Artificial Intelligence based Bank Cheque Signature Verification System

Vinita Mishra¹, Bhavika Adnani², Hema Lulla³, Priya Vidhrani⁴
¹Mentor, ²³⁴Student VESIT, Mumbai

Abstract: Signatures are one of the feature which distinguishes a person’s identity. But to make it as a conventional method to emerge it with the current trends of technology we will try to automate the signature system in order to make it more reliable and efficient. In this project, we present a simple approach of offline signature verification, where the signature is done on paper and then it will be transferred to an image format by capturing it with camera of mobile phone or tablet. For identifying the signature, we will first do some statistical calculations aiming to extract the features from the signature and then we train the captured signature images using some classification algorithm on these features from different signers. And at last, the extracted features from the tested signature are compared with the previously trained features and we know the identity of the signer.

Keywords: Image Preprocessing, Feature Extraction, Training and Testing, Signature Recognition, Signature Verification.

I. INTRODUCTION
Signatures can be widely used as one of the biometrics which can be used to increase the security. As security has become one of the most important part of our life today. In banks, signatures of a person is one of the factor which is used to check the authenticity of user and whenever the person wants to carry out some transactions the signature is used to verify the identity of the user. Nowadays, verification of signatures are done by staff members of the bank and there is more chance that the signature of a genuine person can be forged by someone else. But this is not a precise way of doing it as forgery cannot be detected easily with naked eye. If forgery is not detected then the possibility is high that the customers will suffer from lot of loss and also it will give a bad impact on bank’s reputation. So, our proposed system will make this process automate and it will be more accurate to test the signatures of a person.

Our system will focus on offline signature verification. where the signature of a person will be captured using camera and then it will used as a image to test with the signatures of users which are previously stored in the database. Classification of signatures are done on the basis of the features extracted from the image of the signature. For this our proposed system comprises of two phases training phase and testing phase. During training phase, preprocessing, feature extraction and classification of signature as genuine or forge is done and then during testing phase we will test the signatures based on the details stored in the database.

II. BASIC OPERATIONS
A. Pre Processing
In this phase, we will do some preprocessing steps to remove the noise from images and make it noise free. We have used RGB to gray to convert the colour images to gray shade so as it can be easier during feature extraction. We have also used resize function which will resize all the images to predefined size it will act as a bounding box for each image. As when we scan and upload the images there is possibility that all the images will not have same size so in that case resize function will do resizing of images.

B. Feature Extraction
After preprocessing next step is to extract the features from the captured image. In this phase all the local pattern features, text features from the image are extracted and later it will help in classification of genuine or forged signatures of a person. From one signature image it will extract 3776 features and then it will stored and shown in a matrix form later it will be used for training.

C. Classification
After the extraction of features are done then we will do classification. Classification is necessary because it is the only step after which we will be able to predict the signature as genuine as forged. Classification is done using SVM classification algorithm we will also set some threshold value which will be used for classification as if the threshold value of testing image is greater then the specified threshold value then it will show that the signature is forged.
III. LITERATURE REVIEW

The issue of signature verification and forgery detection on bank cheques has long been an area of interest in the field of image processing. Many studies have been done till now in order to develop offline signature verification systems. Some already developed system in the problem area are explained below:

Ashwini Pansare, Shalini Bhatia. [6] have used the neural network approach for training the dataset and for feature extraction geometric center algorithm is used. They have performed the feature vector by splitting the signature images as vertical split and horizontal split and for each they are dividing the image into four parts as top, bottom, right and left by doing this for both splits at the end they are getting the feature vector of size 60 is formed using 30 features extracted from vertical and horizontal splitting each. Testing with signature samples from database other than that was in the training phase, out of 300 such signatures (150 genuine and 150 forged) it could recognize 257 signatures correctly. Hence, the correct classification rate of the system is 85.7%

Mujahed Jarhad, Dr. Nijad Al-Najdawi, Dr. Sara Tedmori. [7] have used the supervised neural network approach they have used formal learning method in training and also used the back propagation algorithm and while recognition it gives result as how much percentage of the signature has genuineness in it means that suppose a signature has 74% genuineness and remaining it is forged one. Accuracy of system approximately will be near to 86% as from database of 51 samples it could recognize 44 samples correctly.

Sayantan Roy, Sushila Maheshkar. [8] have used the grid based and centroid based approach and they have also classified the type of forgery as skilled forgery or random forgery. In feature extraction different features are extracted based on global and local parameters and while extracting local features they have used grid based approach and matrix is formed and then using centroid based method this matrix is verified and signature will be classified as genuine or forged and if it is forged then which type of forgery it is. The system gives a FAR of 11-20% and FRR of 7-19%.

IV. PROPOSED SYSTEM

Even today all the transactions especially financial require our signatures to be authenticated. If signatures were not authenticated then it may have severe effect on security. Hence the need for automation for signature recognition and verification has increased in recent years to avoid being vulnerable to fraud effects on transactions.

The proposed system accepts signature as input and classifies it into genuine or forged. The system modeled will verify the signature with maximum accuracy and in minimum time using less computational resources. Signature verification is done using a approach that depends on a SVM classifier which enables the user to recognize whether a signature is original or a fraud. The user upload the scanned images and then add it into the dataset, modifies their quality by preprocessing it which will remove the noise from images and it is followed by feature extraction and SVM classification, and finally verifies the authenticity of the signature

A. Proposed System Design

![Fig. 1 General process in offline signature verification](image-url)
B. Algorithms Used

1) LBP: We will use LBP for extracting the features from signature.
   The LBP uses 4 parameters
   a) Radius: It is used to build outer loop for circular and represent the radius around the circle.
   b) Neighbour: The neighbours are the sample point to build the local binary pattern and more numbers of samples the higher computational cost.
   c) Grid X: The number of cells in horizontal direction.
   d) Grid Y: The number of cells in vertical direction.
   The Local Binary Pattern (LBP) method is used as a texture analysis. First divide the signature image in 16*16 pixel. After that compare the pixel with its 8 neighbours follow the pixels along the clockwise circle. Where the center’s pixel value is greater than the neighbor write “1”, otherwise “0”. This gives an 8 digit binary number and after that it will be converted into decimal format. After this we will compute the histogram of frequency of each number occurring. Now normalize the histogram. After performing the steps this gives the feature vector for signature image.

2) SVM: Support Vector Machine (SVM) is used as a classifying algorithm. It is considered as a linear model for classification.
   This algorithm separates the data into classes according to the specified requirement of application. The features which are extracted in the previous stage using LBP algorithm that feature vector will be divided into classes using Hyperplane. Hyperplane is nothing but a single line which separates the data. Normally we can separate the data by just putting a line but in classification separation should be done in a way that gives the maximized margin between two data points. Our purpose here is to indicate a separate hyperplane which is far from the estimated data. By calculating the perpendicular distance from training data to the separate hyperplanes, so we expect that the optimal solution will have maximum margin. We are using Multi class svm because we have to separate the sample of each user into 5 classes.

V. IMPLEMENTATION AND RESULTS

The signature verification system is primarily used for signature analysis. In order to classify it as genuine or forged we will train and test the signature image for that we have created a database which consists of “30” number of users each of which have 5 samples of genuine signatures. Hence a total no of “150” signatures in database are collected.

The collected signatures have to perform some preprocessing steps which is performed on image captured through camera by doing preprocessing we will convert the images from RGB to Gray, resizing of images, removal of noise etc are done. Now the sample image is ready for training and testing. Extraction of features and classification is done during training phase and then in testing phase we will test the genuineness of each user.

A. Dataset

For analysis of Signature verification system we have used the dataset of signatures. In this we have made 30 classes and 5 images for each user. The images are named as NFI-00201002 which specifies that it is the image of second user but out of five samples it is the first sample of user second.

Number of Classes: 30
Number of Train Images for Each Class: 5
Image Extension: “.jpg”
Total Images: “150”

Fig. 2: Signature images NFI-00101001 to NFI-00105001 for First User

Fig. 3: Signature images NFI-00201002 to NFI-00205002 for Second User
B. Recognition Accuracy

| Class Number | Accuracy Percentage |
|--------------|---------------------|
| 1            | 100                 |
| 2            | 100                 |
| 3            | 100                 |
| 4            | 100                 |
| 5            | 100                 |
| 6            | 100                 |
| 7            | 80                  |
| 8            | 100                 |
| 9            | 100                 |
| 10           | 100                 |
| 11           | 100                 |
| 12           | 100                 |
| 13           | 100                 |
| 14           | 0                   |
| 15           | 100                 |

| Class Number | Accuracy Percentage |
|--------------|---------------------|
| 16           | 60                  |
| 17           | 80                  |
| 18           | 60                  |
| 19           | 100                 |
| 20           | 100                 |
| 21           | 100                 |
| 22           | 80                  |
| 23           | 100                 |
| 24           | 0                   |
| 25           | 100                 |
| 26           | 80                  |
| 27           | 100                 |
| 28           | 100                 |
| 29           | 100                 |
| 30           | 80                  |

VI. CONCLUSION

Signature is one of the most used authentication tool in bank transactions which helps in detecting the exact person and thus preventing any fraudulent activity. In our system, signatures of different users has been studied on for their recognition. LBP method is used for feature extraction and the signature samples for different users are classified using SVM classifier. The results show that algorithm is able to characterise and distinguish the different signature samples. High accuracy is achieved since algorithm is tested on a dataset with low variance in the signature samples. Hence, our system deals with computerized signature verification for banking applications.
REFERENCES

[1] Ashish A. Dongare, Prof. R. D. Ghongade: “Artificial Intelligence Based Bank Cheque Signature Verification System,” International Research Journal of Engineering and Technology (IRJET) Volume: 03, Issue: 01, Jan-2016.

[2] Bence Kovari, Hassan Charaf: “Classification approaches in offline Handwritten Signature verification,” WSEAS Transaction on Mathematics - January 2009.

[3] Esa Prakasa: “Texture Feature Extraction by using Local Binary Pattern,” Article - May 2016.

[4] Ashish Pradhan: “Support Vector Machine: A Survey,” Article - September 2012.

[5] Yujun Yang, Jianping Li, Yimei Yang: “The Research of Fast SVM Classifier Method,” IEEE - 2015.

[6] Ashwini Pansare, Shalini Bhatia: “Off-line Signature Verification Using Neural Network,” International Journal of Scientific & Engineering Research, Volume 3, Issue 2, February-2012.

[7] Jarad Mujahed, Nijad Al-Najdawi, Sara Tedmori: “Offline handwritten Signature verification System using a supervised neural network approach,” Conference Paper - March 2014.

[8] Sayantan Roy, Sushila Maheshkar: “Offline Signature Verification using Grid based and Centroid based approach,” International Journal of Computer Applications(0975-8887) Volume 86 - No 8, January 2014.