

# Online Signature Recognition Using Matlab

P.R.Shahane<sup>1</sup>, A.S.Choukade<sup>2</sup>, A.N.Diyewar<sup>3</sup>

Professor, Department, of E&TC, Sinhgad Academy Of Engineering, Pune, India <sup>1</sup>

Student, Department of E&TC, Sinhgad Academy Of Engineering, Pune, India <sup>2,3</sup>

**Abstract:** Signature is a behavioral trait of an individual and forms a special class of handwriting in which legible letters or words may not be exhibited. The purpose of this paper is to design a new system to make the verification of signatures size and angle invariant for cheque system. The invariance can be achieved by scaling and rotational manipulations on the target image. That is the number of crests, troughs and curves remains the same irrespective of the size and orientation of the image. The ratio between consecutive crests and troughs there by remain the same and hence can be used to determine the genuineness of a signature. This system will be used in financial and business to automatic signature verification. It also includes the verification of the account number and amount on the cheque using OCR (Optical Character Recognition) and finds out if the cheque is cleared or bounced.

**Keywords:** image processing, OCR; Feature extraction, Segmentation, Dilation, Thinning.

## I. INTRODUCTION

Signature verification is an important research area in the field of person authentication [1]. A signature is treated as an image carrying a certain pattern of pixels that pertains to a specific individual. Signature verification problem is concerned with examining and determining whether a particular signature truly belongs to a person or not. Signatures are a special case of handwriting in which special characters and flourishes are viable. Signature verification is a different pattern recognition problem as no two genuine signatures of a person are precisely the same. The difficulty also stems from the fact that the skilled forgeries follow the genuine pattern unlike fingerprints which vary widely for two different persons. Ideally, interpersonal variation should be much more than intrapersonal variation. Therefore, it is important to identify those features that minimize the intrapersonal variation and maximize interpersonal variation. The key factor is to differentiate between the parts of the signature that are habitual and those that vary with almost every signature. There are two approaches used for signature verification according to the acquisition of the data as offline and online signature verification system. In offline verification system, only static features are considered, whereas in case of online systems, dynamic features are taken into consideration. Offline signature recognition [2] is performed after the writing is complete. The data is captured at a later time by using an optical scanner to convert the image into a bit pattern.

Online signature recognition, in contrast, means that the machine recognizes the handwriting as the user writes. It requires a transducer that captures the signature as it is written and hence the features are dynamic in nature. Offline data is a 2-D image of the signature. Processing Offline is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. The nature and the variety of the writing pen may also affect the nature of the signature obtained. The non-repetitive nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of

the person, accentuates the problem. All these coupled together cause large intra-personal variation.

A robust system has to be designed which should not only be able to consider these factors but also detect various types of forgeries. The system should neither be too sensitive nor too coarse. It should have an acceptable trade-off between a low False Acceptance Rate (FAR) and a low False Rejection Rate (FRR). The designed system should also find an optimal storage and comparison solution for the extracted feature

## II. LITERATURE SURVEY

In the daily banking system approximately 10% -15% of daily clearing items need the signatures to be verified for the reasons such as a technical fault or the cheque above the floor limit etc. This often involves returning the cheques to the branches where the signature mandates are held, which is a time consuming and costly process. Initially all paper and electronic information were not accurate and there are still chances of forgery. Even now there are very few software's which verifies the signature automatically but, are rarely used in public domain.

A survey of the literature on automatic signature verification, writer identification by computer, an overview of achievements in static and dynamic approaches to solving these problems, with a special focus on pre-processing techniques, feature extraction methods, comparison processes and performance evaluation have been conducted. In addition, for each type of approach special attention is given to requirement analysis, human factors, practical application environments, and appropriate definitions and terminology. There are many techniques present to extract the signature outline as follows-

### A. Fixed Point Arithmetic method

This technique is based on geometrical features which are based on two vectors which represent the envelope description and the interior stroke distribution in polar and Cartesian coordinates [12].

### B. Outline Detection and Representation

The outline is calculated by means of morphological operations [11]. First, the dilation is applied in order to reduce the signature variability and, afterward, a filling operation is applied to simplify the outline extraction process.

When several objects are detected a horizontal dilatation is performed until all the objects are connected.

### C. Feature Vector Based on Polar Coordinates

To represent the signature outline in the polar coordinates [3], it is decimate selecting  $Tr$  equidistant samples of the envelope  $(X_{tp}, Y_{tp})_{t=1}^{Tr}$  (being  $p = \text{fix}(T/Tr)$  and  $\text{fix}$  rounds to the nearest integers toward zero) and represent each sample as a three components feature vector such are the derivation of the radius, angle and the number of black pixel that the radiuses cross when sweeping from one selected point to the next. The latter components have been obtained with an algorithm designed for fixed-point microprocessor.

### D. Feature Vector Based on Cartesian Coordinates

The second feature vector is also based on the envelope and the signature strokes density parameterization [3] but, in this case, in Cartesian coordinates, the envelope is divided through the geometric centre into top and bottom halves.

There are many drawbacks in the previous systems. So, there is a need of a reliable signature verification system that can be used in many applications like cheque's, certificates & contracts etc. The proposed system must fulfils the following requirements as –

1. It provides secure means for authentication, attestation and authorization in legal, banking or other high security environments.
2. Signature verification problem pertains to determine where a particular signature verily written by a person so that forgery can be detected.
3. A full proof signature verification scheme which can guarantee maximum possible security from fake signature.

## III. SYSTEM ARCHITECTURE

The present work is focus on the design and implementation of automated signature verification and cheque processing system to ensure better performance than already established offline signature verification scheme to reduces manual work, saves time, avoids chances of forgery & works efficiently as shown in fig. 1. The training images are obtained using the scanner. The pre-processing operation is applied on these images. The result of pre-processing is a gray scale image which is then used for feature extraction. Features are then extracted by applying different techniques. The account number and amount verification module is used for verifying the account number and amount using the OCR technique. After this verification process the results are generated to decide whether cheque is cleared or bounced.

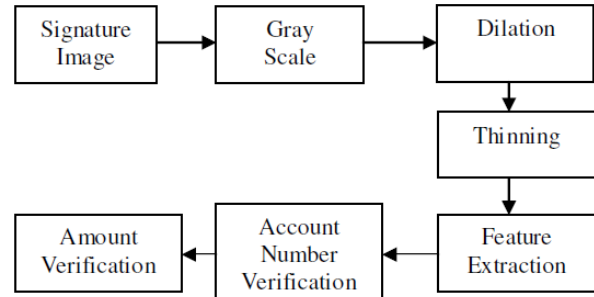


Fig. 1 System Architecture

The design and development of this system is divided into following modules as –

#### A. Signature verification Module –

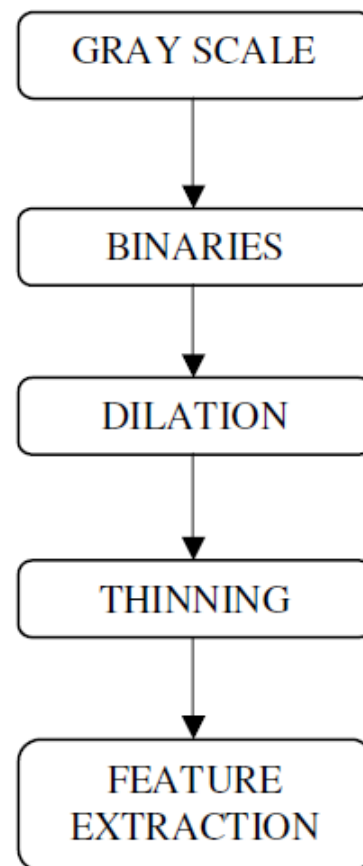


Fig.2 Signature Verification Process

This module is used to avoid forgery & prevents from unauthorized users. In this module the cheque is first scanned using the scanner, the original training set will be used and preprocessed to get suitable for extracting features as shown in fig.

#### 2. It contains following operations as –

##### 1) Database Management-

This handles the various aspects of database management like creation, modification, deletion and training for a signature instance. Data acquisition of the static features is carried out using high resolution scanners. The information regarding a particular signature is stored in database as a feature vector where the entire static features are stored against the account number.

2) *Gray Scale conversion:*

Comparing and verifying an image having multiple color strains is pretty complex. So, the gray scale format of scanned image is obtained by using predefined functions of image processing.

3) *Binaries:*

In this a uniform image pattern is created in which all shades from black to gray are colored black and the rest area colored white. There are 256 gray levels of a gray scale image. Here there is a need of binary image having only black and white values. To do so any threshold value has been taken depending on our capturing device. Lower values of threshold for a good image recorder and high if lighter images are obtained by the scanner. The first step in given approach is to convert the acquisitioned signature to binary form, i.e. black and white pixels. Working in this form is more useful than any other form, since it is easy to work with 2 bits representation of image.

Coloured image (2D)				Binary image			
	296	297	298		296	297	298
26	240	253	255	26	1	1	1
27	255	255	255	27	1	1	1
28	249	252	252	28	1	1	1
29	250	255	253	29	1	1	1
30	255	254	253	30	1	1	1
31	249	250	252	31	1	1	1
32	255	252	254	32	1	1	1
33	255	253	254	33	1	1	1
34	249	253	254	34	1	1	1

Fig. 2 colored Vs binary image matrixes.

The required time to process colored image is longer than binary one, as example applying radon transform on different types of image (colored Vs binary) shows the following deference's.

Table 1: processing time comparison

Type	Coloured(3D)	Gray scale(2D)	Binary
Time	6.2340	2.3440	2.0780

4) *Rotation of image:*

The image rotation has been applied such that maximum feature points are made horizontal. By doing so, many white pixels are obtained in the rotated image which should actually be black. So, the obtained image should be treated before it is processed further.

5) *Dilation:*

The rotated image has certain pixels overlapped and lost due to rounding problems. Also the rotation brings about abnormality in the image texture. So, the dilation is required for rotated image to restore normality. The Dilation has been performed by considering the steps mentioned in [11]. Dilation makes the image continuous.

6) *Thinning:*

The fast and efficient parallel thinning algorithm has been applied to get clear and correct image mentioned in [4].

7) *Determination of the crests and troughs:*

The crests and troughs are calculated from a signature pattern, use them as the feature points and calculate the distance between them.

8) *Obtaining the required lengths:*

According to the new system there is need to find the distances between consecutive crests and troughs. To find

the order in which they occur, arrange them in ascending order of their corresponding column values. For those values in which same column value is present, take their row values to arrange them in ascending order. After this, the distance between the consecutive points has been obtained and uses it to divide all the distance values to obtain the normalized values with maximum value as 1. The standard deviation between of these lengths is obtained and two signatures are said to be matched if the variance lies within some threshold value, called the threshold variance. Or else it is declared as fake image.

9) *Sobel operator:*

The Sobel operator is used in image processing, particularly within edge detection algorithms [9]. In simple terms, the operator calculates the gradient of the image intensity at each point, giving the direction of the largest possible increase from light to dark and the rate of change in that direction.

10) *Feature extraction and parameter calculation:*

This is used for extracting various features from the preprocessed image.

B. *Account Number Verification module –*

In this module the unique account numbers has been checked for all cheques.

C. *Amount Verification module –*

In this module the amount is verified so that the amount to be withdrawn should be less than the amount deposited. The amount is verified using OCR technique.

1) *OCR technique:*

Optical Character Recognition is a process in which the conversion has been carried out from printed document or scanned page to ASCII character. The document image itself can be either machine printed or handwritten, or the combination of two. Recognition of printed characters is itself a challenging problem since there is a variation of the same character due to change of fonts or introduction of different types of noises. Difference in font and sizes makes recognition task difficult. Therefore a good character recognition approach must eliminate the noise. After reading binary image data, smooth the image for better recognition, extract features efficiently, train the system and classify patterns as shown in fig. 3.

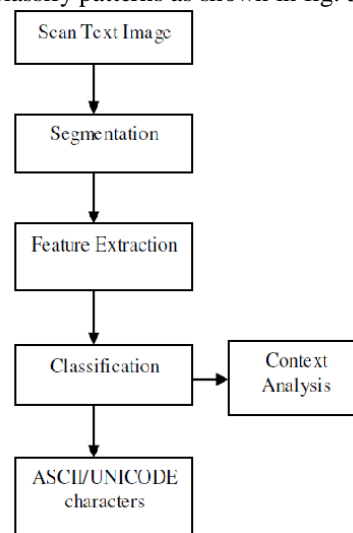


Fig. 3 OCR steps

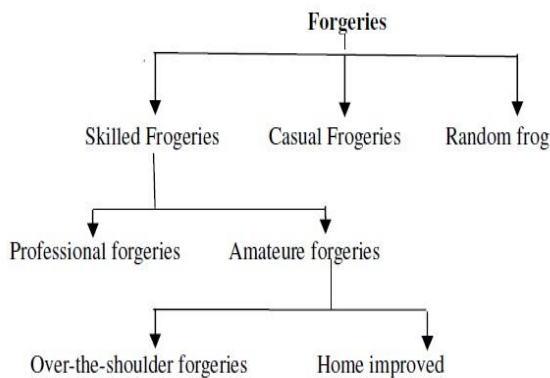
#### IV. FORGERIES

Automatic examinations of questioned signatures were introduced in the late 1960s with the advent of computers. As computer systems became more powerful and more affordable designing an automatic forgery detection system became an active research subject. Most of the work in off-line forgery detection, however, has been on random or simple forgeries and less on skilled or simulated forgeries. Before looking into the landmark contributions in the area of forgery detection, we first enumerate the types of forgeries. Verification is the decision about whether the signature is genuine or forged. Forged images can be classified into three groups there are three kinds of forgeries –Skilled Random and Casual. Shown below is a self explanatory image of the various kinds of forgeries:

**Random Images:** Are formed without any knowledge of the signer's name or signature shape.

**Simple Images:** Produce by people knowing the name of the signer's but without any example of the signature.

**Skilled Images:** Are produce by people looking at the original signature image and try to imitate it as closely as possible.



#### Forgeries

Skilled Forgeries Casual Forgeries Random frog Professional forgeries Amateur forgeries Over-the-shoulder forgeries Home improved Various kinds of forgeries are classified into the following types:

#### Random Forgery

The signer uses the name of the victim in his own style to create a forgery known as the simple forgery or random forgery.

This forgery accounts for the majority of the forgery cases although they are very easy to detect even by the naked eye

#### Unskilled Forgery

The signer imitates the signature in his own style without any knowledge of the spelling and does not have any prior experience. The imitation is preceded by observing the signature closely for awhile.

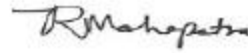
#### Skilled Forgery

Undoubtedly the most difficult of all forgeries is created by professional impostors or persons who have experience in copying the signature. For achieving this one could either trace or imitate the signature by hard way. Figure shows the different types of forgeries and how much they are varies from original signature.

#### Signature Verification & Recognition -

##### 1) Types of Forgery

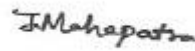
###### a) original signature:



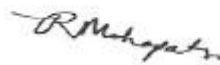
###### b) Random forgery:



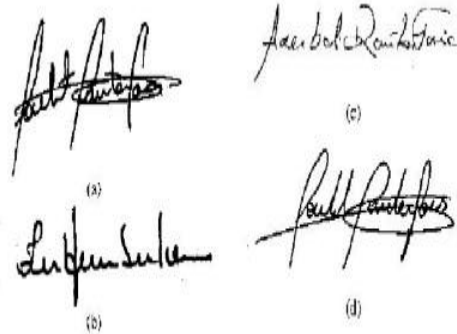
###### c) Simple forgery:



###### d) Skilled Forgery:



##### 2) Types of forgery



(a) Genuine Signature; (b) Random Forgery; (c) Simulated Simple Forgery; (d) Simulated Skilled Forgery

#### About Forgeries:

Initially a set of signatures are obtained from the subject and fed to the system. These signatures and preprocessed Then the preprocessed 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 preprocessed 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. Handwritten signature verification is the process of confirming the identity of a user sing the handwritten signature of the user as a form of behavioral biometrics [1][2]. Automatic handwritten signature verification has been studied for decades. Many early research attempts were reviewed in the survey papers

[3]. The main advantage that signature verification has over other forms of biometric technologies, such as fingerprints or voice verification, is that handwritten signature is already the most widely accepted biometric for identity verification in society for years. The long history of trust of signature verification means that people are very willing to accept a signature-based biometric authentication system [4].

### 2.3 Various types of signature detect action:

There are two approaches used for signature verification according to the acquisition of the data as:

- Offline signature verification system
- Online signature verification system

#### Offline signature verification system

In offline verification system, only static features are considered, whereas in case of online systems, dynamic features are taken into consideration. Offline signature recognition is performed after the writing is complete. The data is captured at a later time by using an optical scanner to convert the image into a bit pattern. As compared to on-line signature verification systems, off-line systems are difficult to design as many desirable characteristics such as the order of strokes, the velocity and other dynamic information are not available in the off-line case. The verification process has to fully rely on the features that can be extracted from the trace of the static signature image only. Although difficult to design, off-line signature verification is crucial for determining the writer identification as most of the financial transactions in present times are still carried out on paper. Therefore, it becomes all the more essential to verify a signature for its authenticity. The design of any signature verification system generally requires the solution of five sub-problems: data acquisition, pre-processing, feature extraction, comparison process and performance evaluation. Off-line verification just deals with signature images acquired by a scanner or a digital camera. In an off-line signature verification system, a signature is acquired as an image.

This image represents a personal style of human handwriting, extensively described by the graphometry. In such a system the objective is to detect different types of forgeries, which are related to intra and inter-personal variability. The system applied should be able to overlook inter-personal variability and mark these as original and should be able to detect intra-personal variability and mark them as forgeries. In off-line signature recognition we are having the signature template coming from an imaging device, hence we have only static characteristic of the signatures. The person need not be present at the time of verification. Hence off-line signature verification is convenient in various situations like document verification, banking transactions etc. As we have a limited set of features for verification purpose, off-line signature recognition systems need to be designed very

carefully to achieve the desired accuracy. The difference between the off-line and on-line lies in how data are obtained. In the on-line SRVS data are obtained using special peripheral device, while in the off-line SRVS images on the signature written on a paper are obtained using scanner or a camera [2]. In this research, an approach for off-line signature recognition and verification is proposed. The designed system consist of three stages: the first stage is pre-processing stage which applied some operations and filters to improve and enhance signature image.

The purpose of the preprocessing stage is to determine the best signature image for the next stage which is feature extraction stage, choosing the right feature is an art more than a science. Three powerful features are used: global feature, texture feature and grid information feature [3]. The three features are calculated for each signature image and enter to the last stage which is neural network stage. Neural network consist of two-stage classifiers: the first classifier stage contain three back propagation (BP) neural networks, each one of the three BP takes its input from one of the three features and trained individually of each other.

Each BP have two outputs that enter as an input to the second stage classifier. The second stage classifier consists of two radial basis function (RBF) neural networks. It is the task of the second classifier (RBF) to combine the result of the first classifier (BP) to make the final decision of the system [4]. Offline verification is concerned with the verification of a signature made by a normal pen. Various different approaches to both classes have been proposed.

## V. IMPLEMENTATION

The implementation has been done using Matlab language on windows platform. Fig. 4 shows are self-contained.

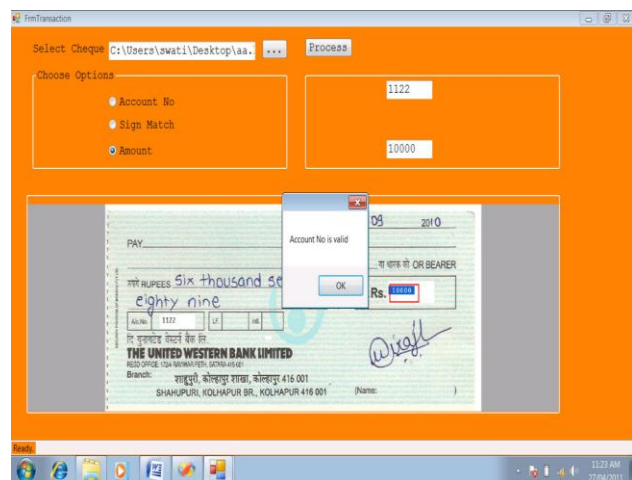


FIG.4 GUI OF THE SYSTEM

The table 1 shows the variance of FAR and FRR with the threshold variance.

TABLE 1  
Variation of FAR and FRR with the threshold Variance

S r N o	Thres hold Varia nce	No of genuine signatures rejected (out of 70)	FRR (False Rejecti on Rate)	No of fake signatures accepted (out of 70)	FAR (False accepta nce Rate)
1	0.15	10	14.2%	25	35.7%
2	0.10	13	18.6%	15	20%
3	0.08	23	33.3%	10	14.2%
4	0.06	34	48.5%	5	7.1%

## VI. CONCLUSION

A reliable signature verification system is an important part of law enforcement, security control and many business processes. It can be used in many applications like cheques, certificates, contracts etc. The integrated signature verification system incorporates database management, noise removal and pre-processing, feature extraction, learning and verification modules. The matching is done and decision making is based on threshold based technique that gives near applications. The system showed promising results. Different threshold values are used for matching depending on testing and training features vectors, thereby boosting the overall performance of the system. This work is used to scans the cheque & tell whether the cheque is bounced or cleared. It verifies the account no from database & then verifies signature from masters & puts the output of matching in percentage. After that the amount is deposited or withdrawn from the respective account.

## REFERENCES

- [1] Kishor T. Mane, Vandana G. Pujari, Signature Matching with Automated Cheque System. 7/2014 International Conference on Intelligent Systems and Signal Processing (ISSP).
- [2] Migual A. Ferrer, Jesus B. Alonso and Carlos M. Travieso, "Off-line Geometric Parameters for Automatic Signature Verification Using Fixed- Point Arithmetic", IEEE Tran. on Pattern Analysis and Machine Intelligence, vol.27, no.6, June 2013.
- [3] Debasish Jena, Banshidhar Majhi, Saroj Kumar Panigrahy, Sanjay Kumar Jena "Improved Offline Signature Verification Scheme Using Feature Point Extraction Method".
- [4] T.Y.Zhang, C.Y. Ceun "A fast algorithm for Thinning Digital Patterns". Communications of ACM, March 2011 Concepts of Image Processing.
- [5] S. Mori et. al, "Historical Review of OCR Research and Development", Proceeding IEEE, 80, no 7, pp. 1029-1058, July .
- [6] A. A. Chaudhary, E.A.S. Ahmad, S. Hossain, C. M. Rahman, "OCR of Bangla Character Using Neural Network: A better Approach", 2<sup>nd</sup> International Conference on Electrical Engineering (ICEE 2010), khuln, Bangladesh.
- [7] Utpal Garain and Bidyut B. Chaudhary, "Segmentation of Touching Character in Printed Devnagari and Bangla Script Using Fuzzy Multi factorial Analysis", IEEE Transaction on System, Man and Cybernetics- Part C: Applications and Reviews, 32, November 2002. Page(s): 449- 459.
- [8] B. B. Chaudhary and U. Pal, "OCR Error Detection and Correction of an Inflectional Indian Language Script", Pattern Recognition 1996, IEEE Proceeding of 13 th International Conference on 25-29 Aug., 3, 1996 page(s): 245-249.
- [9] [en.wikipedia.org/wiki/Sobel\\_operator](http://en.wikipedia.org/wiki/Sobel_operator)
- [10] <http://www.regentsprep.org/Regents/math/geometry/GT3/Ldilate2.htm>
- [11] [www.cs.utexas.edu/~grauman/courses/378/slides/lecture14\\_full.pdf](http://www.cs.utexas.edu/~grauman/courses/378/slides/lecture14_full.pdf)
- [12] <http://darcy.rsgc.on.ca/ACES/ICE4M/FixedPoint/FixedPointRepresentationFractionalMath.pdf>.