Analysis of Banknote Authentication System using Machine Learning Techniques

Sumeet Shahani
Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, India

Aysha Jagiasi
Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, India

Priya R. L.
Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, India

ABSTRACT
Banknotes are one of the most important assets of a country. Some miscreants introduce fake notes which bear a resemblance to original note to create discrepancies of the money in the financial market. It is difficult for humans to tell true and fake banknotes apart especially because they have a lot of similar features. Fake notes are created with precision, hence there is need for an efficient algorithm which accurately predicts whether a banknote is genuine or not. This paper proposes machine learning techniques to evaluate authentication of banknotes. Supervised learning algorithms such as Back propagation Neural Network (BPN) and Support Vector Machine (SVM) are used for differentiating genuine banknotes from fake ones. The study also shows the comparison of these algorithms in classification of banknotes.

Keywords
Banknote Authentication, Back Propagation Neural Network, Support Vector Machine, Hold-out, ROC

1. INTRODUCTION
Despite a decrease in the use of currency due to the recent growth in the use of electronic transactions, cash transactions remain very important in the global market. Banknotes are used to carry out financial activities. To continue with smooth cash transactions, entry of forged banknotes in circulation should be preserved. There has been a drastic increase in the rate of fake notes in the market. Fake money is an imitation of the genuine notes and is created illegally for various motives. These fake notes are created in all denominations which brings the financial market of the country to a low level. The various advancements in the field of scanners and copy machines have led the miscreants to create copies of banknotes. It is difficult for human-eye to recognize a fake note because they are created with great accuracy to look alike a genuine note. Security aspects of banknotes have to be considered and security features are to be introduced to mitigate fake currency. Hence, there is a dire need in banks and ATM machines to implement a system that classifies a note as genuine or fake.

In the recent years, Soft computing techniques have been widely used to solve problems that are difficult to solve using conventional mathematical methods. Supervised learning techniques are widely used in classification problems. This paper evaluates supervised machine learning algorithms to classify genuine and fake notes, and compares algorithms on the basis of accuracy, sensitivity, and specificity. Consider someone wants to deposit money in the bank. The notes that are to be deposited are given to a human being to check for their authenticity. As the fake notes are prepared with precision, it is difficult to differentiate them from genuine ones. A recognition system must be installed to detect legitimacy of the note. The system should extract the features of the note using image processing techniques. These features will be given as input to the machine learning algorithm which will predict if the note is true or fake.

Supervised machine learning techniques such as BPN and SVM were implemented. The dataset used to train these algorithms was collected by extracting features from banknote images. The dataset also classifies all the samples into a particular class i.e. genuine or forged. A comparative study of these techniques with respect to their accuracy, sensitivity, specificity and precision rate is shown.

2. LITERATURE SURVEY
Preserving genuineness of higher denomination printed Banknotes is one of the critical issues. It has the major role in financial activities of every country [1]. The study in [1] evaluates different machine learning algorithms and concludes that Decision-Tree and MLP technique is best to classify a bank note. In [2], the features of the banknote are extracted using Fast Wavelet Transforms. Later, one-against-all classification approach was employed that classifies the note into four different categories: Genuine, High-Quality Forgery, Low-Quality Forgery, and Inappropriate ROI which resulted in 100% detection rate. Evaluation of SVM and BPN is done in [3] and [4] where BPN outperforms SVM. In [3], BPN gives 10% more accuracy than SVM and is determined as the best classifier for predicting proteins sequence based on their compositions, whereas in [5] and [6], SVM outperforms BPN. The results depend on the dataset and the type of classification problem.

The research in [7] implements a system for classifying Thai banknotes using neural networks. Firstly, images of notes are collected by a scanner which is saved as bitmap data. Features are extracted from this data and inputted to BPN for learning and recognition. In [8], a new method is proposed for banknote recognition; Probabilistic Neural Network (PNN) and 100% success rate is obtained. The study in [9] uses LVQ classifier for banknote recognition. The experiment has been applied to US dollars and can be used for another kind of banknotes.

The paper [10] presents a system for detecting counterfeit currency banknotes. The note is processed using camera and image is divided into parts using segmentation. Watermark histogram features are extracted from different segmentation region to match the watermark with Gandhi's portrait. The result is shown on the user interface. In a similar study in [11], the features are extracted from images by segmenting the

image. These features are fed to SVM classifier which then determines the authenticity of the note.

A system has been proposed in [12] for recognition of euro banknotes. The study shows that three-layered perceptron is proved to classify the banknotes into a certain class accurately by taking the banknote images as inputs. This model has been trained by the back-propagation method. After classification, a Radial Basis Function network is used for validation which rejects the invalid data. The model gives 100% acceptance rate of valid notes and 0% acceptance rate of the invalid banknotes.

3. DATASET DESCRIPTION

The dataset used to train the models is taken from UCI machine learning repository [13]. Data were extracted from genuine and counterfeit banknote images. The dataset has 1372 instances. There are 5 attributes out of which 4 are the features and one is the target attribute. The dataset contains a balanced ratio of both classes which is 55:45(genuine: counterfeit). The target class contains two values: 0 and 1 where 0 represents genuine note and 1 represents fake note.

Table 1. Dataset description [13]

Attribute Name	Value Type	Description
Variance of Wavelet Transformed Image	Continuous	Variance finds how each pixel varies from the neighboring pixels and classifies them into different regions [14].
Skewness of Wavelet Transformed image	Continuous	Skewness is the measure of the lack of symmetry [15].
Kurtosis of Wavelet Transformed image	Continuous	Kurtosis is a measure of whether the data are heavy-tailed or light-tailed relative to a normal distribution [15].
Entropy of image	Continuous	Image entropy is a quantity which is used to describe the amount of information which must be coded for, by a compression algorithm [16].
Class	Integer	Class contains two values 0 representing genuine note and 1 representing fake note

4. SETUP

The supervised learning models have been implemented in GNU Octave by applying the hold-out method to the input data. The dataset used is divided into two subsets i.e. ratio of 80:20. The bigger subset is used for training the models and the smaller subset is used to test whether the models can predict the genuineness of note or not.

5. MACHINE LEARNING TECHNIQUES

5.1 Back Propagation Neural Network

BPN uses gradient descent to train the artificial neural network. This method is efficient in adjusting the weights in the network by comparing the desired output with the actual output and distributing the error back to the hidden layers. The difference in actual and expected output is used by the cost function to calculate the error. BPN works in two phases; propagation phase where the input is forwarded through the network to generate the output and error is calculated at the output, weight update phase where the weights in the network are updated according to the error to gain the desired output. A standard BPN consists of 3 layers namely an input layer to accept the input which is connected to the hidden layer which processes the input and the output layer which gives the result.

The BPN model implemented has 1 input layer having four neurons, one hidden layer having eight neurons and one output layer having two neurons that gives the classification result. Fig.1 represents the two-dimensional plot where 100 random data points are displayed. Fig.2 displays the hidden units to see what features they are capturing the data by visualizing what the neural network is learning.

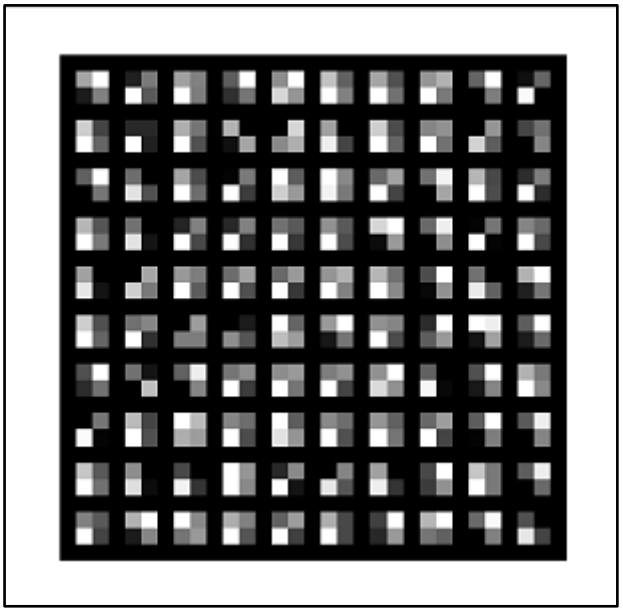

Fig 1: Representation of 100 datasets

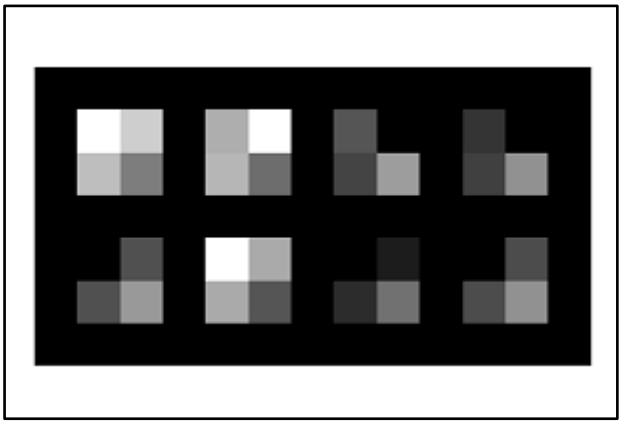

Fig 2: Visualization of BPN

5.2 Support Vector Machine

Support Vector Machines are supervised learning models that evaluate the data and recognize the patterns to classify the data. It creates a decision boundary to separate the two classes in the data. In SVM, each data item is plotted on the graph and then classification is performed to find the hyper plane that differentiates the two classes.

SVM uses a kernel function that projects the data from a lower-dimensional space to a higher-dimensional space [17]. This is done to make the non-linearly separable data into linearly separable.

Kernel functions are used in SVM as SVM does not perform well with huge datasets. For implementation purpose, linear kernel is used which is especially used for classification where there are a few features and the number of test cases is large. In the model, as the dataset has linearly separable data, the linear kernel finds the linear margin that separates the two regions in the graph. This decision boundary is chosen such that it is maximally far away from each data point. Fig.3 represents the data that is visualized on the 2-D plot. Fig.4 represents the classification of the dataset by the hyper plane that linearly separates the data.

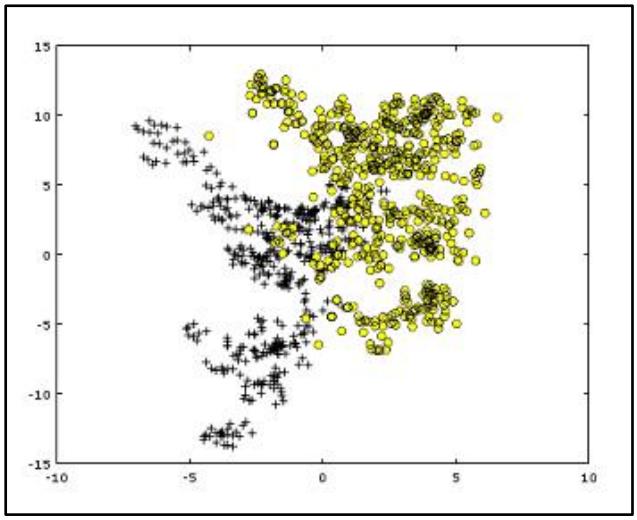

Fig 3: Visualization of SVM

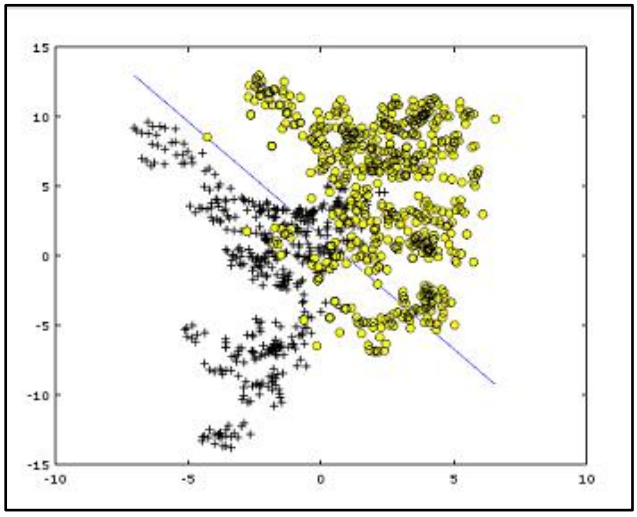

Fig 4: Classification of data by linear decision boundary

6. RESULT AND ANALYSIS

6.1 Performance Measure

Following measures have been used to measure the performance of the models implemented

- Accuracy – The accuracy of the test is its ability to differentiate the genuine and fake note test cases correctly.
  Accuracy =
  $$(TP + TN)/(TP + TN + FP + FN)$$
- Sensitivity - The sensitivity of a test is its ability to determine the genuine note cases correctly.
  Sensitivity =
  $$TP/(TP + FN)$$
- Specificity - The specificity of a test is its ability to determine the fake note cases correctly.
  Specificity =
  $$TN/(TN + FP)$$
- Precision - The precision of a test is its ability to determine the number of notes that classifier labeled as genuine is actually genuine
  Precision =
  $$TP/(TP + FP)$$

Where,

- True Positive (TP) = the number of cases correctly identified as genuine notes.
- True negative (TN) = the number of cases correctly identified as fake notes.
- False positive (FP) = the number of cases incorrectly identified as genuine notes.
- False negative (FN) = the number of cases incorrectly identified as fake notes.

6.2 Comparative Study

Hold-out method is used which divides the dataset into the ratio of 80:20 (training data: test data) and following results have been yielded.

Table 2. Receiver Operating Characteristics

Techniques	TP	TN	FP	FN
BPN	153	122	0	0
SVM	151	121	1	2

Table 3. Comparison Chart (Hold-out method)

Techniques	Accuracy	Specificity	Sensitivity	Precision
BPN	100	100	100	100
SVM	98.90	99.18	98.69	99.34

6.3 Discussion

In the learning phase, the models are trained with 80% data i.e. 1097 samples out of which 609 samples were of genuine notes and 488 were of fake notes. For testing the models, remaining 275 samples have been used, where 153 samples were of genuine notes and 122 samples were of fake notes.

The system evaluates the performance of two models and results have been shown in Table II and Table III. The experiments performed using this dataset as input has resulted in a system providing high recognition rate of banknotes. The goal to get high accuracy of prediction is fulfilled by BPN. As shown in table 3, BPN correctly predicts the genuine and counterfeit notes. At the same time, SVM lacks in predicting the genuine notes and forged notes and gives sensitivity and specificity of 98.69% and 99.18% respectively. These results have been obtained by performing hold-out operation on the data. The results of training and test data do not show much difference except for sensitivity of SVM. The training sensitivity of SVM is 98.68% and the test sensitivity is 98.69%. BPN gives 100% detection rate and SVM gives 98.90% success rate.

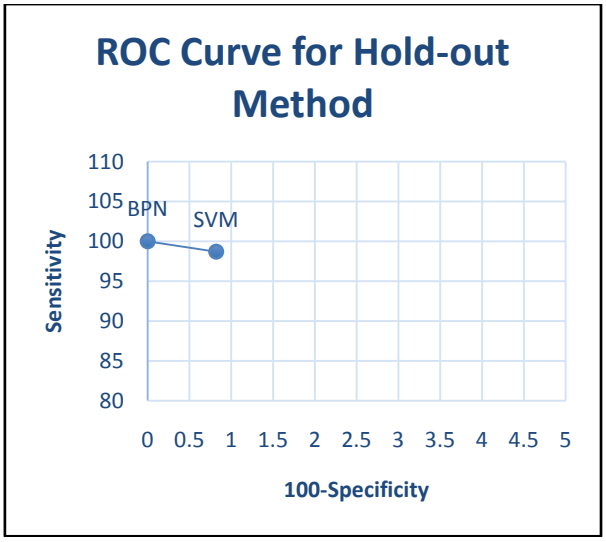

Fig 5: ROC Curve for Hold-out

ROC is graphical plot which is created by plotting Sensitivity against 100-Specificity. ROC graph shows how classifier and threshold choices perform [18]. This curve illustrates the ability of binary classifier system as its discrimination threshold is varied [19].

ROC graph plotted for BPN and SVM suggests that BPN has higher sensitivity and specificity than SVM. Hence, it can be summarized from Table 3 and Fig 5, that BPN yields better result than SVM for recognition of forged notes among the genuine ones.

7. CONCLUSION

After analyzing various techniques used to detect forged banknotes, this paper presents banknote authentication for recognizing the banknote as genuine or fake by using two supervised learning techniques. Extensive experiments have been performed on banknotes dataset using both the models to find the best model suitable for classification of the notes. ROC and other metrics have been calculated to compare the performances of both the techniques. The result shows that back-propagation neural network outperforms support vector machine and gives 100% success rate. These techniques are an efficient way of solving the problem for all banking-machines that accept all types of notes. In future, this work can be extended by categorizing the notes into different categories as Genuine, Low-Quality forgery, High-Quality forgery, Inappropriate ROI.

8. REFERENCES

[1] Chhotu Kumar and Anil Kumar Dudyala, "Banknote Authentication using Decision Tree rules and Machine Learning Techniques", International Conference on Advances in Computer Engineering and Applications(ICACEA), 2015.

[2] Eugen Gillich and Volker Lohweg, "Banknote Authentication", 2014.

[3] Thirunavukkarasu M, Dinakaran K, Satishkumar E.N and Gnanendra S, "Comparison of support vector machine(svm) and Back propagation network (bpn) methods in predicting the protein Virulence factors",Jr. of Industrial Polluction Control 33(2)(2017)pp 11-19.

[4] Zan Huang, Hsinchun Chen, Chia-Jung-Hsu, Wun-Hwa Chen and Soushan Wuc, "Credit rating analysis with support vector machines and neural network: a market comparative study", 2004.

[5] Ming-Chang Lee and Chang To, "Comparison of Support Vector Machine and Back Propagation Neural Network in Evaluating the Enterprise Financial Distress", International Journal of Artificial Intelligence & Applications 1.3 (2010) 31-43.

[6] Prachi Damodhar Shahare and Ram Nivas Giri, "Comparative Analysis of Artificial Neural Network and Support Vector Machine Classification for Breast Cancer Detection", International Research Journal of Engineering and Technology, Dec-2015.

[7] Fumiaki Takeda, Lalita Sakoobunthu and Hironobu Satou, "Thai Banknote Recognition Using Neural Network and Continues Learning by DSP Unit", International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, 2003.

[8] Costas Nastoulis, Apostolos Leros, and Nikolaos Bardis, "Banknote Recognition Based On Probabilistic Neural Network Models", Proceedings of the 10th WSEAS International Conference on SYSTEMS, Vouliagmeni, Athens, Greece, July 10-12, 2006.

[9] Sigeru Omatu, Michifumi Yoshioka and Yoshihisa Kosaka, "Bank Note Classification Using Neural Networks", IEEE, 2007.

[10] Swati V. Walke and Prof. Dr. D. M. Chandwadkar, "Counterfeit Currency Recognition Using SVM With Note to Coin Exchanger", International Journal of Modern Trends in Engineering and Research, July 2015.

[11] Sharmishta Desai, Shraddha Kabade, Apurva Bakshi, Apeksha Gunjal, Meghana Yeole, "Implementation of Multiple Kernel Support Vector Machine for Automatic Recognition and Classification of Counterfeit Notes", International Journal of Scientific & Engineering Research, October-2014.

[12] Masato Aoba, Tetsuo Kikuchi, and Yoshiyasu Takefuji, "Euro Banknote Recognition System Using a Three-layered Perceptron and RBF Networks", IPSJ Transactions on Mathematical Modeling and it's

Applications, May 2003.

[13] https://archive.ics.uci.edu/ml/datasets/banknote+authentication.

[14] https://www.researchgate.net/post/Where_must_we_use_variance_and_mean_of_image.

[15] http://www.itl.nist.gov/div898/handbook/eda/section3/eda35b.htm.

[16] http://www.astro.cornell.edu/research/projects/compression/entropy.html.

[17] Arti Patle and Deepak Singh Chouhan, "SVM Kernel Functions for Classification", ICATE 2013.

[18] Chiara Gigliaranoa, Silvia Figini, Pietro Muliere, "Making classifier performance comparisons when ROC curves intersect", Computational Statistics and Data Analysis 77 (2014) 300–312.

[19] https://en.wikipedia.org/wiki/Receiver_operating_characteristic.

IJCA™ : www.ijcaonline.org