Detecting Counterfeit Currency and Identifying Its Source

Ankit Sarkar, Robin Verma, Gaurav Gupta

▶ **To cite this version:**

Ankit Sarkar, Robin Verma, Gaurav Gupta. Detecting Counterfeit Currency and Identifying Its Source. 9th International Conference on Digital Forensics (DF), Jan 2013, Orlando, FL, United States. pp.367-384, 10.1007/978-3-642-41148-9_24 . hal-01460616

HAL Id: hal-01460616

https://inria.hal.science/hal-01460616

Submitted on 7 Feb 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Chapter 24

DETECTING COUNTERFEIT CURRENCY AND IDENTIFYING ITS SOURCE

Ankit Sarkar, Robin Verma and Gaurav Gupta

Abstract Counterfeit currency varies from low quality color scanner/printer-based notes to high quality counterfeits whose production is sponsored by hostile states. Due to their harmful effect on the economy, detecting counterfeit currency notes is a task of national importance. However, automated approaches for counterfeit currency detection are effective only for low quality counterfeits; manual examination is required to detect high quality counterfeits. Furthermore, no automatic method exists for the more complex – and important – problem of identifying the source of counterfeit notes. This paper describes an efficient automatic framework for detecting counterfeit currency notes. Also, it presents a classification framework for linking genuine notes to their source printing presses. Experimental results demonstrate that the detection and classification frameworks have a high degree of accuracy. Moreover, the approach can be used to link high quality fake Indian currency notes to their unauthorized sources.

Keywords: Counterfeit currency, detection, Indian rupees

1. Introduction

To counterfeit means to illegally make an imitation of something with the intent to take advantage of the superior value of the imitated product. Counterfeit currency refers to currency that closely resembles the original currency of a country but that is produced without the legal sanction of the government. Counterfeit currency is harmful to a nation. Fake notes increase money circulation, potentially leading to inflation. Also, the overall confidence in the currency decreases. Furthermore, individuals who innocently acquire counterfeit currency are victimized –

there are usually no government policies to reimburse them for counterfeit notes that are seized. On the other hand, the individuals who produce counterfeit currency can make significant profits and finance an array of activities, many of which might be against the national interest.

Counterfeits are created in a variety of ways. The easiest and most common way is to use a high resolution scanner to capture both sides of a genuine currency note. The scanned images are then printed using a color inkjet or laser printer. This method works well for small denomination notes that are usually not scrutinized. However, it is easy to identify such counterfeit notes because of the quality of the paper that is used.

A more sophisticated method starts with a low denomination note, bleaches or washes out the ink, and then prints a higher value note. However, the production of a high quality counterfeit requires an entity to use the same raw materials and printing process that are used to produce genuine currency. This is out of the reach of individual counterfeiters due to the high cost and difficulty in procuring the raw materials and equipment. Therefore, the production of high quality counterfeits is generally state sponsored – the goal is usually to undermine the economy of the targeted state. A notable example is the "SuperDollar," a high quality imitation of the U.S. dollar. Another example is the fake Indian rupee notes produced by hostile states that are often indistinguishable from the originals.

Security features are often embedded in currency notes to identify genuine notes. Common security features include watermarks, security threads, latent images, micro-lettering, intaglio (raised print), optically variable ink and fluorescence. In addition to helping verify that a currency note is genuine, the security features deter counterfeiting. Replicating the security features increases the cost of counterfeiting, making it less profitable.

This paper focuses on high quality fake Indian counterfeit notes. While the successful identification of such notes usually requires expert examination, it is a relatively simple problem because only the integrity of the security features has to be investigated. A more difficult task is to identify the source of a counterfeit note. This requires detailed investigation by forensic scientists using expensive instruments. Also, no automatic method exists to link a counterfeit note to its source press. This paper applies digital forensic methods to address the problem, with the ultimate goal of developing an automated and scalable process that can link currency notes to their source presses.

Indian currency notes are printed at dedicated government printing presses. The number of presses is limited and great care is taken to

ensure that all the notes produced by the presses are of the same quality. However, it is extremely difficult to produce currency notes that are exactly similar. Differences creep in due to plate defects, plate wear, ink quantity and inaccuracies in the cutting process. Locard's law of exchange states that every contact leaves a trace. According to this law, all currency notes from a particular press should contain some traces of the defects. Since the plates, printing machinery and raw materials are generally not transported from one press to another, it can be assumed that these characteristics are unique to each press. Thus, notes can be grouped into classes depending on their source printing press. Consequently, this paper focuses on identifying features (with intra-class similarity and inter-class differences) that can be used to classify currency notes. The goal is that, given a genuine Indian currency note, it should be possible to classify it as having been printed at one of the government presses. The approach can then be extended to link a fake Indian currency note to its source printing press in a hostile state.

2. Related Work

This section discusses previous work related to detecting counterfeit documents and linking documents to their source devices.

2.1 Detecting Counterfeit Documents

The problem of detecting a forged document has been the subject of much research. However, most approaches involve manual methods. In the case of counterfeit currency, the approach involves visually verifying security features such as security threads, watermarks, optically variable inks and intaglio. Non-visual methods include the use of chemical analysis to verify paper quality. While manual methods are reliable, they are not scalable – most real-world scenarios require the rapid processing of currency notes as soon as they are proffered by their owners.

Few automated methods have been proposed for detecting fraudulent documents. One of the earliest approaches was proposed by Gupta, *et al.* [3], who focused on fake documents produced using scanners and printers. In particular, they discovered that a fake document has more unique colors than its genuine counterpart. Gupta, *et al.* [4] subsequently introduced two measures for detecting fake documents, variation in intensity and grey level co-occurrence matrix uniformity.

Ryu, *et al.* [9] applied machine learning in an automatic framework for detecting fake documents. They modeled detection as a classification problem with two classes, genuine and fake. An SVM classifier was used with seventeen image quality measures as features. The SVM clas-

sifier worked relatively well for forgeries using scanners and printers, but there is still scope for improvement, especially with regard to detecting counterfeit currency notes (see, e.g., [1, 7, 8, 11, 12]).

Another approach is to use intrinsic features to compute a signature for a genuine document [10]. Given a set of pre-processed (properly rotated and pixelwise aligned) genuine documents, an unsupervised learning algorithm is employed to compute the document signature. The major feature used is the difference in alignment between genuine and fake documents. When an unknown document is presented, an attempt is made to match its signature with the genuine signature; the document is deemed to be fake if the signature does not match. The main assumption of this approach is that all genuine documents must be of the same type (e.g., like a particular bill or receipt) and a sufficient number of genuine samples must be available. Also, the approach assumes that a forged document is created using a scanner and printer, which introduce distortions.

2.2 Linking Documents to Source Devices

After a document is deemed to have been forged, it is often necessary to conduct a forensic investigation to discover its source. This is a hard problem.

One approach is to use a watermarking scheme in which a predetermined watermark is embedded in the document. The watermark is usually invisible to the naked eye but can be seen under a microscope. Depending on the level of sophistication, the watermark can help identify the make, model and even the specific printing device. However, a major shortcoming of this approach is that it relies on security through obscurity – the watermarking scheme must be kept secret to prevent unauthorized parties from creating the watermarks themselves.

Another approach is to characterize the defects that are unique to a particular scanner or printer. In this case, the amount of quantization done by a scanner, which differs from scanner to scanner, is used to link a fake document to a specific scanner [1, 4]. The unique color count is often used to link a forged document to a printer. Morphological features are also used to identify a printer [5]. The main advantages of this approach are that it does not rely on embedded watermarks and can be applied to any document.

Most approaches focus on detecting forgeries created by scanners and printers. However, high quality counterfeit currency is rarely, if ever, produced by scanners and printers. Indeed, high quality counterfeits are created using the same raw materials and printing processes used

Table 1. Mapping of inset letters to printing presses.

Inset Letter	Printing Press
Nothing, A, B, C, D	Press 1 in City 1
E, F, G, H, K	Press 2 in City 2
L, M, N, P, Q	Press 3 in City 3
R, S, T, U, V	Press 4 in City 4

to produce the originals. Therefore, it is extremely important to link counterfeit currency notes to their source printing presses. To the best of our knowledge, no research has specifically focused on this problem.

3. Currency Note Database

This section describes the database used for Indian currency note analysis. First, an overview is provided of Indian currency notes. Next, the genuine and counterfeit currency samples used in this work are described. Finally, the approach used to create digitized samples is detailed.

3.1 Indian Currency Notes

Indian currency notes are printed by the Reserve Bank of India (RBI) at four authorized currency presses. The presses are located in four different cities in India; the names of the cities are not publicized for security reasons [2].

An inset letter – a capital letter found on the number panel on the top right or bottom left of a currency note – is used to identify the printing press. Each of the four presses is allocated a set of inset letters for identification purposes. According to Gupta, *et al.* [2], 20 letters are currently used as inset letters. Table 1 presents the mapping of inset letters to printing presses. This information was inferred by Gupta, *et al.* [2] based on the name of the printer that appears on reams of printed banknotes.

This information is used as the ground truth in our experiments. Our goal is to attempt to construct a classifier for genuine Indian Rs. 500 notes. The classifier should partition input notes according to their source printing press.

3.2 Currency Samples

No publicly available database of genuine and counterfeit Indian currency notes currently exists. Furthermore, according to RBI regulations, no high resolution images of Indian currency notes may be publicly dis-

Table 2. Genuine currency samples.

Year	Inset Letter	RBI Governor	Series
2011	Nothing, E, L, R	Subbarao	Yellow
2010	Nothing, E, L, R	Subbarao	Yellow
2009	Nothing, E, L, R	Subbarao	Yellow
2008	Nothing, E, L, R	Reddy	Yellow
2007	E, L, R	Reddy	Yellow
2006	Nothing, E, L, R	Reddy	Yellow
2005	R	Reddy	Yellow
No Year	B	Reddy	Yellow
No Year	A	Jalan	Yellow
No Year	A	Jalan	Blue

seminated. Therefore, our only option was to create our own database of images.

We collected several Rs. 500 currency notes. In the case of genuine notes, we attempted to collect as many samples as possible of each type (i.e., year, inset letter and RBI Governor). The sample size was limited because some older series of notes were not readily available. Another limiting factor was cost. Our genuine currency sample set comprised three notes of each type listed in Table 2.

We were able to collect only ten counterfeit currency notes. Four of these notes were in very bad condition. Thus, the counterfeit currency sample set included just six notes.

3.3 Image Creation

High resolution images of the samples were created under different parts of the light spectrum. A visual spectral comparator (VSC 6000) with facilities for examining and photographing documents in varying lighting conditions was used for this purpose.

A total of 23 images were taken for each sample currency note. The images covered various parts of the notes under different lighting conditions and magnifications (Table 3). The imaging decisions were made based on a preliminary examination of the notes using the visual spectral comparator. The 23 images showed the most perceptible differences for the different currency notes examined. As such, they were assumed to be the most promising features for detecting counterfeits and identifying the source presses.

The digitized database thus consisted of 33 currency notes, 27 of them genuine and six counterfeit. Since 23 images were taken for each note, the database contained a total of 759 images.

Table 3. Features collected for each currency note.

Feature ID	Area of Note	VSC Setting	Mag.
IMG_01	Front, Entire note	Longpass = VIS	3.04
IMG_02	Front, Entire note	Longpass = RG925	3.04
IMG_03	Front, Entire note	IR, Longpass = RG630	3.04
IMG_04	Front, Entire note	IR, Longpass = OG530	3.04
IMG_05	Front, Entire note	UV 365nm	3.04
IMG_06	Front, Entire note	UV 312nm	3.04
IMG_07	Front, Entire note	UV 254nm	3.04
IMG_08	Front, Entire note	UV 365nm passthrough	3.04
IMG_09	Front, Entire note	Dim overhead light	3.04
IMG_10	Front center, Denomination in OVI	Longpass = VIS	16
IMG_11	Front center, Denomination in OVI	Longpass = VIS, Pseudocolor	16
IMG_12	Front center, Denomination in OVI	Longpass = RG925, Pseudocolor	16
IMG_13	Front, Hindi text RBI Governor	Longpass = VIS	61
IMG_14	Front, Braille identifier	Longpass = VIS	61
IMG_15	Front, Braille identifier	Longpass = VIS, Sidelight = Right	61
IMG_16	Front, Gandhi face	Longpass = VIS	25
IMG_17	Front, Gandhi ear, Micro-lettering	Longpass = VIS	30
IMG_18	Front, Inset letter	Longpass = VIS	50
IMG_19	Back, Entire note	Longpass = VIS	3.04
IMG_20	Back, Entire note	UV 365nm	3.04
IMG_21	Back, Entire note	UV 312nm	3.04
IMG_22	Back, Entire note	UV 254nm	3.04
IMG_23	Back, Entire note	UV 365nm passthrough	3.04

The database size was limited by the time constraints imposed by the digitizing process. It took an average of ten minutes to apply the required settings, focus, capture and save each image. Thus, it took about 230 minutes to fully digitize each sample. Due to the time factor, we decided to digitize one sample from each class (combination of year, inset letter and RBI Governor) of genuine notes along with the six counterfeit note samples. Thus, the database contained one representative sample from each series and type.

4. Detecting Counterfeit Currency Notes

This section describes the technique used to detect counterfeit currency notes, and the results that were obtained.

4.1 Preliminary Experiments

A preliminary experiment was conducted to determine which of the 23 features collected for each note would be useful in detecting counterfeit currency notes. Histograms of each feature were generated for all the currency notes and the histogram correlations of the corresponding features of the currency notes were examined. Also, the histograms were manually examined to discern differences that could assist in classifying notes as genuine or counterfeit. Since previous approaches successfully used the unique color count to detect fraudulent documents, the number of unique colors in each image was recorded.

The preliminary analysis also involved observations of the currency notes under a microscope. The Veho VMS-004D 400X USB microscope used for this purpose had fixed optical zooms of 20X and 400X. Various portions of the notes were examined for features that could be used to discriminate between genuine and fake notes.

The preliminary analysis revealed that features related to particular areas of a currency note were more discriminating that those related to the entire note. The most promising features observed were the Rs. 500 denomination lettering in optically variable ink, the area of Gandhi's face and the inset letter. The red, blue and green histograms of these features for genuine and counterfeit notes were compared, but no significant correlations were discerned. However, it appeared that there were clear differences between the unique color counts of features of genuine and fake currency notes, most likely due to differences in the printing process and ink.

4.2 Feature Selection

Three features were selected: (i) IMG_10 (Figure 1); (ii) IMG_11 (Figure 2); and (iii) IMG_12 (Figure 3). Based on the results of the preliminary experiments, the unique color count was used as a measure for quantifying the features. For each currency note, the corresponding images were selected and the total number of unique colors in the image was calculated. A C# program was written to perform this task and generate the corresponding CSV file of extracted features. It was not necessary to pre-process the features because they were already focused and adjusted at the time of sampling.

4.3 Classifier Design

A C4.5 decision tree was used to classify currency notes as genuine or counterfeit. The implementation of C4.5 in WEKA [6] was employed for

(a) Genuine note. (b) Counterfeit note.

Figure 1. Image IMG_10.

(a) Genuine note. (b) Counterfeit note.

Figure 2. Image IMG_11.

(a) Genuine note. (b) Counterfeit note.

Figure 3. Image IMG_12.

training and testing. A relatively simple classifier was preferred because the feature set comprised only three features.

We experimented with other classifiers, including neural networks, radial basis function networks and C4.5 using grafting. However, all four classifiers had comparable accuracy, so the classifier with the least complexity was selected. A simpler classifier requires less time for training and testing compared with a more complex classifier. In a real-world application involving counterfeit currency detection, it is necessary to provide a quick answer because the owner of a currency note would be unwilling to wait for a long period of time.

4.4 Results and Evaluation

A C4.5 decision tree was trained and tested using the database of 33 images (27 genuine notes and six counterfeit notes). Ten-fold stratified cross validation was employed; 90% of the set was used for training and the remaining 10% for testing. The number of correctly classified instances was 31 while the number of incorrectly classified instances was two, yielding an average accuracy of 93.94%. Of the two incorrectly classified instances, one was a false positive (genuine detected as fake) and the other was a false negative (fake detected as genuine).

Upon closer examination of the two incorrectly classified instances, we discovered that one was a genuine note that belonged to the old "Blue Series." This older series of Rs. 500 notes does not have as many security features as the newer notes, which may have led to it being erroneously classified as fake. Manual examination of the fake note that was classified as genuine revealed that the note had extensive markings (zigzag lines) in blue ink (possibly made with a ball point pen).

The two currency note samples were then removed and the classifier was tested once again. The results were 100% accurate with all 31 instances classified correctly.

5. Identifying the Source Printing Press

This section describes the technique used to link a currency note to its source printing press, and the results that were obtained.

5.1 Preliminary Experiments

Preliminary experiments were also conducted to identify the features that would help link a currency note to its source printing press. Only genuine notes were used in this experiment because the ground truth was known only for genuine notes. As mentioned earlier, notes with the same inset letter come from the same press. Consequently, the goal was

to successfully classify notes with the same inset letter and, thus, the same origin.

As in the previous experiment, histograms of the corresponding features of the notes were constructed. However, since there were more classes, it was difficult to identify one feature that could be used to differentiate between all the classes. Therefore, we attempted to discern some peculiar properties of each class of notes that would support the identification. We observed that, while no single feature was able to discriminate between all the classes, certain features were able to differentiate between one particular class and the others. Hence, we framed the task as a multilevel classification problem and used a cascade of classifiers. The cascade incorporates multiple levels of individual classifiers and passes the output of one classifier to another.

5.2 Pre-Processing

Pre-processing was required for some of the images before extracting the features. Two techniques were used for pre-processing:

- **Percentage Histogram Bins:** Histograms (bins 0–255) of the blue, green and red channels were constructed. The values of each bin were divided by the total pixels in the image and multiplied by 100 to expresses it as a percentage of pixels in the image with a particular intensity. This was necessary because the images had different sizes, which precluded the use of regular histograms for comparison (i.e., using only the numbers of pixels).

- **Threshold UV Images:** Threshold images were created from images obtained under ultraviolet (UV) light (Figure 4). Each pixel was given a value of 255 if its intensity in the green channel was greater than 100 and its intensity in the red channel was greater than 100; otherwise, it was given a value of zero. Thus, binary images were obtained with pixels of intensity zero or 255 (Figure 5).

5.3 Feature Selection

Based on the experimental results, we selected seven features to be used by the cascade of classifiers. Note that pre-processing was required for feature extraction and quantification.

Figure 4. UV image.

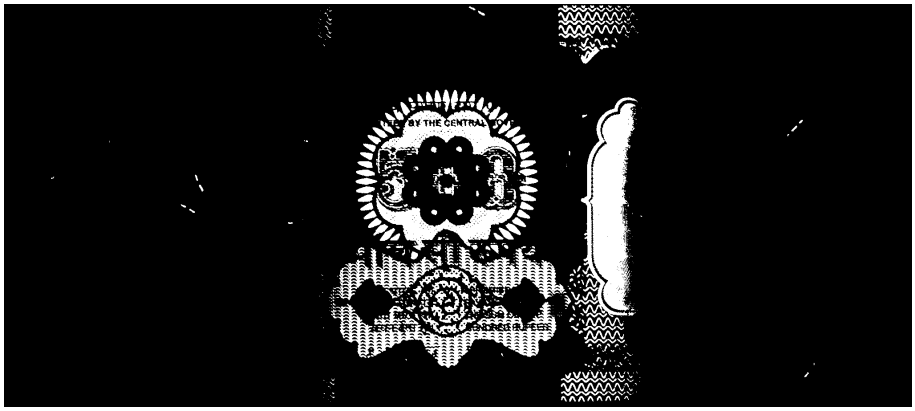

Figure 5. Threshold UV image.

- **Feat_01_Link:** The percentage histogram bins were calculated for IMG_18 (Figure 6). The quantification was performed using the sum of the histogram bins of the blue channel from 0 to 210.

- **Feat_02_Link:** The percentage histogram bins were calculated for IMG_18. The quantification was performed using the sum of the histogram bins of the blue channel from 0 to 100.

- **Feat_03_Link:** The percentage histogram bins were calculated for IMG_18. The quantification was performed using the sum of the histogram bins of the blue channel from 0 to 40.

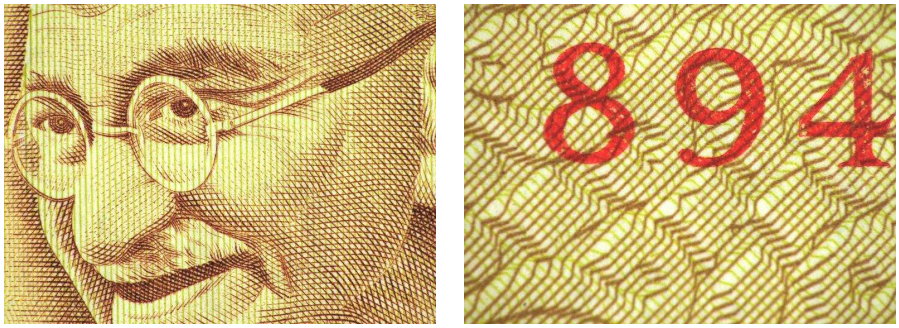

Figure 6. Images IMG_16 (left) and IMG_18 (right).

Figure 7. Image IMG_19.

- **Feat_04_Link:** The percentage histogram bins were calculated for IMG_16. The quantification was performed using the sum of the histogram bins of the green channel from 0 to 40.
- **Feat_05_Link:** The number of white pixels in each half of the threshold UV image of IMG_07 was computed. The quantification was performed using the ratio of the white pixels in the right half to those in the left half.
- **Feat_06_Link:** Image IMG_10 was used. The quantification was performed by counting the total number of unique colors.
- **Feat_07_Link:** Image IMG_19 was used (Figure 7). The quantification was performed by counting the total number of unique colors.

5.4 Classifier Design

As described above, a cascade of classifiers uses multiple levels of individual classifiers in which the output of one classifier is input to another. In our design, an individual classifier was used to filter currency notes belonging to one particular class. Thus, each succeeding classifier dealt with one less class than the preceding classifier in the cascade. Each level used a C4.5 decision tree as the classifier. A total of five classifiers were used.

- **Level 1:** This classifier was designed to filter the old Blue Series notes (i.e., Rs. 500 notes printed prior to or during Bimal Jalan's term as RBI Governor). These notes differ significantly from the newer Yellow Series notes. The old Blue Series notes have inset letters A, C or blank, and are from Press 1 in City 1. The features used in Level 1 were Feat_01_Link and Feat_02_Link. All the genuine notes were passed to the classifier, which classified them either as "Old Blue Series with inset letters A, C or nothing" or "New Yellow Series with any inset letter." The currency notes classified as "New Yellow Series" were passed to the Level 2 classifier.

- **Level 2:** This classifier was designed to filter notes with no inset letters. These notes are also from Press 1 in City 1. The feature used was Feat_03_Link. The output of the Level 1 classifier ("New Yellow Series") was passed as input to the Level 2 classifier, which classified the currency notes as "No inset letter" and "Inset letter A, B, E, L or R." The notes with inset letters A, B, E, L or R were passed to the Level 3 classifier.

- **Level 3:** This classifier was designed to filter notes with the inset letter L. These notes are from Press 3 in City 3. The feature used was Feat_04_Link. The output of the Level 2 classifier ("Inset letter "A, B, E, L or R") was passed as input to the Level 3 classifier, which classified the currency notes as "Inset letter L" and "Inset letter A, B, E or R." The notes with inset letters A, B, E or R were passed to the Level 4 classifier.

- **Level 4:** This classifier was designed to filter notes with the inset letter E. These notes are from Press 2 in City 2. The features used were Feat_05_Link and Feat_06_Link. Feat_05_Link was specifically used because our preliminary experiments revealed that the right portion of currency notes with the inset letter E had a larger area that glowed under UV light. The output of the Level 3 classifier ("Inset letter "A, B, E or R") was passed as input to the Level

Table 4. Results.

Level	Correctly Classified Instances	Incorrectly Classified Instances	Correctly Classified Percentage	Incorrectly Classified Percentage
Level 1	27	0	100%	0%
Level 2	26	0	100%	0%
Level 3	20	1	95.24%	4.76%
Level 4	14	1	93.33%	6.67%
Level 5	9	0	100%	0%

4 classifier, which classified the currency notes as "Inset letter E" and "Inset letter A, B or R." The notes with inset letters A, B or R were passed to the Level 5 classifier.

- **Level 5:** This classifier was designed to filter notes with the inset letter R. These notes are from Press 4 in City 4. Any note that was classified at this level was assumed to have inset letter A or B (from Press 1 in City 1). Feature Feat_07_Link was used because none of the other features could discriminate between notes with inset letters A, B and R. The output of the Level 4 classifier ("Inset letter "A, B or R") was passed as input to the Level 5 classifier, which classified the currency notes as "Inset letter R" and "Inset letter A or B."

5.5 Experimental Results

This section describes the results obtained for the individual classifiers and the cascade classifier.

- **Individual Classification:** In passing input to a classifier at a given level, we assumed that all the classifiers at the previous levels gave the correct results. Thus, the classifier input only contained instances that would be passed to it from the previous classifier. Ten-fold stratified cross validation was used for each classifier, except for the last (Level 5) classifier, which used eight-fold stratified cross validation.

  Table 4 shows the results that were obtained. Note that all five classifiers have high degrees of accuracy.

- **Cascaded Classification:** In this case, we evaluated the system of five cascaded classifiers as a whole. Each classifier was individually trained and then combined to create the cascade. We used

the entire set of currency notes to test the cascaded classifier – this was done to use all the available samples for testing and to see if the cascaded classifier failed on any sample.

A total of 27 samples were provided as input to the cascade classifier. Of these, 25 were classified correctly based on their inset letter and two were classified incorrectly. This corresponds to an overall accuracy of 92.59%.

5.6 Evaluation

While the experimental results indicate that the individual classifiers and the cascaded classifier have high degrees of accuracy, some limitations do in fact exist. First, the classifiers are dependent on the fact that the input images are correct and well focused. For example, the Level 2 classifier is sensitive to changes in focus. To verify this fact, we deliberately blurred a sharp image and provided it to the classifier, which gave an incorrect result.

The second limitation is that the currency notes are assumed to be of good quality. The presence of oil, cellotape, pen marks or dirt on the surface of a note can render it difficult to classify correctly. For example, one of the fake samples had blue pen marks over it, which caused it to be classified as genuine. Also, the presence of cellotape on a currency note produces an abnormal glow when viewed under UV light. The handling of such cases is important because many Indian currency notes are worn or soiled.

A third limitation is that, because the classifiers were trained with Rs. 500 notes, they cannot be applied to other denomination notes. Also, different denomination notes have different security features, and these differences have to be taken into account when training the classifiers.

6. Integrated Tool

The classifiers were implemented in an integrated tool, which was written in C#. The EmguCV library (a C# wrapper for OpenCV) was used to perform image processing operations. The tool was run on a Compaq Presario laptop with a 2 GHz Intel Core 2 Duo Processor T5800 and 2 GB RAM. The tool took as input the folder containing all 23 image features of the sample currency notes and classified each note as genuine or counterfeit. In the case of a genuine note, the tool also attempted to identify its source printing press. The evaluation of each note was completed within five seconds.

Most individuals do not have the expertise to manually examine a currency note and determine if it is counterfeit. The tool, especially one with an enhanced GUI, would be very useful to individuals who do not have much technical and forensic knowledge. Furthermore, the tool could be integrated with a USB microscope and scanner, which would greatly reduce the possibility of commercial establishments accepting counterfeit currency as payment for goods and services.

7. Conclusions

The single classifier approach described in this paper is well suited to detecting counterfeit currency notes. The cascaded classifier approach for linking genuine currency notes to their source printing presses is also fast and accurate. The prototype tool, which integrates the two classification approaches, functions as a standalone system for counterfeit currency detection and source press identification.

Our future research will expand the image database and test the classification approaches on samples of different denominations. Additionally, we will extend the identification approach to link counterfeit currency notes to their source printing presses in hostile states. Our ultimate goal is to develop a versatile and inexpensive tool that would enable individuals without much technical and forensic knowledge to quickly detect counterfeit currency notes and identify their source presses.

References

[1] C. Chang, T. Yu and H. Yen, Paper currency verification with support vector machines, *Proceedings of the Third IEEE International Conference on Signal-Image Technologies and Internet-Based Systems*, pp. 860–865, 2007.

[2] S. Gupta, D. Handa, R. Singh and K. Kumar, Forensic identification of Rs. 1,000 – Awareness for genuineness, *CBI Bulletin*, pp. 41–45, July-September 2011.

[3] G. Gupta, C. Mazumdar, M. Rao and R. Bhosale, Paradigm shift in document related frauds: Characteristics identification for development of a non-destructive automated system for printed documents, *Digital Investigation*, vol. 3(1), pp. 43–55, 2006.

[4] G. Gupta, S. Saha, S. Chakraborty and C. Mazumdar, Document frauds: Identification and linking fake documents to scanners and printers, *Proceedings of the International Conference on Computing Theory and Applications*, pp. 497–501, 2007.

[5] G. Gupta, R. Sultania, S. Mondal, S. Saha and B. Chanda, A structured approach to detect a scanner-printer used in generating fake documents, *Proceedings of the Third International Conference on Information Systems Security*, pp. 250–253, 2007.

[6] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann and I. Witten, The WEKA data mining software: An update, *ACM SIGKDD Explorations Newsletter*, vol. 11(1), pp. 10–18, 2009.

[7] M. Ionescu and A. Ralescu, Fuzzy Hamming distance based banknote validator, *Proceedings of the Fourteenth IEEE International Conference on Fuzzy Systems*, pp. 300–305, 2005.

[8] C. Liu, S. Ruan, G. Huang, Y. Jian and L. Zhang, Research on identification of counterfeits by recognizing infrared images, *Proceedings of the International Conference on Microwave and Millimeter Wave Technology*, vol. 4, pp. 2081–2084, 2008.

[9] S. Ryu, H. Lee, I. Cho and H. Lee, Document forgery detection with SVM classifier and image quality measures, *Proceedings of the Ninth Pacific Rim Conference on Multimedia*, pp. 486–495, 2008.

[10] J. van Beusekom, F. Shafait and T. Breuel, Document signature using intrinsic features for counterfeit detection, *Proceedings of the Second International Workshop on Computational Forensics*, pp. 47–57, 2008.

[11] J. Xie, C. Qin, T. Liu, Y. He and M. Xu, A new method to identify the authenticity of banknotes based on the texture roughness, *Proceedings of the IEEE International Conference on Robotics and Biomimetics*, pp. 1268–1271, 2009.

[12] C. Yeh, W. Su and S. Lee, Employing multiple-kernel support vector machines for counterfeit banknote recognition, *Applied Soft Computing*, vol. 11(1), pp. 1439–1447, 2011.