Simple template matching gives the section of note containing the latent image which due to the presence of a pattern, consisting of lines and edges is encoded with a HOG (Histogram of Oriented Gradients) descriptor [7]. The Support Vector Machine (SVM) classifier obtains the optimum hyperplane and augments the distance from the decision boundary [10]. The SVM model is trained using a dataset and provides the decision on the authenticity of the note.

II. SECURITY FEATURES OF INDIAN BANK NOTES

The latest design of the bank notes is in contrast to the old Mahatma Gandhi Series in terms of colour, size and theme. The theme of the new series notes is India's heritage sites. There are various security features incorporated into the banknotes to protect them against counterfeiting as shown in Fig.2. Thus, the authenticity of a genuine currency note is predicated on the basis of these security features.

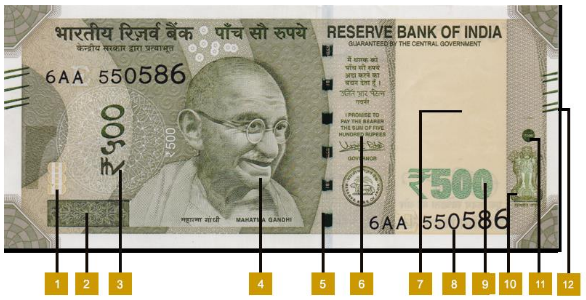
भारतीय रिज़र्व बैंक पाँच सौ रुपये
RESERVE BANK OF INDIA
GUARANTEED BY THE CENTRAL GOVERNMENT
6AA 550586
₹500
6AA 550586
1
2
3
4
5
6
7
8
9
10
11
12

Fig. 2. Rs 500 note along with security features

1) See through Register
2) Latent Image
3) Devanagari Script
4) Portrait of Mahatma Gandhi
5) Security Thread
6) Guarantee Clause
7) Electrotype Watermark
8) Number Panel
9) Denominational Number
10) Ashoka Pillar
11) Circle with 500 raised(Rectangle for 2000)
12) Bleed lines

The following security features, being abstract and intricate in their design are difficult to replicate and hence were used to determine whether the note is counterfeit:

1. **Security Thread**: The notes contain a security thread having distinct windowed characteristics and inscriptions of Bharat (in hindi) and RBI. When viewed against the light, it is seen as a continuous line. When the note is tilted, the security thread changes colour from green to blue.

2. **Latent Image**: In the notes, there is a horizontal band on the bottom left corner containing a latent image showing the respective denominational value in numeral. The latent image is visible only when the note is held horizontally at eye level.

III. PROPOSED METHODOLOGY

Since the security features of bank notes are different for each country, the counterfeit detection tool also differs based on the particular security features of the bank notes of that country. The proposed framework involves acquisition of the necessary image using a mobile camera followed by the required pre-processing, feature extraction and classification. The overall methodology is depicted in Fig. 3.

A. *Security Thread*

The approach and style associated with the stitching of security thread makes it a singular attribute. Also, the security thread does not fade with rough usage. Hence, this security feature is difficult to replicate. The pre-processing of the acquired image involved transforming the RGB image to YCrCb, LUV and HSV colour space so that the luma and chroma components could be separated [8].

The transformed YCrCb, LUV and HSV images were then split into their respective components

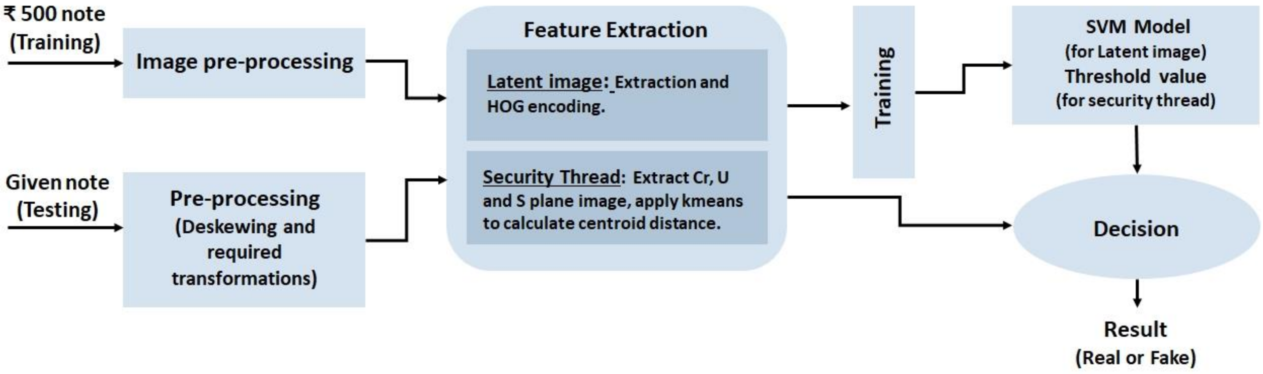

Fig. 3. Block diagram of overall methodology

from which Cr, U and S planes were used because of the clear visibility of security thread in these planes due to their unique colour characteristics. Given that the security thread was prominent in the Cr, U and S plane images for the real notes and not for the fake, further analysis of these images can be used to determine if the note is genuine. This is shown in Fig. 4.

In each image plane, two colours were dominant in the case of real notes, one of the background and another that of security thread. These colours were not distinct in the fake notes. Thus, for the purpose of classification, a clustering algorithm, k-means was employed. K-means is an algorithm that partitions n data points into k clusters. The mean of every cluster is termed its "centroid". Since the data points in a given cluster are deemed to be more comparable to one another than the data points that are in other clusters, we partitioned the dataset(image) into two clusters. The Euclidean distance between the centroids of the two clusters was calculated and was compared with the predetermined threshold value to categorize the note as real or fake. As we had three planes and their corresponding Euclidean distances between the centroids, weighted mean was employed to combine the individual results to produce a more robust output.

B. Latent Image

In order to get the proper orientation before segmenting out the latent image, the note was deskewed using affine transform [4]. The skewness of the image was calculated on the basis of its central moments using equation (1) [6], and the affine transform matrix (A) was determined according to equation (2).

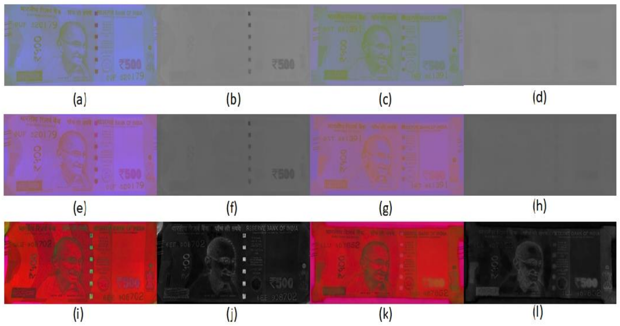

Fig. 4. (a) YCrCb image (Real note) (b) Cr-plane image (Real note) (c) YCrCb image (Fake note) (d) Cr-plane image (Fake note) (e) LUV image (Real note) (f) U-plane image (Real note) (g) LUV image (Fake note) (h) U-plane image (Fake note) (i) HSV image (Real note) (j) S-plane image (Real note) (k) HSV image (Fake note) (l) S-plane image (Fake note).

$$skew = \frac{\sum_{x,y} I(x,y).(x-\bar{x})^1(y-\bar{y})^1}{\sum_{x,y} I(x,y).(y-\bar{y})^2} \tag{1}$$

$$A_{2\times 3} = \begin{bmatrix} 1 & skew & -0.5 \times skew \times imageHeight \\ 0 & 1 & 0 \end{bmatrix} \tag{2}$$

After preprocessing, template matching was performed to segment the latent image. The following correlation formula was applied to find the best match of the standard template for comparison:

$$R(x,y) = \sum_{x',y'} T'(x',y').I'(x+x',y+y') \tag{3}$$

where

$$T'(x',y') = T(x',y') - \frac{1}{w \times h} \cdot \sum_{x'',y''} T(x'',y'') \quad (4)$$

$$I'(x+x',y+y') = I(x+x',y+y') - \frac{1}{w \times h} \cdot \sum_{x'',y''} I(x+x'',y+y'') \quad (5)$$

I = Image
T= Template image
w = width of template image
h = height of template image

The best location of the latent image was given by the maximum value of $R(x,y)$. When the segmented image was transformed to HSV space, the S-plane image was taken, as the features were seen more vividly in this plane. This is shown in Fig.5.

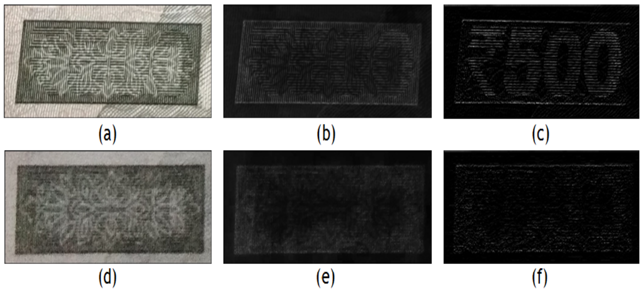

Fig. 5. (a) Extracted latent image from real note (b) S-plane of latent image of real note (c) Extracted pattern from S-plane image of real note (d) Extracted latent image from fake note (d) S-plane of latent image (fake note) (c) Extracted pattern from S-plane image of fake note

From Fig. 5 it can be observed that most of the information contained within the pattern is due to lines and edges and is present in real notes whereas it is distorted in the fake notes. Thus, to encode this feature, HOG descriptor was calculated with cell size 8×8 and normalization was done over a 16×16 block.

To distinguish on the basis of this feature, Support Vector Machine (SVM) classifier, a supervised learning algorithm was used. Assume a set of N training samples of two separable classes represented by (x_1,y_1), $(x_2,y_2)...(x_N,y_N)$; where $x \in R^M$ is a M-dimensional dimensional space and class label denoted by $y, y_i \in \{-1,+1\}$, the SVM finds an optimal hyperplane which linearly separates a larger portion of the training data points while also maximizing the distance from the decision boundary thus minimizing classification error. The hyperplane discriminant function is calculated using equation (6).

$$f(x) = \sum_{<x_i>} y_i \alpha_i k(x,x_i) + b \quad (6)$$

where, the membership of x is determined by the sign of $f(x,y)$, k denotes the kernel function and b is the bias. Finding all the nonzero α_i is the equivalent of constructing an optimal hyperplane. A vector x_i is said to be support vector (SV) of the hyperplane, if it complied to a nonzero α_i. The SVM model provides a compact classifier. This is because the number of training data points maintained as the support vectors generally continue to be very small [10].

In this work, the dataset included 40 real and 20 fake notes which were used train our SVM model and Gaussian Radial Basis Function was being used as kernel function.

IV. Results

The proposed methodology was implemented in C++ using OpenCV library on a system bearing the following specifications:

CPU: Intel(R) Core(TM) i7-3520M @ 2.90GHz
RAM: 8.00GB
OS: Ubuntu 16.04LTS (64 bit)

A total of 40 real and 20 fake notes were used to create training dataset. Also, all the images were captured with a mobile phone equipped with a camera having minimum resolution of 8MP. This dataset was used to train the SVM classifier and determine the threshold value as discussed in section III.A. The testing dataset consisting of 20 real and 10 fake notes was employed to determine the performance shown in Table I and Table II.

Total test images	**Performance Parameters**				
	True positive	True negative	False positive	False negative	Accuracy (%)
30	18	9	1	2	90.0

TABLE I
PERFORMANCE ON BASIS OF SECURITY THREAD

Total test images	**Performance Parameters**				
	True positive	True negative	False positive	False negative	Accuracy (%)
30	20	10	0	0	100

TABLE II
PERFORMANCE ON BASIS OF LATENT IMAGE

The note is considered to be correctly classified only if authenticity of both the security features is verified.

V. CONCLUSIONS

In this paper, we presented an automated counterfeit detection tool exploiting image processing and machine learning based algorithms. The security features of the bank notes were extracted and encoded using image processing techniques while k-means clustering and SVM classifier were used for classification. Limited testing of the aforementioned methodology yielded 90% accurate results. Our future work involves rigorous testing, improvement in computational efficiency and further incorporation of other security features to make it more robust and reliable. The proposed method is developed and tested on the new Rs 500 notes but can also be utilized for Rs 2000 notes.

VI. AKNOWLEDGEMENT

We would like to thank Vipin Kamble, Research Scholar, VNIT, for his mentorship and time and would like to express gratitude to Prof. K. Surender, VNIT, for his immense guidance and kind attention towards the development of this project. Also, we are grateful to SBI VRCE branch for providing us relevant information related to counterfeiting and helping us in building our database.

REFERENCES

[1] A. Vila, N. Ferrer, J. Mantecon, D. Breton, J.F. Garca,“Development of a fast and non-destructive procedure for characterizing and distinguishing original and fake euro notes”, Analytica Chimica Acta - ANAL CHIM ACTA. 559. 257-263. 10.1016/j.aca.2005.11.084, 2006.

[2] A. Bhingare and S. Dixit, “Counterfeit Indian Currency Detection Through Image Processing in Labview”, *International Journal for Research in Applied Science and Engineering Technology*, V. 617-621. 10.22214/ijraset.2017.2093, Februry 2017.

[3] K. Santhanam, S. Sekaran, S. Vaikundam and A. M. Kumarasamy, “Counterfeit Currency Detection Technique Using Image Processing, Polarization Principle and Holographic Technique”, 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation, Seoul, 2013, pp. 231-235.

[4] Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing (3 ed.)*, Prentice Hall, August 2007.

[5] Jiawei Han, Micheline Kamber, and Jian Pei, *Data Mining: Concepts and Techniques (3rd ed.)*, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2011.

[6] Ramteke, Rakesh and Pathan, Imran and Mehrotra, Suresh, “Skew Angle Estimation of Urdu Document Images: A Moments Based Approach”, *International Journal of Machine Learning and Computing*, 1. 7-12. 10.7763/IJMLC.2011.V1.2, 2011.

[7] N. Dalal and B. Triggs, “Histograms of oriented gradients for human detection”, 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR’05), San Diego, CA, USA, 2005, pp. 886-893 vol. 1.

[8] M. Tkalcic and J. F. Tasic, “Colour spaces: perceptual, historical and applicational background”, The IEEE Region 8 EUROCON 2003. Computer as a Tool., 2003, pp. 304-308 vol.1.

[9] G. A. Wilkin and X. Huang, “K-Means Clustering Algorithms: Implementation and Comparison”, Second International Multi-Symposiums on Computer and Computational Sciences (IMSCCS 2007), Iowa City, IA, 2007, pp. 133-136.

[10] V. Jakkula, “Tutorial on support vector machine (svm)”, School of EECS, Washington State University, 2006 [online]. Available: https://www.semanticscholar.org/paper/Tutorial-on-Support-Vector-Machine-(SVM)-Jakkula/7cc83e98367721bfb908a8f703ef5379042c4bd9

[11] https://www.rbi.org.in/