Image-Based Approach for the Detection of Counterfeit Banknotes of Bangladesh

Mohammad Shorif Uddin, Pronaya Prosun Das, Md. Shamim Ahmed Roney
Department of Computer Science and Engineering
Jahangirnagar University
Dhaka, Bangladesh.
shorifuddin@juniv.edu, pronaya.prosun@gmail.com, roney.ewu@gmail.com

***Abstract*— Currency duplication also known as counterfeit currency is a vulnerable threat on economy. It is now a common phenomenon due to advanced printing and scanning technology. Bangladesh has been facing serious problem by the increasing rate of fake notes in the market. To get rid of this problem various fake note detection methods are available around the world and most of these are hardware based and costly. In the present paper an automated image-based technique is described for the detection of fake banknotes of Bangladesh. Security features of banknotes such as watermark, micro-printing and hologram etc. are extracted from the banknote images and then detection is performed using Support Vector Machine (SVM). Experimental results confirm the effectiveness of the proposed algorithm.**

Keywords— Counterfeit currency; Canny edge detector; Image Registration; Histogram of Oriented Gradient (HOG); Support Vector Machine (SVM)

I. INTRODUCTION

Nowadays all the countries are facing the growing and challenging difficulties of counterfeiting of its banknotes. Since from the invention of currency around the world a global challenge has been started to stop counterfeiting of currency. Though there are several security features has been incorporated to protect the banknotes from counterfeiting, but due to advancement of the printing media technology, it has become an easy task to counterfeit paper banknotes. Hence, fake banknotes' detection is an emergence issue for a country to protect its economy as well as people's faith on currency.

There are allegations that money withdrawn in a bundle from banks or from Automated Teller Machines (ATMs) contains one or two fake notes. People having in their possession such notes have no option but to suffer financial loss since the banks would flatly refuse to admit their folly. Banks are very much vulnerable to the attack of currency racketeers as some of their branches are not equipped well with counterfeit money detectors.

At present there are many techniques have been used to detect the fake notes but unfortunately these are expensive, complex, less accurate, not conveniently portable and also not in the range of general people's ability. To overcome these drawbacks, in this paper an image-based automated fake note detection approach is described. This technique extracts security features from the images of a banknote and detects its authenticity using Support Vector Machine (SVM). Our ultimate goal is to develop an algorithm that will be efficient for the mobile devices such as smart phone, tablets etc.

The remainder of this paper maintains the following organization. Section II presents summary of related works. In section III, security features of Bangladesh banknotes are discussed. Proposed methodology is demonstrated in Section IV. Section V shows experimental results and finally conclusions are drawn in section VI.

II. RELATED WORKS

Here we are going to highlights some image-based techniques for counterfeit currencies. One of the most recent works on fake currency detection of Bangladesh is presented in reference [1] where image features of the banknotes were extracted using contour analysis, Canny-edge detection and Hough transformation. In another paper [2], Ensemble Neural Network (ENN) was used to develop a currency recognition system. It was trained using negative correlation learning method. Various types of note images are converted to grayscale and compressed. Then each pixel of that image is fed to the network as an input. Old or noisy image of banknote can be recognized by this system. Aoba et al [3] presented a method for recognizing Euro-banknotes using a three-layered perception and a Radial Basis Function (RBF) neural networks. Three-layered perception is used for classifying banknotes and validation is done using several RBF networks. In addition, Power et al [4] proposed a counterfeit Indian currency detection using HSV (Hue Saturation Value) color-based method. All these methods have limitations.

III. SECURITY FEATURES OF BANGLADESH BANKNOTES

In the current work we have investigated only 500 and 1000 taka-valued two Bangladesh banknotes. Security features of 500 and 1000 Bangladesh Taka (BDT) are presented here briefly [5]. There are 9 and 10 types of security features are available in the notes of 500 and 1000 BDT, respectively. Some of these are visual and some can only be quantified physically. The security features are described below and some are shown in Figure 1.

- Size: The size of 1000 BDT is 160mm × 70mm and 500 BDT is 152mm × 65mm.
- Paper Quality: Both notes are printed on highly durable paper containing synthetic fiber.

978-1-5090-1269-5/16/$31.00 ©2016 IEEE

- Optical Variable Ink (OVI): The numeral 500 and 1000 in the upper right hand side for the notes of 500 and 1000 BDT, respectively, will change their colour in the event of oscillation.
- Latent Image: When the notes are headed horizontally, they show an image of ৫০০ for 500 taka note and ১০০০ for 1000 taka note.
- Security Thread: Both notes have a 4mm security thread embedded on the left side of the note containing the logo of the Bangladesh Bank with their respective note value and they appear white when seen directly and black when seen from 90 degree angle.
- Micro Lettering: For 500 BDT, repeated microprints of the text 'BANGLADESH BANK' can be seen in the vertical straight line left to the security thread and also just beside the text 'FIVE HUNDRED TAKA' on the left-back side. There are repeated microprints of the text 'BANGLADESH BANK' over the denomination '500' which is printed in light color at the bottom-left corner on the back side of the note. For 1000 BDT, repeated microprints of the texts '1000 TAKA' and 'BANGLADESH BANK' in two distinct vertical straight lines can be found on the left to the security thread and vertical straight lines of the text 'BANGLADESH BANK' just inside the pattern on the back-left side and of the text 'ONE THOUSAND TAKA' on the back-right side. There are repeated microprints of the text 'BANGLADESH BANK' over the denomination '1000' which is printed in light color at the bottom-left corner on the back side of the note These microprints can only be seen with the help of a magnifying glass.
- Watermark: This feature contains the Portrait of the Father of the Nation Bangabandhu Sheikh Muzibur Rahman, an electrolyte mark showing the number 500 for 500 BDT and 1000 for 1000 BDT and on the left side of the portrait a logo of Bangladesh Bank. These marks become comprehensible if the banknotes are placed opposed to light. The best way to recognize an original note by identifying the specific pattern printed upon hologram.
- Intaglio Ink: Seven parallel slanted straight lines in the right hand side, the portrait of the Father of the Nation Bangabandhu Sheikh Muzibur Rahman in the left hand side, four (500 BDT) and five (1000 BDT) small dots at the right hand side for the blind to recognize the note, value of the notes were written in Bengali and English on the middle portion of the front side and photograph of cultivation in 500 BDT and National Parliament building in 1000 BDT are printed in intaglio ink which are felt rough when rubbed by finger.
- Others: Both notes contain picture of National Monument in light color in the middle of the front side. The text 'BANGLADESH BANK' is printed on the 'Iridescent Stripe' in light blue colour in 1000 BDT. The colour will vary when the note is oscillated.

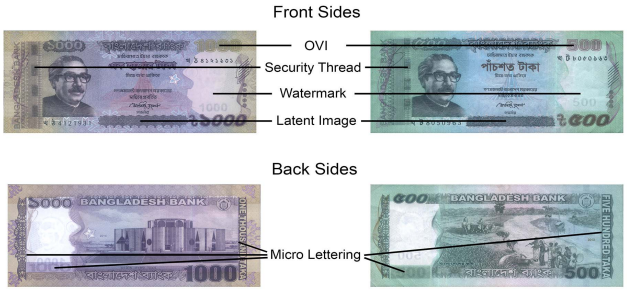

Figure 1: Some visual security features of 500 and 1000 BDT.

IV. Proposed Methodology

Counterfeit currency detector differs based on particular security features of banknotes of a country. In our work, we have chosen three features which will be used to test the fakeness and these features are used as inputs to train the SVM for classification. Image acquisition is performed using mobile camera. So automated image registration is used to separate the note portion from the background. At the same time, a decision is made about note denomination. Based on this decision, particular classifier is invoked as there are two sets of classifiers in this system. One for 500 BDT and another for 1000 BDT. The overall methodology is shown in Figure 2.

A. Selected Features

500 and 1000 BDT contains 5 and 6 types of visual feature, respectively. Those security features can be used to check the originality of a note via image processing based approaches. Among them, Optical Variable Ink, Security Thread and Iridescent Stripe are not considered in this work. To check Optical Variable Ink and Iridescent Stripe (only available in 1000 BDT), we need at least two snapshots which are differentiated by certain angles. Common user may face difficulty to take pictures in that way. Besides it also increases the number of images that is needed to be processed. Security thread contains the logo of the Bangladesh Bank with their respective note value. They change colour when seen from different angle. So again users need to take multiple images which increases difficulty. For this reason, we choose not to include these features in our work. For testing fakeness of banknotes following features are considered.

1) *Watermark*
2) *Latent Image*
3) *Micro-printing*

In original note, the watermark is printed perfectly. Its quality is excellent and unblemished. Besides, there are some precise and distinguishable pattern on watermark which is not available on fake notes. Another basic and potent feature of Bangladesh banknotes is micro-printing. It is not visible to our bare eyes. We have to use magnifying glass to validate its existence. As well the camera is needed to be focused appropriately to acquire the image of micro-text. Replication of this feature in counterfeit notes is very hard by using ordinary printers. It requires very costly printing. Latent Image in horizontal bands on the lower border is also hard to duplicate for the counterfeiters. The above mentioned features of Bangladesh banknotes are salient, easily detectable using computer and

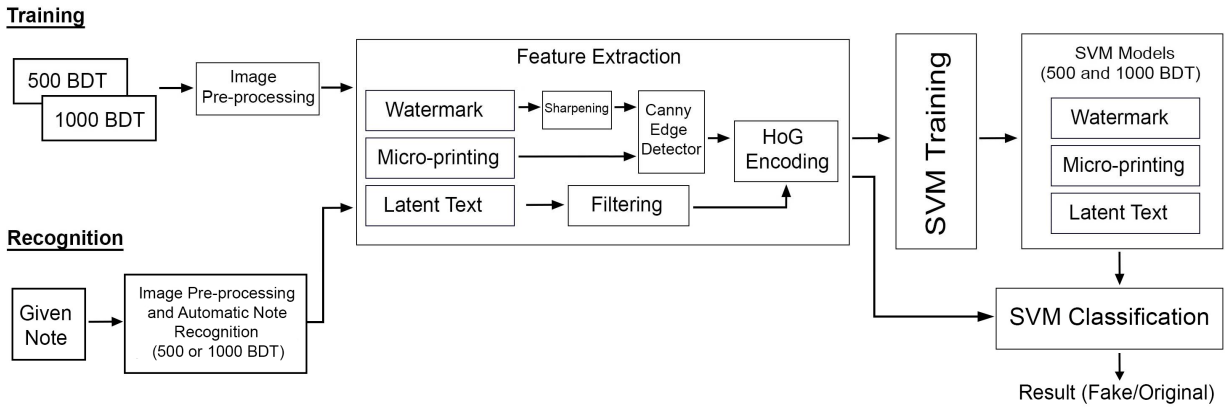

Figure 2: Overall methodology of our proposed approach.

gives solid foundation against counterfeiting. So these visual features are chosen to perform forgery detection.

B. Image Acquisition and Pre-processing

Images of banknotes are obtained using mobile camera that has at least 8MP CCD. An acquired image of 1000BDT is given in Figure 3.

Figure 3: An acquired image of 1000 BDT note by a mobile camera.

As mobile camera is used to capture the image, it is evident that there will be some distortion like scale, rotation, skewness etc. The aim of image pre-processing is to suppress undesired distortions and crop the note portion from background using image registration technique [6].

Initially, we use a high speed corner detector Algorithm [7] to detect important keypoints from the acquired image. Extracted keypoints are shown in Figure 4. Then those keypoints are described using FREAK (Fast Retina Keypoint) descriptor [8]. Euclidian distances between descriptors from acquired and referenced images are calculated. The pair with smallest distance is considered to be matched point.

Figure 4: Keypoints are matched between acquired and referenced images.

Then homography matrix is computed from corresponding points where unreliable points are discarded using RANSAC (Random Sample Consensus) algorithm [9].

The acquired image is registered using homography matrix. There are different kinds of transformations. We use 2D Projective transformation [10] to complete our registration process.

Figure 5: The registered image of 1000 BDT shown in Figure 3.

C. Pattern Extraction from Watermark

Watermark contains on the portrait of Bangabandhu Sheikh Muzibur Rahman. Our main concern is to extract the pattern that is imprinted upon watermark. Initially the feature is sharpened using unsharp masking technique [11]. Then Canny-edge detector [12] is used to enhance the edges. Figure 6 shows the visual differences between original and fake patterns obtained from watermark portion of 1000 BDT after Canny-edge detection.

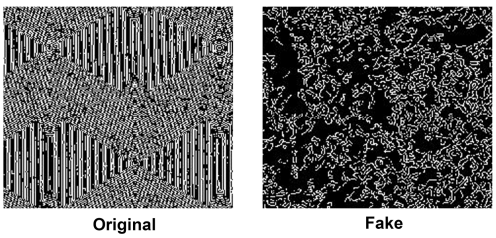

Figure 6: Visual differences between original and fake patterns obtained from watermark portion of 1000 BDT after Canny-edge detection.

From here, we can intuitively say that edge directions or distribution of intensity gradients are very important in this context. So it will be convenient to use a kind of encoding that is able to preserve the gradient orientation from the pattern. For this purpose, we can use descriptor like Speeded Up Robust

Features (SURF), Scale-Invariant Feature Transform (SIFT), Histograms of Oriented Gradients (HOG), binary descriptors etc. But SIFT and SURF are patented and also computationally expensive. Binary descriptors have some performance issue. That is why we choose to use HOG as a global descriptor to describe the whole image [13]. It produces a vector of oriented gradients that is used to train SVM. The process is illustrated in Figure 7 for 1000 BDT.

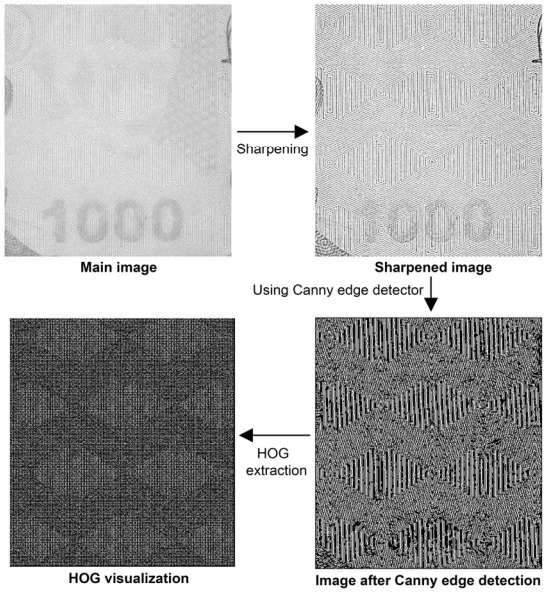

Figure 7: Pattern extraction from watermark of 1000 BDT.

D. Obtaining Pattern from Latent Image

Both 500 and 1000 BDT contain the inscription ৫০০ and ১০০০ latently on the lower border. For 500 BDT, the inscription contains a set of straight lines which are vertical and tilted rightward. Upon this ৫০০ is imprinted using vertical leftward tilted straight lines. In case of 1000 BDT, lines are drawn in opposite manner. That means, inscription contains straight lines that lie vertically and are tilted leftward and ১০০০ is imprinted using vertical rightward tilted straight lines. To enhance the pattern of the latent image, we use the filters of Figures 8(a) and 8(b) for 500 and 1000 BDT, respectively. Those filters mute the lines which are inside ৫০০ and ১০০০ and enhance the lines outside of those figures. The idea is to keep and intensify the lines that are outside of inscription ৫০০ and ১০০০. Figure 9 shows the enhancement of latent image of 500 and 1000 BDT.

2	1	0
1	0	-1
0	-1	-2

(a)

0	1	2
-1	0	1
-2	-1	0

(b)

Figure 8: (a) is used for 500 BDT and (b) is used for 1000 BDT.

Now HOG is used to encode the enhanced image for the same reason as it is used earlier. Then the HOG feature vectors are used as an input for SVM.

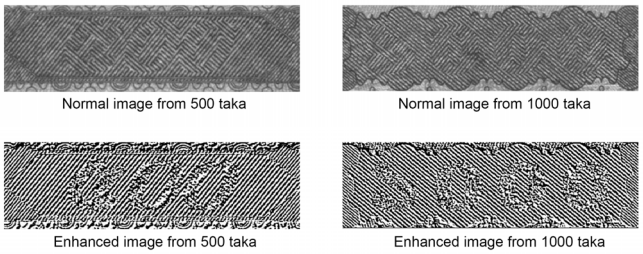

Figure 9: Enhancement of latent image of 500 and 1000 taka notes.

E. Obtaining Pattern from Micro-printing

One of the strong security features of Bangladesh banknotes is micro-printing. “500 TAKA”, “1000 TAKA”, “BANGLADESH BANK” etc. are repeatedly written on the banknotes of 500 and 1000 BDT using micro-letter. For simplicity and robustness, micro-prints in light color at the bottom-left corner on the back side of the note are chosen. Canny-edge detector is used to enhance the edges of the pattern and then HOGs are extracted, as it will be used to train SVM.

Our goal is not to recognize characters as it was done in paper [1], rather to recognize the pattern. Figure 10 shows pattern after using Canny-edge detector.

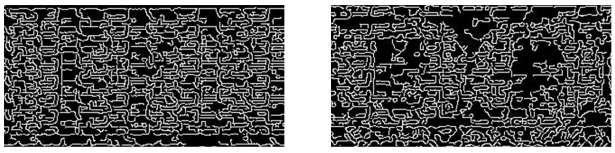

Figure 10: Difference between the patterns obtained from Micro-printing of 1000 BDT (After Canny-edge detection).

F. HOG and SVM

We use HOG descriptor of cell size 4 × 4 to encode the patterns (HOG feature vectors) which are illustrated earlier. The HOG feature vectors are fed to SVM.

In our work, Support Vector Machine (SVM) is used to perform classification [14], [15]. SVM is trained for two sets of models: one for 500BDT and another for 1000 BDT. The main idea behind training of SVMs is to find the separating hyperplane optimally so that the classification error is minimized for the given test samples.

Assume a set of M training samples of two separable classes are represented by (x_1, y_1), (x_2, y_2), …, (x_M, y_M); where $x \in R^N$ is an N-dimensional space and class label is denoted by y, $(y_i \in \{-1, +1\})$. A SVM attain the optimal hyperplane which linearly classifies (separates) the larger portion of the training data points while maximizing the distance from the hyperplane. Twice of this distance is called the margin. The hyperplane discriminant function is described by the following equation:

$$f(x) = \sum_{i=1}^{M} y_i, \alpha_i \,.\, k(x, x_i) + b$$

Where, the membership of x is determined by the sign of $f(x)$ and kernel function is denoted by $k(\cdot,\cdot)$. Finding all the

nonzero α_i is the equivalent of constructing an optimal hyperplane. A vector x_i is said to be supported vector (SV) of the hyperplane, if it comply to a nonzero α_i. SVMs provide a compact classifier as the number of training data points which are maintained as the support vectors is generally very small.

V. Result Discussion

We have implemented our algorithm in MATLAB (version 8.4.0 (64bit)). All the experiment were performed on a computer bearing the configuration as follows:

CPU: Intel Core i3-2350M 2.30 GHz

RAM: 8 GB DDR3 1333MHz

Operating System: Windows 10 64bit.

There are 70 banknotes in our dataset. 20 notes are used to train our system where 10 notes are of 500 BDT and another 10 notes are of 1000 BDT. Among them half of the notes are fake and other half of the notes are original. Test sample contains 25 notes each of 500 and 1000 BDT, in total 50 notes. 500 BDT set has 11 fake and 14 original notes. 1000 BDT set has 8 fake and 17 original notes.

Each feature of 500 and 1000 BDT is trained and tested separately. So 2 sets of SVM models are trained and each set contains 3 models for 3 features. For simplicity, watermark, latent image and micro-printing models are going to be denoted using f1, f2 and f3, respectively. The output of these models is either 0 if it is fake or 1 for original. Finally, we combine these result using the following equation.

$$result = \left(\frac{f1}{3} + \frac{f2}{3} + \frac{f3}{3}\right) \times 100$$

If the result value is more than 50, then the note is detected as original. That means 2 out of 3 features have to recognize as original to testify the note as original. Our method produces 100% recognition accuracy so far. This is because of small data size and also images are taken with good resolution mobile camera and with care. Confusion matrices for 500 and 1000 BDT are given in Table I and Table II, respectively.

TABLE I. CONFUSION MATRIX FOR 500 TAKA NOTE.

		Predicted Class	
		Fake	**Original**
Actual Class	**Fake**	11	0
	Original	0	14

TABLE II. CONFUSION MATRIX FOR 1000 TAKA NOTE.

		Predicted Class	
		Fake	**Original**
Actual Class	**Fake**	8	0
	Original	0	17

Average computational time for individual steps are shown in Table III.

TABLE III. COMPUTATIONAL TIME FOR DIFFERENT STEPS.

Steps	**Average Time (s)**
Image Pre-processing and Registration	2.91
Watermark Classification	0.28
Latent Image Classification	0.06
Micro-printing Classification	0.08

VI. Conclusion

In this paper, an image-based methodology has been proposed to identify counterfeit Bangladesh banknotes of 500 and 1000 BDT. We used SVM classifier after extracting three security features (watermark, latent image and micro-text) from the acquired images of the banknotes. Here we have considered two types of banknotes (500 BDT and 1000 BDT). With limited testing we have got 100% recognition accuracy. However, rigorous testing with diverse situations of currencies is required for full validation of the proposed approach that will be our immediate work. In addition, we are interested to involve more features to detect forgery and also extend the support for all kinds of Bangladesh banknotes. Besides we are going to implement this technique for Android framework that will ensure greater portability.

References

[1] Z. Ahmed, S. Yasmin, M. N. Islam, R. U. Ahmed, "Image processing based Feature extraction of Bangladeshi banknotes," Proc. Software, Knowledge, Information Management and Applications (SKIMA), pp.1-8, 18-20 Dec. 2014.

[2] Kalyan Kumar Debnath, Sultan Uddin Ahmed, Md. Shahjahan, "A Paper Currency Recognition System Using Negatively Correlated Neural Network Ensemble", Journal of Multimedia, December 2010, Vol. 5, No. 6, pp. 560-567.

[3] Masato Aoba, Tetsuo Kikuchi, Yoshiyasu Takefuji, "Eurobanknote recognition system using a three layer perceptron and RBF networks", IPSJ Transactions on Mathematical Modeling and Its Application, Vol 44, May 2003, pp. 99-109.

[4] Pragati D. Pawar, Shrikant B. Kale, "Recognition of Indian Currency Note Based on HSV Parameters", International Journal of Science and Research (IJSR), Vol 3, Issue 6, pp.132-137, June 2014.

[5] Bangladesh Bank Notes, Available Online: https://www.bb.org.bd/currency/note.php, accessed on January 10, 2016.

[6] Barbara Zitova, Jan Flusser, "Image registration methods: a survey", Image and Vision Computing, Vol. 21, pp. 977–1000, 2003.

[7] E. Rosten and T. Drummond, "Machine Learning for High-Speed Corner Detection", Proc. 9th European Conference on Computer Vision (ECCV), Graz, Austria, May 7-13, 2006, pp.430-443.

[8] A. Alahi, R. Ortiz, P. Vandergheynst, "FREAK: Fast Retina Keypoint," Proc. IEEE CVPR, pp. 510-517, 16-21 June 2012.

[9] T. Vincent and R. Laganiere "Detecting planar homographies in an image pair," Proc. ISPA 2001. pp.182-187.

[10] Chi Yu-Tseh, Ho Jeffrey and Yang Ming-Hsuan, "A Direct Method for Estimating Planar Projective Transform", Proc. 10th Asian Conference on

Computer Vision, Queenstown, New Zealand, November 8-12, 2010, pp. 268-281.

[11] A. K. Jain, Fundamentals of Digital Image Processing. Englewood Cliffs, NJ: Prentice-Hall, 1989.

[12] Canny, John, "A Computational Approach to Edge Detection," in Pattern Analysis and Machine Intelligence, IEEE Transactions on PAMI, Vol. 8, no.6, pp. 679-698, Nov. 1986.

[13] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," Proc. IEEE CVPR 2005, pp.886-893, 25-25 June 2005.

[14] V. Vapnik, *The Nature of Statistical Learning Theory*, Springer, 1995.

[15] C. Cortes and V. Vapnik. Support vector networks. Machine Learning, 20, 1995.