SASI INSTITUTE OF TECHNOLOGY & ENGINEERING
(Approved by AICTE-New Delhi, Affiliated to JNTUK-Kakinada and SBTET-Hyderabad)
TADEPALLIGUDEM - 534101, West Godavari District, Andhra Pradesh
☎ : 08818-244986,987,989,990 Fax:08818-244628 Web : www.sasi.ac.in., hodece@sasi.ac.in
Department of Electronics & Communication Engineering

Academic Year 2016-17

Annexure I

1. Project Title: Authentication of Signature using Scale Invariant Feature Transform (SIFT)

TABLE OF CONTENTS

1. Abstract & Objective

1.1 Abstract

Signature is a particular pattern used by human beings for their personal identification. Till now signature on cheques are authenticated manually, but sometimes forgery cheques are overlooked due to some human errors which results in loss of money. So the signature authentication system is designed using image processing techniques. The signature is acquired through a camera and it is compared with original signature in database of banks.

For each known writer we took a sample of three genuine signatures and extracted their key points using "Scale Invariant Feature Transform" (SIFT) algorithm and then calculated the

Euclidean distances among SIFT key points of this known signatures. Various distance thresholds like the maximum, average, minimum values are evaluated. For each signature claimed to be of the known writers, key points are extracted and the Euclidean distances between each of it's SIFT key points are calculated and compared with that of genuine samples.

HSV (Handwritten Signature Verification) systems are used for forgery detection as till now signature on cheques are authenticated manually, but sometimes forgery cheques are over-looked due to some human errors which results in loss of money. The objective of signature verification systems is to differentiate between original and forged signature, which are related to intra-personal and inter-personal variability. Intra-personal variation is variation among the signatures of the same person and inter-personal is the variation between the originals and the forgeries.

Signature recognition technology has some advantages such as sufficient dynamic information, difficult imitation, higher discrimination, and efficient access to information, and the characteristics of the collecting features, body injury acceptability and robustness are very outstanding. Improving signature recognition quality and speed has important theoretical value and practical significance in information processing, artificial intelligence.

Distinction between signature recognition and signature verification is made. Verification decides whether a claim that a particular signature belong to a specific class (writer) is true or false whereas recognition decides to which of a certain number of classes (writers) a particular signature belongs.

1.2 Motivation

Paper cheques still play a big role in the non-cash transactions in the world even after the arrival of credit cards, debit cards and other electronic means of payment. In many developing countries, the present cheque processing procedure requires a bank employee to read and manually enter the information present on a cheque (or its image) and also verify the entries like signature and date. As a large number of cheques have to be processed every day in a bank, an automatic reading system can save much of the work. Even with the success achieved in character recognition over the last few decades, the recognition of handwritten information and the verification of signatures present on bank cheques still remain a challenging problem in document image analysis.

1.3 Objective

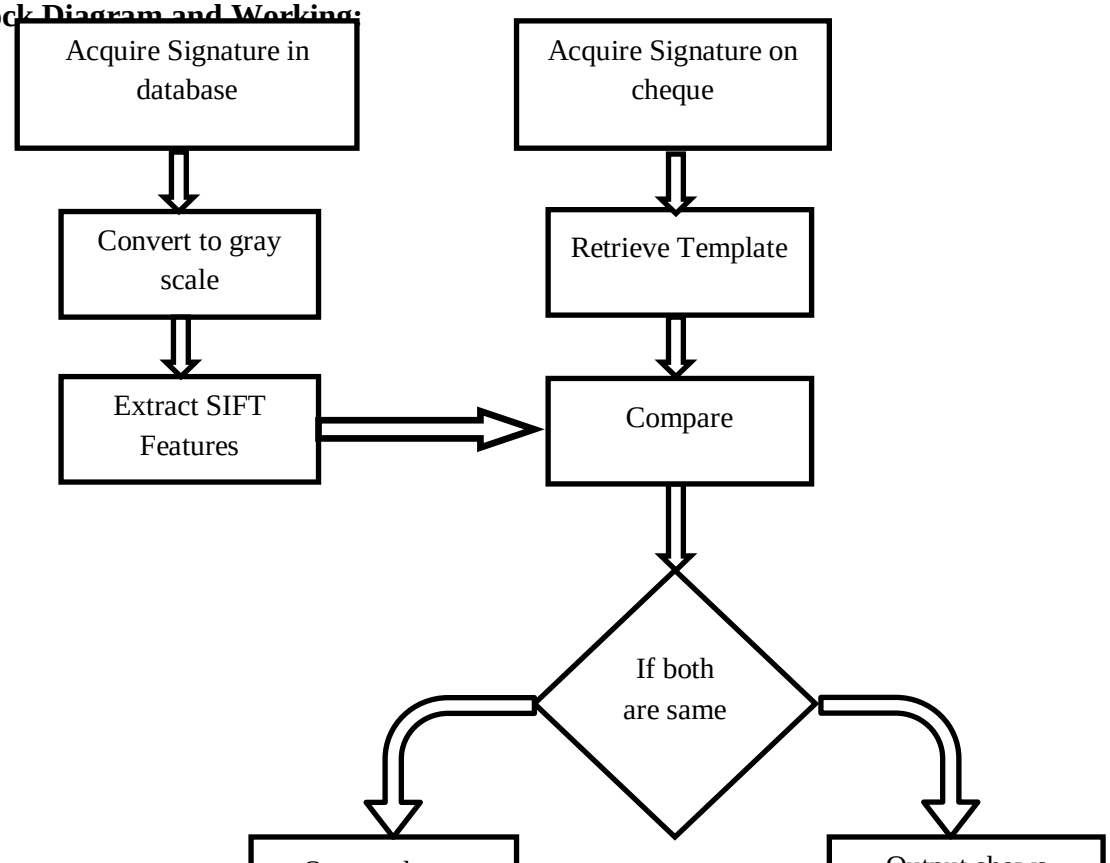
HSV (Handwritten Signature Verification) systems are used for forgery detection as till now signature on cheques are authenticated manually, but sometimes forgery cheques are over-looked due to some human errors which results in loss of money. The objective of signature verification systems is to differentiate between original and forged signature, which are related to intra-personal and inter-personal variability. Intra-personal variation is variation among the signatures of the same person and inter-personal is the variation between the originals and the forgeries.

Signature recognition technology has some advantages such as sufficient dynamic information, difficult imitation, higher discrimination, and efficient access to information, and the characteristics of the collecting features, body injury acceptability and robustness are very outstanding. Improving signature recognition quality and speed has important theoretical value and practical significance in information processing, artificial intelligence.

Distinction between signature recognition and signature verification is made. Verification decides whether a claim that a particular signature belong to a specific class (writer) is true or false whereas recognition decides to which of a certain number of classes (writers) a particular signature belongs.

2. Block Diagram & Technical Specifications

2.1 Block Diagram and Working:



2.2 Signature Enrolment:

Signature enrolment involved preparation of signatures, extraction of SIFT features and registration of signatures images and their SIFT features in the system.

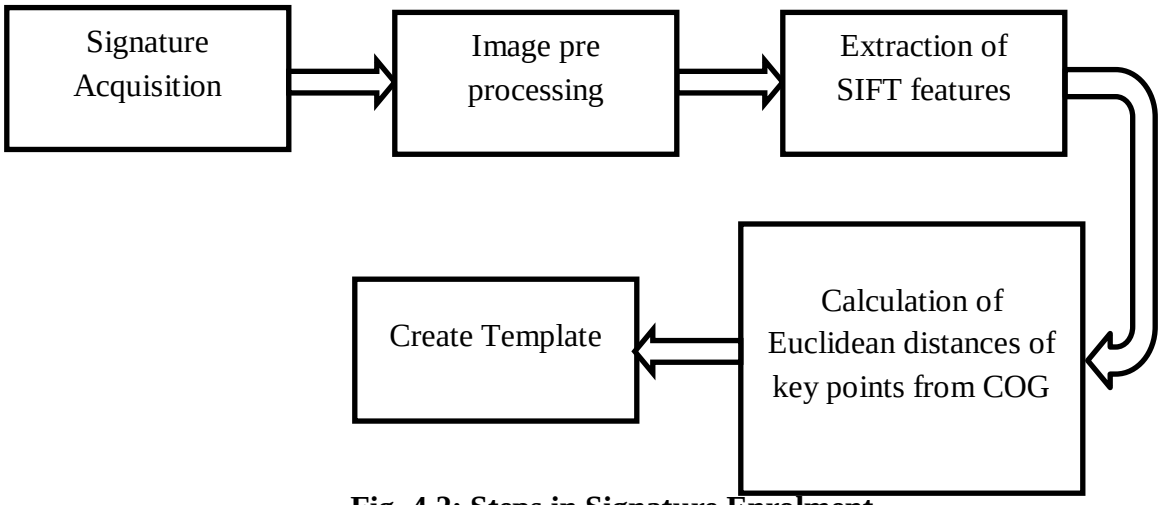


Fig .4.2: Steps in Signature Enrolment.

2.2.1 Image Pre-Processing:

The Signatures are to be extracted from documents through scanning and cropping. Signature images were stored in portable network graphic (JPG) format. These images were converted to grey scale for further processing. For converting an RGB image to gray scale, the RGB values for each pixel are taken and made as output a single value reflecting the brightness of that pixel. Such approach is to take the average of the contribution from each channel: (R+B+C)/3. However, since the perceived brightness is often dominated by the green component, a different, method is to take a weighted average, e.g.: 0.3R + 0.59G + 0.11B.

The signature is extracted using webcam or a scanner. Then the required portion is cropped .Now the resolution of the image is found and the number of planes are also found. If the number of planes is three then the image is colour image. It is given to a conditional statement that if number of planes are three then convert it into black and white using the command rgb2gray()

which converts RGB images to grey scale intensity image by eliminating the hue and saturation information while retaining the luminance.

The image resolution is resized using the command imresize() so that size of the image is reduced such that the processing time is reduced and will be a constant time for every image irrespective of original image resolution.

To enhance image we use adapthisteq() which enhances the contrast of the gray scale image by transforming the values using contrast limited adaptive histogram equalization.The image is now complemented using the command imcomplement() which computes the complement of image where the image is binary or grey scale or RGB. This is done because the SIFT features are extracted for high intensity values and signature is low intensity where as background is high intensity. So the image is complemented.

Again the image is enhanced using the command imadjust() which maps the intensity value in grey scale image to new values such that 1% data is saturated at low and high intensities of original image. Now the image is binary which has only 1 or 0 by keeping a threshold value such that if intensity is greater than threshold then it is 1 otherwise it is 0.im2double() converts the intensity image to double precision, rescaling the data if necessary.

2.2.2 Calculation of Euclidean Distances:

Euclidean distances are calculated between the SIFT features of two given signature images to measure the variability between them. The motivation to use Euclidean distance as a measure of variability between images is derived from its success in object recognition and lately in fingerprint verification. Say we have two signatures **A** and **B**. Let A_i be the i^{th} key point in signature **A** and B_j is the j^{th} key point in signature **B**. The distance D (A_i, B_j) was calculated as the Euclidean distance between A_i and B_j. K_a, $K_b$are the number of key points in signature A and B respectively. The distance measure D (Ai, B) was taken as the average Euclidean distance from the i^{th} key point in signature **A** to all the key points of signature **B**. The image distance between signature **A** and signature **B** is given by

$$D(A,B) = \frac{1}{k_a}\sum_{i=1}^{k_a} D(A_i, B) \qquad (4.7)$$

2.2.3 Creation of the Known Signature Template:

Signatures and arbitrary writer IDs were used. For each known writer, a sample of three signatures say **A**, **B** and **C** were taken to cater for intra-personal variations. A template was generated as a MATLAB file and stored. The template has the following:

(i) Writer ID.

(ii) The Euclidean distances between key points i.e. D (A_i, B), D (A_i, C), and D (B_j, C).
(iii)The distances between the Signature images i.e. D (A, B), D (A, C) and D (B, C).
(iv)Intra-class thresholds: The maximum among D (A, B), D (A, C) and D (B, C) i.e.

Max(D (A, B), D (A, C), D (B, C)). The minimum among D (A, B), D(A, C) and D(B, C)

i.e. min (D(A, B), D(A, C), D(B, C)). The average on D(A, B), D(A, C) and D(B, C) i.e. avg (D(A, B), D(A, C), D(B, C)). The range on maximum intra-class distance given by max (D (A, B), D (A, C), D(B, C)) ± 0.05. The range on minimum intra -class distance given by min (D (A, B), D (A, C), D (B, C)) ± 0.05.

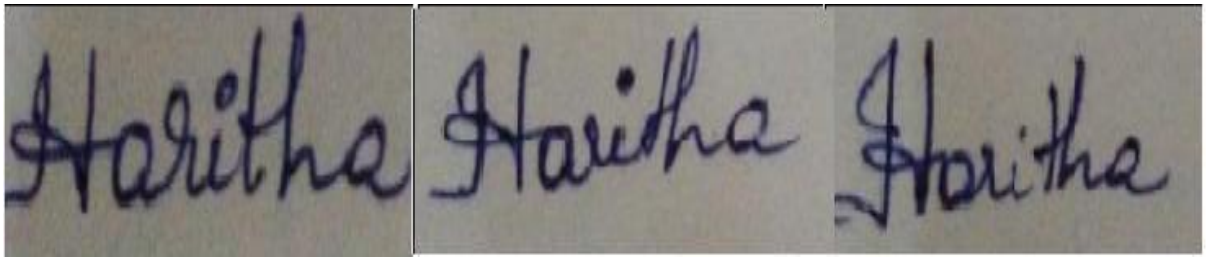


Fig. 5.0: Example of Intra-Personal Variation.

2.3 Signature Verification:

Verification is the process of testing whether a claimed signature is of the same (class) writer as the set of signatures enrolled in the system for that class. Verification involved loading the template MATLAB file enrolled in the system and comparing its stored parameters with those calculated by the outlier detection process.

2.3.1 Outlier Detection:

Test signature say T claimed to be of a particular writer, the Euclidean distances were calculated between the test signature and each of the three sample signatures, resulting to distances between the images i.e. D(T,A), D(T,B) and D(T,C).

The inter-class thresholds, max(D(T, A), D(T, B), D(T, C)), min(D(T, A), D(T, B), D(T, C)), avg (D(T, A), D(T, B), D(T, C)) are computed.

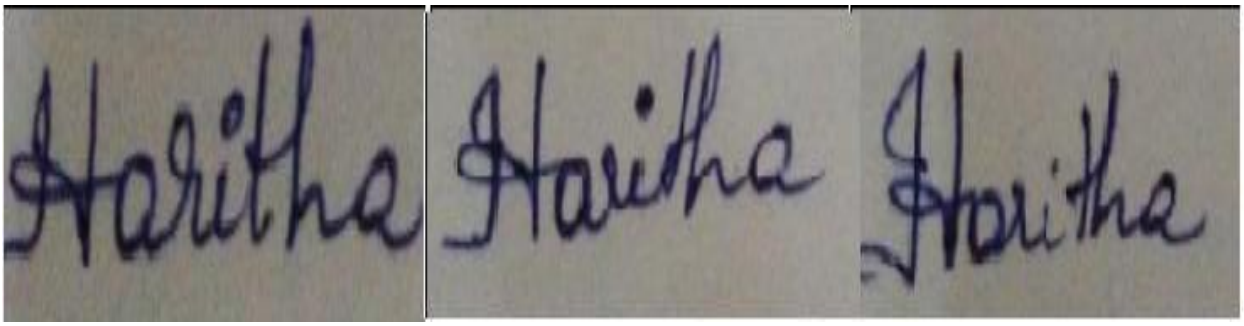
2.3.2 Comparison and Decision Criteria:

The comparison between the distance parameters of the SIFT features of the claimed test signature was done with those of the stored template. Each decision criteria was a binary classification and was taken independently.

Let W be (D(T, A), D(T, B), D(T, C)) and Z be(D(A, B), D(A, C), D(B, C)).

2.4 Results

Intra-personal variations:



Enrolled signatures

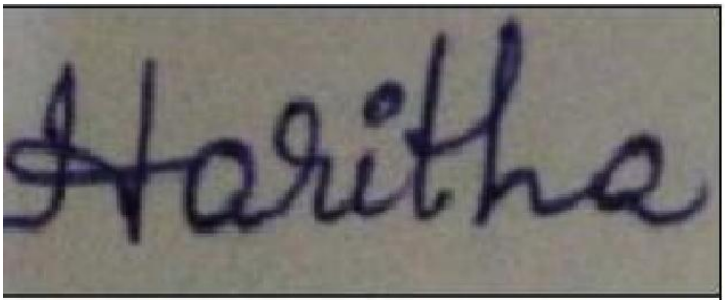


Image for processing

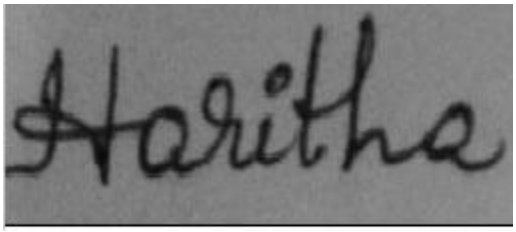
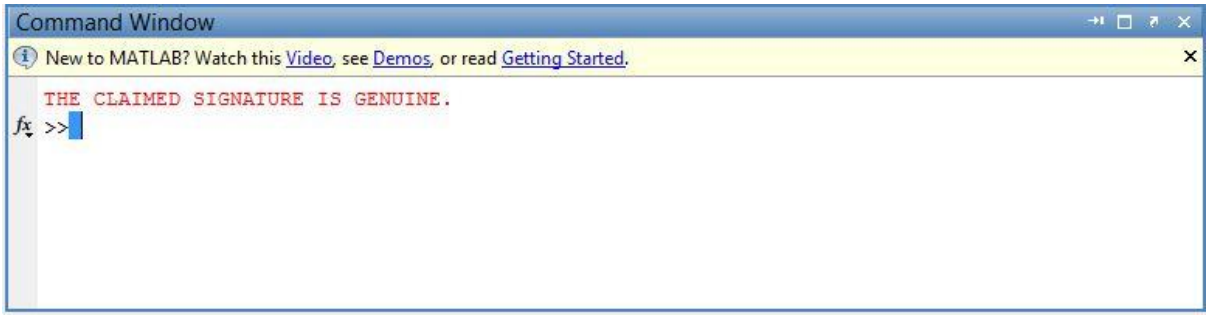


Fig 5.3: Complemented Black and white image

Binary image

Mapping of keypoints



For a genuine signature output

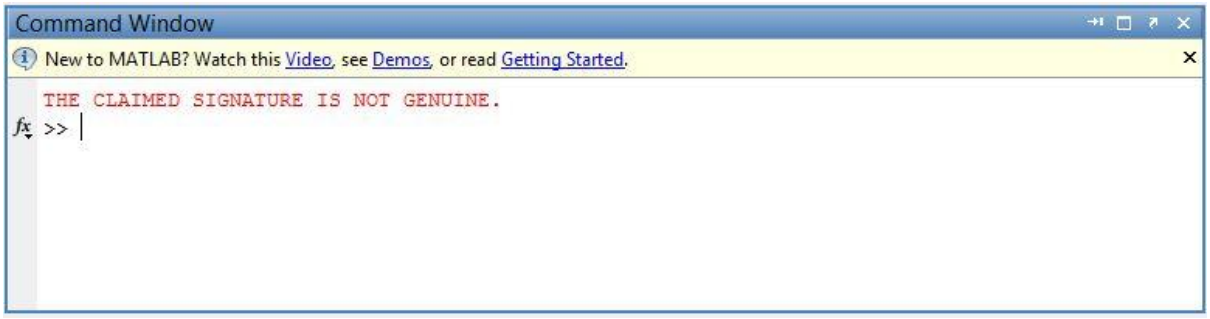


Fig 5.7: For a forgered signature output

3. Conclusion

3.0. Conclusion

This project was mainly to offer an efficient and economically viable offline handwritten signature verifier. The survey has been done on various existing methods of offline handwritten signature verification were reviewed and SIFT features were decided as they are cheap to compute in terms of processing requirements compared with other methods. The proposed system aim is to validate if the given signature is genuine or not.

In order to meet the objective various existing methods of offline handwritten signature verification were reviewed and SIFT features were decided as robust image descriptors.A database of signatures was collected consisting of known writers' signatures and forgeries. It was noted that some writers have large discrepancies between three of their sample signatures such that even a forgery may fall within the intra class distances which may result to a false negative notification this might have been caused by physiological factors.