Bank Cheque Signature Verification System

Vaibhav Tambade[1], Priyanka Varma[2], Aditya Sonawale[3]

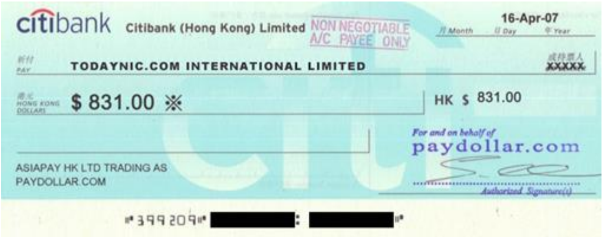
[1,2,3]*Student, Department of Computer Engineering, MGM CET, Navi-Mumbai, India*

***Abstract*—Our Signature Verification System creates a repository of signatures and policy mandates that can be dynamically accessed for the clearing process. This solution supports defining of accounts, mapping of signatories, scanning of mandates, and cropping of signature images. Further, it supports the definition of complex logics based on different amount bands and signatory categories. Using this solution, you can ensure auto-validation of these rules based on the amount and signatories present on the cheque / mandate form. This ensures process compliance, as well as reduced risk in clearing different payment instructions. Thus, you can easily define financial rules, as well as rules for non-financial transactions into the system. Signatures are imperative biometric attributes of humans that have long been used for authorization purposes. Most organizations primarily focus on the visual appearance of the signature for verification purposes. Many documents, such as forms, contracts, bank cheques, and credit card transactions require the signing of a signature. Therefore, it is of upmost importance to be able to recognize signatures accurately, effortlessly, and in a timely manner. In this work, an artificial neural network based on the well-known Back-propagation algorithm is used for recognition and verification. To test the performance of the system, the False Reject Rate, the False Accept Rate, and the Equal Error Rate (EER) are calculated. The system was tested with 400 test signature samples, which include genuine and forged signatures of twenty individuals. The aim of this work is to limit the computer singularity in deciding whether the signature is forged or not, and to allow the signature verification personnel to participate in the deciding process through adding a label which indicates the amount of similarity between the signature which we want to recognize and the original signature. This approach allows judging the signature accuracy, and achieving more effective results.**

***Index Terms*—Feature extraction, Handwriting recognition, Training, Artificial neural networks, Neurons, Classification algorithms**

I. Introduction

Signature is the widely used and accepted form of authentication and it is used even before the usage of computers. Behavioural biometric identifiers, on the other hand, are related to the pattern of behaviour of a person, such as typing rhythm, gait, and voice. Handwritten signatures are used in almost all documents where authentication is required. It has low conflict percentage. The number of bank cheque fraud cases are rising and there are number of modern techniques followed by the fraudulent to counterfeit. Signatures are not easy to verify like that of characters. Verifying signatures in bank cheques is a challenging opportunity in image processing. The amount of the cheque should be mentioned both in words and figures clearly. The amount written in words should tally with the amount written in figures. The drawer should sign the cheque properly. The signature given on the cheque should tally with the signature given on the signature specification car. Image show the signature on cheque.


citibank Citibank (Hong Kong) Limited NON NEGOTIABLE A/C PAYEE ONLY

16-Apr-07
Month Day Year

PAY TODAYNIC.COM INTERNATIONAL LIMITED XXXXX

HONG KONG DOLLARS $ 831.00 ※ HK $ 831.00

ASIAPAY HK LTD TRADING AS
PAYDOLLAR.COM

For and on behalf of
paydollar.com
Authorized Signature(s)

⑈399209⑈ [redacted] : [redacted] ⑈

Fig. 1. Sample cheque

Handwritten signatures can be verified using online or offline schemes. Online signature can be captured using electronic devices like writing pad or stylus attached to a computer. Offline signature will have only the digitized signature from which required features can be extracted. Since this paper deals with signatures on bank cheques, offline signature verification scheme is chosen. A signature which is suspicious is called a forged signature.

Signature of a banker or a customer can be broadly divided into two categories:

1. *Initials*

This is the short form of signature wherein the signatory put son his signature in a very short form. These initials are not accepted for wide range of transactions by bankers. These are used for intra official transactions and on cop-ies of instruments. Normally, institutions do not retain these signatures as a specimen.

2. *Full signature*

These are the signatures widely used in banking transactions and are retained as a specimen signature by the banker. Bank officials verify the signatures appearing in the instruments against these specimen signatures. In the cases of corporate or institutional customers, company seal or stamp is also retained as a part of signature.

II. Approach

We approach the problem in two steps. Initially a set of signatures are obtained from the subject and fed to the system. These signatures and pre-processed Then the pre-processed images are used to extract relevant geometric parameters that can distinguish signatures of different persons. These are used to train the system. The mean value of these features is obtained. In the next step the scanned signature image to be verified is fed to the system. It is pre-processed to be suitable for extracting features. It is fed to the system and various features are extracted from them. These values are then compared with the mean features that were used to train the system. The Euclidian distance is calculated and a suitable threshold per user is chosen. Depending on whether the input signature satisfies the threshold condition the system either accepts or rejects the signature.

Section 3 deals types of signatures and Section 4 explains signatures verification model and steps to involve that are extracted followed by the verification procedure by Neural Network in Section 5. Features use of signature verification system listed in Section 6. The conclusion and references are follows in last section.

III. Types of Verification

A. *Online/ Dynamic Signature*

Online or Dynamic signature publish in early in 1990's. It can be consider only Uses shape, speed and pressure. In online signature system needs special digital surface, pads and pen etc. It's required some numeric data and small amount of storage. It can use speed, pressure, angle of pen to further exploit individuality. In online signature it's hard to easier to forge. Accuracy of signature verification on offline method is around 99%.

B. *Off-Line/Static Signature*

Offline or Static signature publish in early in 1970's. It can be consider only image signature. In offline signature system no need to use special hardware, ubiquitous etc. It's required large amount of storage. It cannot be trace speed, style, pressure etc. In offline signature it's easy to easier to forge. Accuracy of signature verification on offline method is around 95%.

IV. Algorithm Models and Steps

A. *Algorithm of Signature Verification*

Step 1: Hand written signature is scan using camera or scanner.
Step 2: Signature is pre-processing and converted into binary or grey scale as per requirement, Removing noise from signatures and finally normalize the signatures.
Step 3: Special domain feature as high intensity variation points and cross over points extract from test signatures.
Step 4: Compared features with help of graph matching methods as a classifier.

B. *Model of Verification*

The Fig. 2. Shows the signature verification model

C. *Steps Involved In Signature Verification*

1) *Data acquisition*

Data acquisition actually means giving data to the system. In this system the data is provided to the system in the form of a scanned image. The signature is scanned and stored as a digital image.

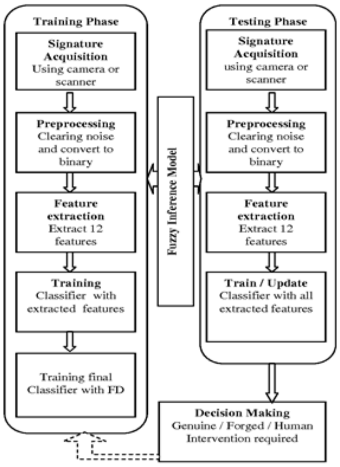

Training Phase
Signature Acquisition Using camera or scanner
Preprocessing Clearing noise and convert to binary
Feature extraction Extract 12 features
Training Classifier with extracted features
Training final Classifier with FD
Fuzzy Inference Model
Testing Phase
Signature Acquisition using camera or scanner
Preprocessing Clearing noise and convert to binary
Feature extraction Extract 12 features
Train / Update Classifier with all extracted features
Decision Making Genuine / Forged / Human Intervention required

Fig. 2. Signature model verification

2) *Pre-processing*

Data preprocessing describes any type of processing performed on raw data to prepare it for another processing procedure. There are 4 steps to use to pre-processing steps and steps of pre-processing are followed.

a) *Image Conversion:* The first step is to convert the obtained RGB image into gray scale image. This is done to reduce the complexity and the execution time of the system. It is easy for the system to work with grayscale images rather than the RGB images.

b) *Image Cropping:* Then a cropping algorithm is applied to the grayscale image. Cropping is done to separate out precisely the actual region of interest from the complete image. This removes the extra pixels from the image thus reducing the processing time.

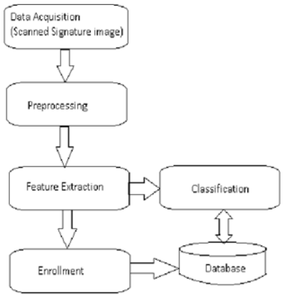


Fig. 3. Basic signature verification system

c) *Image Filtering:* After obtaining the cropped image the noise that entered while scanning or via any other source has to be removed. For this a Gaussian filter along with the unsharp filter is used. The Gaussian filters smooth the image removing the noise and the unsharp filter removes the blur created by the Gaussian filter.

d) *Thresholding:* This filtered image is then threshold to convert it into a binary form. Finally the boundary of the signature is extracted from this binary image using the canny edge detector.

3) *Feature extraction*

In pattern recognition and in image processing, feature extraction is a special form of dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be notoriously redundant then the input data is transformed into a reduced representation set of features. Transforming the input data into the set of features is called feature extraction.

The main function of this step is to generate features which can be used as comparison measurements. Since the issue of signature verification is a highly sensitive process, more than one feature has to be generated in order to enhance the accuracy of the result.

4) *Classification*

Image classification analyzes the numerical properties of various image features and organizes data into categories. Classification algorithms typically employ two phases of processing: training and testing as show in signature verification model. In the initial training phase, characteristic properties of typical image features are isolated and, based on these, a unique description of each classification category, i.e. training class, is created. In the subsequent testing phase, these feature-space partitions are used to classify image features.

5) *Signature verification using neural network*

In a neural network, you have a set of inputs, which results in an output. Between the input and the output are multiple layers of artificial neurons. These neurons take the input, and a weight inside them works out if it triggers or not. This is then passed to the next layer which does likewise. The more complex your problem the more layer and artificial neurons you might need

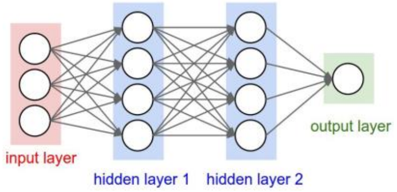


Fig. 4. Neural network diagram

The whole thing works as a multilayered transformational matrix. What happens is you feed through training data, the system compares the output it gets with the expected output. It then applies feedback which adjusts the weighted trigger levels of some of the neurons. Then it tries again with another piece of data, and makes an adjustment. It keeps doing this, repeating cycles of data and adjusting the trigger levels, and hopefully getting closer to a repeatable pattern.

V. Features Used

1. Total time
2. Signature path length
3. Path tangent angles
4. Signature velocity
5. Signature accelerations
6. Pen-up times & durations
7. [Crane83] proposed 44 while [Parks85] proposed 90 features [Lee96] used 15 static & 34 dynamic
    a. None related to shape
    b. 1% FRR, 20% FAR on timed forgeries

VI. Conclusion

- The new system should be an on-line system
- Shape is an integral part of signature verification, it is a metric that is most easily imitated by a forger
- Both global & local features should be used
- Different methods have been tried with varying results, About 99% at the best
- Great deal of speed improvement to be done
- Signature segmentation into individual strokes needs attention
- Multi-expert system to integrate different methods
- Analysis on proper setting of thresholds & use of user-specific thresholds
- Sensors have developed to a fair point of saturation
- Study on multi-lingual signatures is unfocused

References

[1] S. Chen, and S. Srihari, “Use of Exterior Contour and Shape Features in Off-line Signature Verification”, 8th International Conference on Document Analysis and Recognition (ICDAR ’05), 2005, pp. 1280-1284

[2] Fernando Alonso-Fernandez, Julian Fierrez, Almudena Gilperez, Javier Galbally, Javier Ortega-Garcia, Robustness of Signature Verification Systems to Imitators With Increasing skills, IEEE 2009,pp. 728-732.

[3] Vibha Pandey, Sanjivani Shantaiya. “ Signature Verification Using Morphological Features Based on Artificial Neural Network”, 2012 pp. 288-292

[4] Bradley Schafer, Serestina Viriri, An Off-Line Signature Verification System, IEEE International Conference on Signal and Image Processing Applications, 2009, pp. 95-100

[5] Daramola Samuel and Prof.Ibiyemi Samuel, Novel feature extraction technique for off-line signature verification system, IJEST, Vol ED-2(7), 2010.

[6] Imran Hussain, Vikash Shrivastava, Vivek Kr. Shrivastava, Review On Offline Signature Verification Methods Based On Artificial Intelligence Technique, IJOART, Volume 2, Issue 5, May-2013.