Authentication of Currency Notes through Printing Technique Verification

Ankush Roy
Student, Dept. of Electrical Engg.
Jadavpur University
Kolkata 700032, India
ankush1123roy@gmail.com

Biswajit Halder
Dept. of Information Technology
Mallabhum Institute of Technology
Bisnupur, WB, India
biswajithalder88@gmail.com

Utpal Garain*
CVPR Unit
Indian Statistical Institute
203, BT Road, Kolkata 700108, India
utpal@isical.ac.in

ABSTRACT
An image analysis based pattern classification method is proposed to authentic the printing process used in printing different texts on currency notes. Features suitable for doing this are selected and then studied to detect fraudulent samples based on the printing method. This classification is done by using Support Vector Machines and Neural Nets. The discriminatory power of the selected features in authenticating the printing process is tested using the Linear Discriminate Analysis. Experimental results show that the proposed framework provides a highly accurate framework for authenticating the printing process in bank notes.

Categories and Subject Descriptors
I.4 [**Image Processing and Computer Vision**]: Feature measurement, Applications.
I.5.4 [**Pattern Recognition**]: Applications— *Computer Vision*.
K.6.5 [**Security and Protection**]: Authentication.

General Terms
Experimentation, Security, Verification.

Keywords
Banknotes, Printing processes, Computational forensic, Security paper documents.

INTRODUCTION
The paper currency notes being accepted as the most appropriate agent of monetary transaction the problem of counterfeit on a large scale have recently been posing a serious threat to our society. With the advancement of printing and scanning technology this problem has become acute one. Advancement in digital image processing is also playing a significant role in producing increasing number of fake banknotes every year.

ICVGIP '10, December 12-15, 2010, Chennai, India

For example, Reserve Bank of India (RBI) anxiously noticed that the value of fake currency detected in 2007-08 was at INR 55 million, a 137% increase over the previous year's amount, i.e. INR 24 million [1]. This statistic is an indicator to understand the role of fake notes in jeopardizing a country's economy.

The bank staffs are specially trained to detect counterfeit notes but problem begins once such notes are infiltrated into the market and circulated through common people. Even receiving fake notes from ATM counters have also been reported at some places. Although the forensic experts (i.e. the questioned document examiners) are available to trap these forgeries, but the existing method for detecting fake notes is cumbersome as this involves filing a case to the police, sending the document for verification and then waiting for results to come. Handling of large volume of counterfeit notes imposes additional problems. Therefore, it would be of great help if we can involve machines (independently or as assistance to the human experts) for automatic authentication of bank notes. This paper is directed to this end.

Research on developing automatic means for detection of counterfeit notes is not yet very mature as the need was not felt before. Earlier researchers did some studies on recognition of currency notes, i.e. the goal was to recognize paper currency notes of different countries. For this purpose, features like size of currency notes, color spectrum analysis, texture analysis, etc. had been used. However, it is observed [2, 3] that such a framework is not capable of distinguishing genuine notes from counterfeit. The study by Herley *et. al.* [4] addressed the problem of counterfeiting of banknotes. However, instead of detecting whether a note is genuine or fake they attempted to show how simple changes in banknote design coupled with possible changes in rendering engines can make the task of counterfeiting difficult. Such a study is significant as to help the banknote designers to understand robustness of banknote features against possible attempt of counterfeiting [5]. Although not explored but this approach may help to understand which features of existing banknotes are robust enough so that they can be used to authenticate a note as genuine.

In another study, Vila *et. al.* [6] proposed a semi-automatic approach for characterizing and distinguishing original and fake Euro notes. Their method is based on the analysis of several areas of the banknotes using Fourier transformed infrared spectrometer with a microscope with an attenuated total reflectance (ATR) objective. In their study, they considered four different regions of a note and showed that the infrared spectra obtained from these regions nicely characterize the genuine notes. The authors also observed that fake notes are easily identifiable from analysis of

the spectra. However, the authors did not propose any automated scheme for decision-making. Their study would definitely help those who adopt manual or semi-automatic approach to authenticate bank notes.

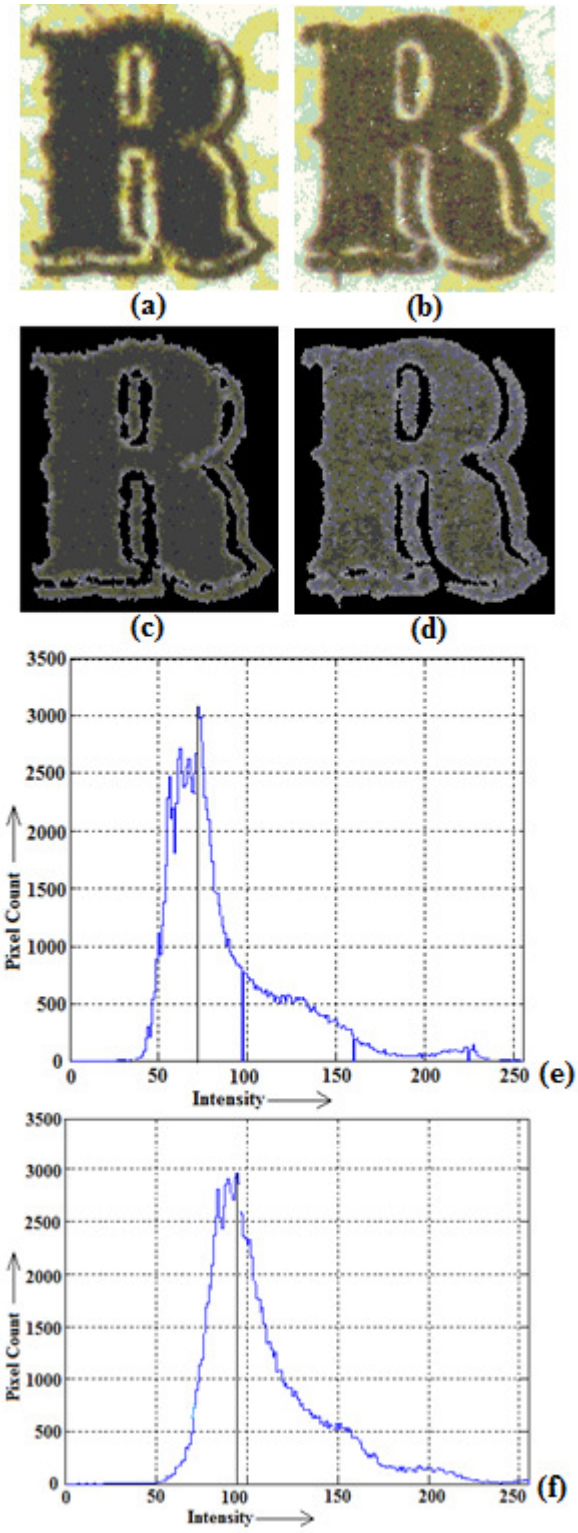


Figure 1. Role of dominant intensity.

1.1 Printing technique as a security feature in Banknotes

A banknote carries security features mainly on its paper, design and printing process. Examination or verification of currency notes is mostly conducted by checking the following aspects: i) physical dimensions, ii) paper quality, iii) design, and (iv) printing technique. Physical dimension of currency note depends on its cut size of length, width, grammage and thickness of paper. The paper on which currency note is printed carries important level of security. Watermarks and security thread are other important parts of security on currency note paper. Similarly, artwork design of the banknote carries significant security aspects. Different design techniques like Guilloche design, portrait design, etc. are used for defining different patterns, ants, stumping, thicknesses, frequencies, modulations, colors, etc. at different parts of a note. Micro lettering, see through register, anti scan lines, Braille mark, rainbow effect, layers of CYMK, bleeding effect, latent image, Omron effect, etc are also involved in the security design.

Apart from these features, the process used to print banknotes provides important checkup for authentication of the notes. In many cases counterfeiting have been reported even on the paper identical to one as used for genuine notes leaving a very narrow gap to identify the original from the fake. However, the printing technique that is hard to replicate because some of its inherent characteristics. There are numerous printing processes like offset, dry offset, intaglio, letterpress, serigraphy, screen printing, photostat copying, inkjet, bubble-jet, digital printing, etc. that can be used for printing currency notes. Out of these many possibilities, only a few processes are normally used in practice. For example, in case of Indian currency notes, dry offset, intaglio, and electronic monitored number printing process are mainly involved. Different printing processes are used to print different parts of a note. However, not all of these printing techniques are applied at a time. The sequence by which the printing processes are executed one after another is itself a security aspect.

Any printing process involves ink pigment. There are many types of inks like CMYK (cyan, magenta, yellow, and black ink) ink, fluorescence ink, optical ink, etc. Final finish of print result applies varnishing and fused. The basic components of printing ink are pigment, solvent and drier. Where ink pigment is responsible for color effect on a substrate, drier is responsible to bind ink pigment to substrate. Solvent is responsible for soluble of ink pigment and drier. Drying mechanism of intaglio and offset printing are quite different. The solvent of offset printing ink is oily based and normally drying under heating effect. Chemical polymerization takes place during drying of offset ink. Here drying time is less and final effect on substrate is brighter and sharper edge. In intaglio printing, drying mechanisms of ink pigment is mainly achieved through evaporation and penetrations of ink solvent on its substrates. Here, the tendency of deposited ink spread beyond its deposition area. In addition, the required drying time of intaglio printing is more than offset printing. Therefore, the final effect of intaglio printing is less bright and less sharp edge as compared to that of offset printing.

Examination of final printing effect is an important aspect for verification of security documents' authenticity. Final effects on currency note are defined by unique color, impression, water resistance, line work (width, thickness, sharpness, etc.), halftone

effect, digitized patterns and also reflectivity and feel/tactility. Many of these effects are due to the chemical composition of the ink used and the particular drying mechanism as followed in particular printing technique. Most of these effects are visualized through microscope with high magnification or by different scanning technologies. Forensic experts often take their decision by checking these effects of printing on currency note with mostly the help of a microscope. In this paper, we involve machine that closely follows a similar approach in order to authenticate the printing process in a bank note.

1.2 Previous studies on automatic detection of printing techniques

With the recent use of digital imaging techniques for the forensic examination of documents, determination of underlying printing technology of a document has gained significant attention of the research community. Two different approaches are prevalent for identifying printing technology. One approach is to geometric distortion or degradation to characterize particular printing techniques. On the other hand, second approach does use color/gray level features for printer identification. The studies reported in [7-12] adopted the first approach. In 2002, Oliver and Chen [7] described a machine-vision based print quality analyzer to derive a particular printer's characteristics and identify printing technology. Seven different digital (ink jet and dry/liquid xerography) and impact (computer-to-plate offset lithography) printing technologies were considered and their characteristics were quantitatively analyzed using features like line width/raggedness and over-spray; dot roundness/perimeter and number of satellite drops, image sharpness and image growth (positive versus negative prints). Experiment showed that it was possible to resolve a unique print quality signature which enables differentiation of one printer technology/supplier from another. Though no framework was proposed towards how machine can take decision about the printing technology but this study demonstrated the potential of a machine-vision based approach in the context of digital printing forensic document examination.

The study reported by Kee and Farid [8] attempt to model different geometric degradations caused by different printing processes. This method is heavily dependent on availability of character images in the document in question. A set of characters (e.g. the letter 'e') is considered and degradation observed in these character images is used to represent the printer degradation. Obviously, existence of a few letters in a document may not produce a good model of a printer. However, it was experimentally verified that a document with considerable amount of text resulted in sufficiently consistent printer profile which was used for printer identification of printers of different make and model and also to detect local tampering in a document. However, it was also experienced that as a printer profile depends on its toner level, different profiles corresponding to different toner levels are to be made for the same printer. However, such dependence has been avoided in a recent study by Bulan *et al* [9] who also used geometric distortions to generate printer signatures. Geometric/structural information is also used by Li *et al* [10, 11] for identifying colour printers. They found that the dotted motifs can be used to characterize printers of different makes. The authors even observed that printers of different serial numbers of the same make result in distinctive dotted patterns. Tweedy [12] investigated the use of such a coded pattern on each color laser copy so that the forensic people easily and uniquely identify the make, model, and serial number of the copier used.

Instead of using geometric properties, second class of approaches makes use of gray level or colour of image pixels for discriminating a specific printing technique from others. For example, Mikkilineni *et al* [13, 14] considered small printed areas of a document and print quality defects are modelled as texture. Texture features are then used to classify the model and manufacturer of the printed used to print a document in question. In doing so, the authors considered images of the letter "e" in a page and gray-level co-occurrence features are computed to describe the texture generated by the printer used to print the page. Classification of the printers is done by using a nearest neighbour classifier. Ten different printers were considered in the experiment and it is found that 9 out of 10 printers were correctly classified. However, this approach makes use of a large number (e.g. test pages containing 300 "e"s) of "e" images to compute the features. Behaviour of this method for pages containing small amount of text was not investigated.

Further evaluation of a method using gray-level features was reported in [15] where documents were scanned at low resolutions (e.g. 100dpi to 400 dpi instead of 1200 dpi as used in [14]) to achieve a high-throughput system. They considered two kinds of printing techniques namely, laser and inkjet but a number of different printers (e.g. 49 laser and 13 inkjet printers) were considered in the experiment. Both the texture and edge based gray-level features [16] were used to compute the feature vectors. Classification was done by using three different classifiers namely, C4.5 decision tree, multi-layer perceptron, and support vector machines. Experiment nicely illustrated the effect of scanning resolution, the kind of features used and the particular classification approach on the accuracy of identifying printers. The authors suggested that apart from gray-level features use of color properties of documents may help to achieve better accuracy. Use of color features to a limited extent is available in the study conducted by Dasari and Chakravarthy [17]. They used HSV color space and, in particular, hue images at high-resolution to distinguish between the different printing processes. Their initial study indicated that the results traditionally obtained by document examiners using a microscope or through chemical analysis could be replicated by adopting automatic means.

1.3 Contribution of our work

After reviewing the existing literature, it is evident that both the geometric and the gray or color level features contribute significantly towards printer identification. However, there is a gap in integrating these two types of features in detecting printing techniques. Moreover, many of the studies illustrated certain geometric properties that would play important role in printer identification but a complete framework starting from computation of features till a decision made by a machine has not been well addressed in many of those studies. Another general shortcoming in the existing studies is the use of synthetic data. The authors generate print outs at lab and then test their algorithms on these samples. Therefore, behavior of these algorithms on real forensic samples is yet to explore. On the other hand, the central goal of this research is to be used for forensic purposes and therefore, forensic community would obviously be interested to know the results when real data is involved.

All these shortcomings motivate us to take up the present research. In this paper, we attempt to formulate a general framework for authentication of the printing techniques in banknotes. The entire approach is based on scrutinizing the printing technique. We consider three different aspects like geometric properties, gray-level features, and color properties for characterizing a particular printer. Most importantly, we attempt to closely follow the practice of the questioned document examiners in detecting printers and try to simulate the same in a machine-vision based framework. Most of the aspects that the forensic experts look for identifying the expected printing technique are computationally grabbed and a machine is configured to give the decision about the authentication of the printing process. This framework is then used for a practical problem namely, identification of fake banknotes based on authentication of printing technique. The experiment involves real samples of genuine and fake notes. Results are computed and analyzed to bring out the potential of the proposed framework. The rest of the paper discusses about the computation of features, implementation of the method and experimental results.

2. FEATURES

Feature extraction in this experiment is largely dominated by the input from the forensic experts. Altogether nine features are extracted which can be broadly classified into three as (i) gray-level features (ii) color features and (iii) structural or geometric features. The features and rationales behind choosing them are explained below.

Dominant intensity (f_1): Dominant intensity is defined by the intensity level that majority of the pixels in the character stroke possess. As the dominant intensity of an image is typical to its process of printing, we use it as a feature. Measuring of this feature requires construction of a suitable mask in order to eliminate most of the background pixels keeping only the character parts. Figure 1 (c) and (d) show the masked images of two character images extracted from two currency notes (one genuine and one fake). Figures 1 (e) and (f) show the histograms of gray levels as computed on the masked images.

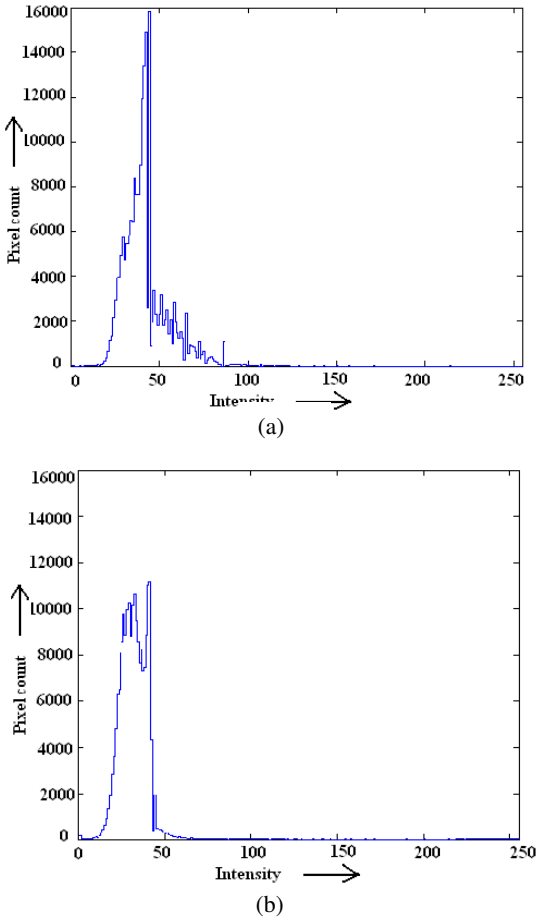
Hole count (f_2): Number of holes appearing on character strokes gives a significant clue about the genuineness of a bank note. In binary images of the characters, holes appear as patches of white on the black background of the character. Hole refers to an eight connected white pixel cluster appearing on the character stroke. The ratio of the number of holes to the character area (total area covered by the character stroke) is considered a feature. The images in figures 2 (a) and (b) clearly (visually) show that this ratio is significantly greater in characters corresponding to fake currencies than in letters of authentic banknotes. Such ratios for images in Figure 1(a) and 2 (a) are 0.0009 and 0.0011, respectively, whereas for the images in Figure 1(b) and 2 (b) are 0.0015 and 0.0021.

Average hue (f_3): Fake banknotes may sometime appear same as genuine notes in color but by computing the average hue from the character strokes, we may be able to decide whether they are actually printed by using the same technique. Figure 3 shows the discriminatory power of this feature for the genuine and fake samples corresponding to figures 1(a) and (b).

Contrast (f_4): The human eye normally fails to capture slight difference in brightness (or glossiness) of two banknotes and this aspect is tactfully used by the counterfeiters. The difference in brightness (or the reflectivity of light) between two samples can be used to detect the method of printing. We capture this feature

(a) (b)

Figure 2. Holes in character images: (a) a genuine and (b) a fraudulent samples.



(a) (b)

Figure 3. Histogram of hue of character strokes: (a) genuine and (b) fake samples.

by computing the RMS contrast [18] of a character images extracted from a banknote. The RMS contrast does not depend on the spatial frequency content or the spatial distribution of intensity in the image. It is defined as the standard deviation of the pixel intensities as follows: $\sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(I_i-\bar{I})^2}$, where N is the total number of pixels in the image, I_i is the intensity of the i-th pixel and $\bar{I}$ is the mean pixel intensity. Background masking is not done in this case as the background does not affect the results significantly and thus saves computational time. For example, when the genuine samples as in figures 1(a) and 2(a) are processed, we get 68.7374 and 66.7003 as the values of this feature, whereas the corresponding values are 58.7816 and 55.9164 for the fake samples as shown in figures 1(b) and 2(b).

Key tone (f_5): The tonal range of an image refers to its general distribution of intensity. Key tone of an image is represented by the mean gray value of all the pixels. The value of key tone indicates whether the bulk of information in an image is stored in the high/middle/low intensity zone. The value of key tone indeed varies from genuine to fake currency notes due to the difference in pigments used for the printing process. Therefore, we use key tone as a feature in identifying printing techniques.

Average Color (f_6): The amount of a particular color used for printing is different for different printing processes. This difference is further magnified by reconstructing the image matrix using a function *S(i)* as given in Eq. (1). Here we have considered two different color streams blue (B_{blue}) and black (B_{black}) (these two colors mostly occurring in the character strokes) and altered their contribution in the image according to the *S(i)* function. This transformation is controlled by a parameter, p, and further details can be found in [4].

$$S(i) = pB_{blue}(i) + (1-p)B_{black}(i) \quad , 0<p<0.5 \tag{1}$$

where $B_{blue}(i)$ and $B_{black}(i)$ are the individual blue and black values of a pixel of the original image. The images in figure 1(a) and (b) after the said color transformations are shown in Figure 4(a) and (b), respectively. The average of the newly computed color stream S_{AVG} ($=\frac{\sum s(i)}{N}$) is used as a feature to predict the printing process. When p is set to 0.2, we get S_{AVG} values for the image in Fig. 1(a) and 2(a) as 40.3973 and 34.98, whereas these values for Fig. 1(b) and 2(b) are 27.1902 and 25.2481.

Edge roughness (f_7): The interaction of the ink with the substrate (paper) leaves some typical characteristic of the printing process. This issued has been discussed in the papers [15, 16] from where we borrow the following three features that explicitly capture this aspect in order to give a measure to gaze the printing process. The first one is to measure edge roughness. The difference in the amount of smoothening of the character image with respect to its original image on application of an averaging filter is useful to categorize a particular printing process. Here we have used a median filter to smoothen the image. Then the images are converted to binary level using the Otsu threshold. The difference of perimeter of the two images (smoothened image and original image) is expressed as a ratio as follows:

$$E_{\text{PBER}} = (p_a - p_b)/p_b \tag{2}$$

Here p_a is the perimeter of the actual image, p_b is perimeter of the filtered binary image and E_{PBER} is the *perimeter based edge roughness* [15] based on a relative difference of boundary perimeters.

Area difference (f_8): The feature related to area difference [16] is calculated as follows. At first, a character image is binarized using Otsu threshold value (say, T). The same image is again binarized using a different threshold value that is calculated by adding a normalized parameter *sc* to T. The difference in character areas that results on binarization is then expressed as a ratio of the area of the original Otsu-given image as given below.

$$\text{Area difference} = \left|(A_{\text{otsu+sc}} - A_{\text{otsu}})\right| / A_{\text{otsu}} \tag{3}$$

Correlation coefficient (f_9): Measuring the correlation coefficient between original gray-scale image and the corresponding binary image characterizes individual printer's behavior in producing letter contours [16]. This is calculated by using edge images of the gray and binary images. Let A be the original gray value image and B be the corresponding binary image, then the correlation coefficient is calculated as,

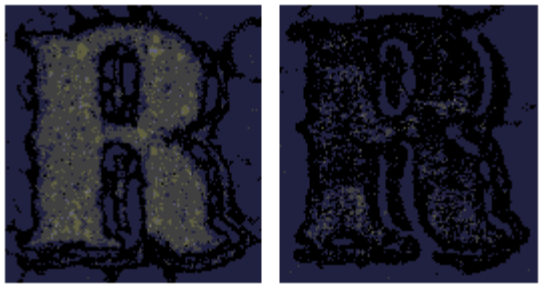


Figure 4. Parametric color transformation: (a) genuine and (b) fake samples.

$$\frac{\sum_{[i,j]\in ROI}\left(A[i,j]-\bar{A}\right)\left(B[i,j]-\bar{B}\right)}{\sqrt{\sum_{[i,j]\in ROI}\left(A[i,j]-\bar{A}\right)^2}\sqrt{\sum_{[i,j]\in ROI}\left(B[i,j]-\bar{B}\right)^2}} \tag{4}$$

where $\bar{A}$ and $\bar{B}$ are the mean of A and B. In our study, this coefficient is used as a feature.

3. AUTHENTICATION OF PRINTING TECHNIQUE

As mentioned earlier that intaglio printing technique is used to print letters and numbers on currency notes. For example, texts like "RESERVE BANK OF INDIA" or currency note denominations (e.g. 500 or 1000, etc.) are printed using this technique. Authentication of this printing technique is modeled as a 2-class classification problem, i.e. whether the printing technique is the particular intaglio category that is supposed to be used (say, this class is termed as *genuine, G*) or not (the class representing *fake* or *duplicate, D*). Let m be the number of text samples (i.e. character images) known as genuine and n be the number of samples known as duplicate. In the feature space, it is expected that these m samples would form a cluster (C_G) and n duplicate samples would form another cluster, C_D. To check whether these two clusters are linearly separable, we implement a

K-means algorithm and cluster the *m+n* labeled samples into two classes. Selecting two samples randomly initializes the centers in K-means algorithm. Since K-means results get affected by this initialization phase, K-means is executed more than once (three times) and each time clustering results are investigated. This investigation reveals that the clusters always overlap and therefore, it is difficult to find a linear decision boundary.

Next, support vector machines (SVM) are used aiming at determining the location of decision boundaries that produce the optimal separation of classes. Two types of common non-linear kernel functions namely, polynomial and radial basis function (RBF) are considered. The whole sample set consisting of genuine as well as duplicate samples is divided into four subsets. A four-fold test is conducted so that each subset appears at least once as in training, validation and testing. The proportion in which samples appear in training, validation and test data is 2:1:1 (training: 50%, validation: 25% and testing: 25%).

The classification accuracy is also checked with a Neural Network (NN)-based classifier. An MLP (Multi-Layer Perceptrons) consisting of 9 input nodes correspond to nine dimensions of a feature vector is used. The output consists of only one node to gives binary output (genuine or duplicate). Hidden layer, in the present experiment, contains 2 nodes. A logistic function as explained in the next section is used as the activation function of the network. Like SVM-based classifier a four-fold test is conducted for NN-based classification. Samples appear in training, validation and test data following the ratio 2:1:1.

The final decision about whether the printing technique of a currency note is genuine does not depend on checking of a single character image. As there are many character images on a note, therefore, printing technique is authenticated for number of character images all of which should pass the authenticity criteria. Failure for one image mark the banknote questioned. The decision making process is intentionally made very stringent to reduce false acceptance rate to almost zero.

Finally, a LDA (linear discriminant analysis) is also implemented. The features used in this experiment to authenticate printing technique vary in their power of discrimination. Hence, individual feature wise discrimination power is also studied. Next, features are sorted based on their decreasing power of classification and then gradually combined to achieve more classification accuracy.

Table 1. Clustering of Currency Note Printing Techniques using K-Means

Iterations	Distribution of Samples in Clusters				Clustering accuracy (%) = $(g_1+d_2)/2$
	#samples in genuine (G)		#samples in duplicate (D)		
	#G (g_1)	#D (d_1)	#D (d_2)	#G (g_2)	
1	95	9	91	5	93%
2	93	11	89	7	91%
3	95	7	93	5	94%
Avg	94.3	9	91	5.7	92.7%

4. EXPERIMENTS

Magnified scan digitized images of genuine and fake currency notes (Indian rupees of denomination 500) are collected. For considering our study, we consider 100 genuine samples and another 100 samples of fake currency note images. Note that here samples are marked as genuine and fake just based on the fact that whether expected intaglio printing has been used or not to print the samples.

Results of K-means: All the samples are at first clustered using some unsupervised clustering method. The purpose of this clustering is to analyze the distribution of samples in the feature space. The K-means algorithm is used for this purpose. The algorithm finds two clusters one corresponding to *genuine* samples and another for *duplicate* samples, i.e. value of K is set to 2. Initialization is done by choosing two samples randomly as to initialize two cluster centers.

The K-means results are evaluated by computing the number similar samples grouped together vs. the number of dissimilar samples contained in that group. Since all samples are tagged with their classes (*genuine* or *fake*) evaluating clustering results in this way is straightforward. Table-1 presents the evaluation of K-means results. Since cluster centers are initialized randomly, K-means were executed three times to get an average result.

Classification using SVM: Support vector machines are designed using two different types of non-linear kernel functions namely polynomial and radial basis function (RBF). These two kernel functions are defined as:

$$\text{Polynomial: } K(x, x') = (x.x' + 1)^d \tag{5a}$$

$$\text{RBF: } K(x, x') = \exp\left(-\gamma \|x - x'\|^2\right), \text{for } \gamma > 0 \tag{5b}$$

Where x denotes training vectors and d, γ are kernel parameters.

The set of 200 samples are divided into four sets to realize a four-fold experiment. In each run of an experiment, two sets are considered as training sets, the remaining two sets serve as validation and test sets. Four different runs were executed. Selecting sets in such a way that each set appears once as a test set and as a validation set (in another run) ensuring that each set would eventually appears twice as training set. The result of this four-fold experiment is reported in Table-2 (given on the last page of this paper). It is to be noted that the following values were estimated for the kernel parameters. For polynomial: $d = 3$ and for RBF: $\gamma = 1$ and they do not change with changing of training sets.

Table-2 shows some important observations. For the present problem, polynomial kernel function and RBF based kernel function perform similarly; both the kernels achieve very high classification accuracies. Moreover, the number of support vectors used by the polynomial kernel is far less than the number used by the RBF based kernel. Average number of iterations and norms of weight vectors of polynomial kernel function are far less than those of the RBF kernel function. Mean squared errors (MSE) show that the RBF kernel gives very low MSE when compared to the polynomial (poly) kernel. The MSE is computed as follows:

$$MSE = \frac{\sum_{j=1}^{T}\sum_{i=1}^{V}(d_{ij} - y_{ij})^2}{V \times T}$$ where V and T are the number of

support vectors and test samples, respectively, d_{ij} and y_{ij} are the desired output and SVM output, respectively for the i-th support vector and the j-th test sample.

Classification using Neural Network: A multilayer perceptron (MLP) is used to design a Neural Network-based classifier. Well-known back propagation algorithm is used to train the network. The network does use of the following logistic function as transfer or activation function.

$$f(x) = e^x/(1+e^x) \tag{6a}$$

A gradient descent method is used to find the optimized set of connection weights that are updated as per the following equation:

$$W_{(t+1)} = W_t + \alpha * (\frac{\partial E}{\partial W})|_{W(t)} + \beta * (W_{(t)} - W_{(t-1)}) \tag{6b}$$

Where α is the learning parameter, β is known as the momentum and E is the error term. In the present experiment, α is set to 0.9 and β is assigned 0.1. The same dataset as used for the SVM-based classifier is also used here to train and test the MLP. Like the SVM-based classification a four-fold experiment is conducted. Experiment shows that like SVM-based classifier NN-based classification too achieves very high accuracy (about 99.5%, 0.5% error is attributed to true negative) in classifying printing process as genuine or fake.

Table 3: Classification of Currency Note Printing Techniques Using LDA

	Bias (b)	Separability	% error
Run-1	-19.2192	5.7692	0.5
Run-2	0.9741	3.3903	0
Run-3	-28.8222	7.7076	0
Run-4	-3.7869	3.2253	0
Avg.	-12.71355	5.0231	0.125

Classification using LDA: Finally, we use Fisher linear discrimination analysis (LDA) for authentication of printing process. Suppose $\vec{\omega}$ is the normal to the discriminating hyper plane, $\vec{\mu}_{y=0}, \vec{\mu}_{y=1}$ are the sample means and $\sum_{y=0}$ and $\sum_{y=1}$ are the covariance matrices of the two classes (*genuine* and *duplicate*). Now we can consider that $y = 0$ for $\vec{\omega}^T .X + b >= 0$ for one class and $y = 1$ for $\vec{\omega}^T .X + b < 0$ for the other class. From these equations, parameter vector $\vec{\omega}$ is computed to maximize class separability criterion and b is the bias, which lies in between the means of the training samples projected onto this direction. The separation between these two distributions is to be the ratio of the variance between the two classes and is given by

$$S = \frac{\sigma^2_{between}}{\sigma^2_{within}} = \frac{(\vec{\omega}.\vec{\mu}_{y=1} - \vec{\omega}.\vec{\mu}_{y=0})^2}{(\vec{\omega}^T \sum_{y=1} \vec{\omega} + \vec{\omega}^T \sum_{y=0} \vec{\omega})} \tag{7}$$

For Fisher LDA, this separation achieves maximum when

$$\vec{w} = (\sum_{y=0} + \sum_{y=1})^{-1} (\vec{\mu}_{y=1} - \vec{\mu}_{y=0}) \tag{8}$$

Like SVM and NN a four-fold experiment is conducted and results are reported in Table-3. The average weight vector $\vec{\omega}$ on maximizing class separablility criterion is 5.0231 whereas the bias b is computed as –12.7136.

Gradation of the features: In this experiment, we use nine features but all of them do not contribute equally in authenticating the printing technique. Fig. 5 shows their power of discrimination when LDA is used for classification. The correlation feature (i.e. f_9 as discussed in section-2) shows the highest discriminatory power (93%) for this purpose. Next is dominant intensity i.e. feature f_1 (91.1%). The blue line shows the features in their decreasing power of classification. The brown line shows the effect of combining features. When f_9 and f_1 are combined, the classification rate goes up to 95.4% and finally combination of all the nine features gives an accuracy of about 99.8%.

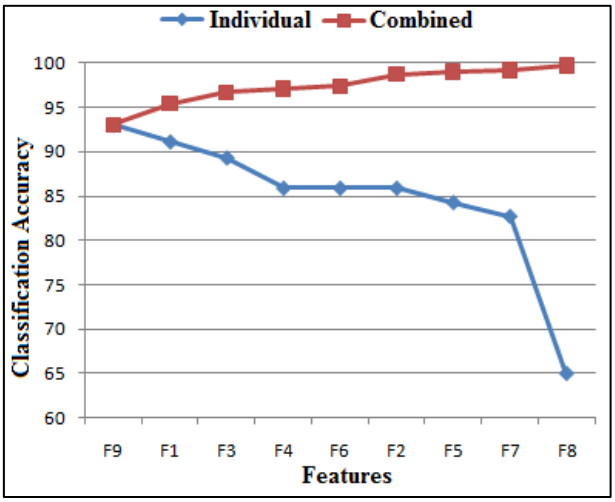


Figure 5. Classification capability of individual (blue line) features and their gradual combination (brown line).

5. CONCLUSIONS

This paper presents a novel experiment on authenticating the printing technique in currency notes. Fraudulent currency notes often could not match the genuine printing technique while producing fake notes. The research embodied in this paper nicely shows that using the standard image analysis and pattern classification techniques an automatic method can be designed to capture many fraudulent cases. This authentication method would assist the people in forensic sciences or in financial organizations to identify fake notes. The features used in this experiment are quickly computable and therefore, the proposed method provides a quick (and possibly low cost too) solution to the problem.

Three different classifiers have been used in this study. Integration of them can also be done in future to build a more robust classification scheme. However, testing of this method using a large dataset is required to establish it as a standard practice. The method, indeed, is not only restricted to currency notes only. Printing technique is itself a security feature in most of the

security paper documents. Therefore, this research provides a viable framework for machine authentication of security documents through verifying the printing technique.

6. ACKNOWLEDGEMENT

The authors sincerely acknowledge the active help and cooperation of the question document examiners of the Department of Forensic Sciences, Kolkata, India.

Table 2: Classification of Currency Note Printing Techniques Using SVM

	#Support Vec.		#Iterations		Weight Vector |w|		% accuracy		MSE	
	Poly	**RBF**	**Poly**	**RBF**	**Poly**	**RBF**	**Poly**	**RBF**	**Poly**	**RBF**
Run-1	3	25	11	16	1.0597	4.0832	100	100	1.297	0.129
Run-2	6	24	4	10	1.1435	4.188	100	99	1.576	0.132
Run-3	4	23	3	10	0.8056	4.1843	100	99.5	1.044	0.154
Run-4	4	23	6	13	0.9311	4.28	99.5	100	1.354	0.112
Avg.	4.25	24	6	12.3	0.9852	4.1839	99.9	99.6	1.318	0.134

7. REFERENCES

[1] The Times of India, 1st March 2009, http://timesofindia.indiatimes.com/news/india/Beware-the-fakes-RBI-teaches-kids/articleshow/4206645.cms [last accessed on 14th July 2010]

[2] H. Hassanpour, A. Yaseri, and G. Ardeshiri, "Feature extraction for paper currency recognition," in Proc. of the 9th International Symposium on Signal Processing and Its Applications (ISSPA), pp. 1-4, Sharjah, United Arab Emirate, 2007.

[3] H. Hassanpour and P.M. Farahabadi, "Using Hidden Markov Models for paper currency recognition," Expert Systems with Applications: an International Journal, Vol. 36 (6), pp.10105-10111, 2009.

[4] C. Herley, P. Vora, and S. Yang, "Detection and deterrence of counterfeiting of valuable documents," in Proc. of the Int. Conf. on Image Processing (ICIP), pp. 2423-2426, Singapore, 2004.

[5] D. Gruhl and W. Bender, "Information hiding to foil the casual counterfeiter," in Proc. of the 2nd Int. Workshop on Information Hiding, LNCS, Vol. 1525, pp. 1-15, Springer-Verlag, London, UK, 1998.

[6] A. Vila, N. Ferrer, J. Mantecon, D. Breton, and J.F. Garcia, "Development of a fast and non-destructive procedure for characterizing and distinguishing original and fake euro notes," Analytica Chimica Acta, Vol. 559 (2), pp. 257-263, 2006.

[7] J. Oliver and J. Chen, "Use of signature analysis to discriminate digital printing technologies," in Proc. of the Int. Conf. on Digital Printing Technologies, pp. 218-222, San Diego, California, 2002.

[8] Eric Kee and Hany Farid, "Printer Profiling for Forensics and Ballistics," in Proc. of the 10th ACM workshop on Multimedia and Security, pp. 3-10, Oxford, UK, 2008.

[9] Orhan Bulan, Junwen Mao and Gaurav Sharma, "Geometric distortion signatures for printer identification," in Proc. of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp.1401-1404, 2009.

[10] C. K. Li and S. C. Leung, "The Identification of Colour Photocopiers: A Case Study," Journal of the American Society of Questioned Document Examiners, Vol. 1(1), pp. 8-11, 1998.

[11] C.K. Li, W.C. Chan, Y.S. Cheng and S.C. Leung, "The Differentiation of Color Laser Printers," Journal of the American Society of Questioned Document Examiners, Vol. 7(2), pp. 105-109, 2004.

[12] J.S. Tweedy, "Class Characteristics of Counterfeit Protection System Codes of Color Laser Copiers," Journal of the American Society of Questioned Document Examiners, Vol. 4(2), pp. 53-66, 2001.

[13] A.K. Mikkilineni, P.-J. Chiang, G.N. Ali, G.T.C. Chiu, J.P. Allebach, and E.J. Delp, "Printer identification based on texture features," in Proc. of the Int. Conf. on Digital Printing Technologies, pp. 306-311, Salt Lake City, UT, 2004.

[14] A.K. Mikkilineni, P.-J. Chiang, G.N. Ali, G.T.C. Chiu, J.P. Allebach, and E.J. Delp, "Printer identification based on graylevel co-occurrence features for security and forensic applications," in Proc. of the SPIE Int. Conf. on Security, Steganography and Watermarking of Multimedia Contents VII, Vol. 5681, pp. 430-440, San Jose, CA, 2005.

[15] C. Schulze, M. Schreyer, A. Stahl, and T.M. Breuel, "Evaluation of Gray level Features for Printing Technique Classification in High Throughput Document Management Systems," in 2nd Int. Workshop on Computational Forensics (IWCF), LNCS, Springer Berlin/Heidelberg, Vol. 5158, pp. 35 – 46, Washington, DC, USA, August, 2008.

[16] C.H. Lampert, L. Mei, and T.M. Breuel, "Printing Technique Classification for Document Counterfeit Detection," in Proc. of Int. Conf. on Computational Intelligence and Security, pp. 639-644, China, 2006.

[17] H. Dasari and B. Chakravarthy, "Identification of Non-Black Inks Using HSV Colour Space," in Proc. of Int. Conf. on Docu. Anal. Recog. (ICDAR), pp. 486-490, Brazil, 2007.

[18] E. Peli, "Contrast in complex images," J Opt Soc. of Am., Vol. **7**(10):2032-40, 1990.