Signature Verification through Pattern Recognition

Asst. Prof. SoniyaHingu
Department of ComputerEngineering,
A.D.Patel Institute of Technology,
CVM,V.V.Nagar,India
soniya17nov@yahoo.com

Asst. Prof. Macwan Kiran
Department of ComputerEngineering,
A.D.Patel Institute of Technology,
CVM,V.V.Nagar,India
Kiranmac711@gmail.com

Abstract**—**The signature is being used as a personal authentication this fact forces the need for an automatic verification system. The verification can be done either Offline or Online based on the application that is to be prepared. The Online systems use dynamic characteristics of a signature captured at the time the signature is made. While Offline systems work on the scanned image of a signature.[4[We have worked on the Offline Verification of signatures using a set of shape based geometric characteristics. Features that are used are Baseline Slant Angle, Aspect Ratio, Normalized Area, Center of Gravity, number of edge points, number of cross points, and the Slope of the line joining the Centers of Gravity of two halves of a signature scanned image. Pre-processing of a scanned image is necessary to differentiate the signature part and to remove any spurious noise present, before extracting the features. [4] The system is initially trained using a database of signatures acquired from those individuals whose signatures have to be authenticated by the system. For each subject a average signature is obtained integrating the above features derived from a set of his/her genuine sample signatures. This average signature acts as the basis for verification against a claimed test signature. Euclidian distance in the feature space between the claimed signature and the template serves as a measure of similarity between the two. If this distance is less than a pre-defined threshold (corresponding to minimum acceptable degree of similarity), the test signature is verified to be that of the claimed subject else detected as a forgery.[4] The details of pre-processing as well as the features depicted above are described in the report along with the implementation details and simulation results.[4]

Keywords—*Verification, Features Extraction, Forgery*

*****

I. INTRODUCTION

For person identification Signature has been a differentiating biometric feature. Even today an increasing number of transactions, especially related to finance and business are being authorized via signatures. So the need to have methods of automatic signature verification must be developed if authenticity is to be verified and guaranteed successfully on a regular basis. Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line.[6]

Processing Off-line is complex due to the absence of stable dynamic characteristics. Offline data is a 2-D image of the signature. Processing Off-line is complex due to the absence of stable dynamic characteristics. The main issue also lies in the fact that it is hard to segment signature strokes due to highly stylish and different writing patterns.[6] The variety of the writing pen and its nature may also affect the nature of the signature obtained. The no repetitive nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, raises 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 points.[6[

On-line verification records the motion of the stylus while the signature is produced, and includes location, and percentage velocity, acceleration and pressure of pen, as functions of time. These dynamic characteristics are specific to each individual and sufficiently stable and repetitive. Online systems use this information captured during acquisition. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive.[6]

II. PROBLEM STATEMENT

We approach the problem in two steps. Initially the scanned signature image is pre-processed to be suitable for extracting features. Then the pre-processed image is used to extract relevant geometric parameters that can distinguish signatures of different persons. The next step involves the use of these extracted features to verify a given image. If the signature is not valid then it will detect the forger attempts.

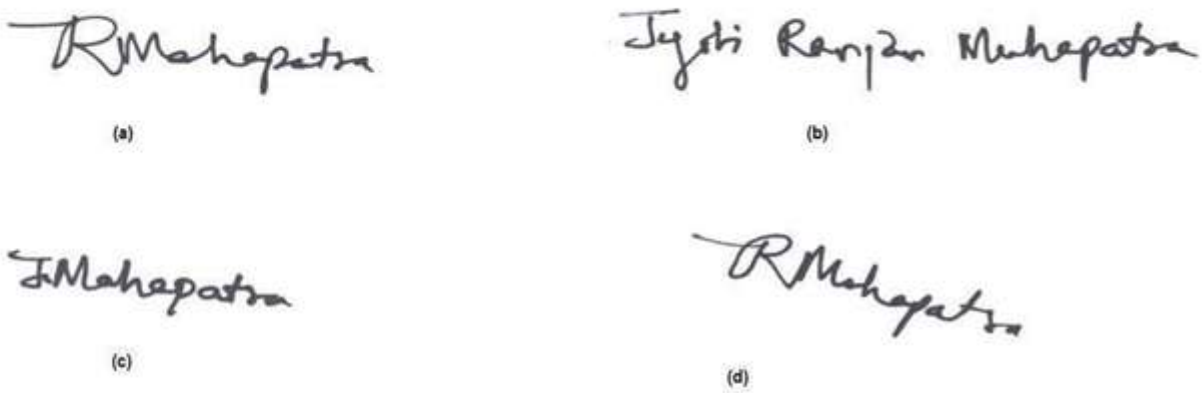
Types of Forgery

The various types of forgery include.

Random Forgery: A person who is unaware about the shape and style of the original signature.try to attempt a random one.fig 1(b)

Simple Forgery: The person concerned has a little idea of the original signature in this type of forgery, but is signing without much practice. fig 1(c)

Skilled Forgery: It includes decent knowledge about the true signature along with ample time for proper practice.The proposed scheme reduces random and simple forgeries and also reduces skilled forgery to a great extent. Fig 1(d)

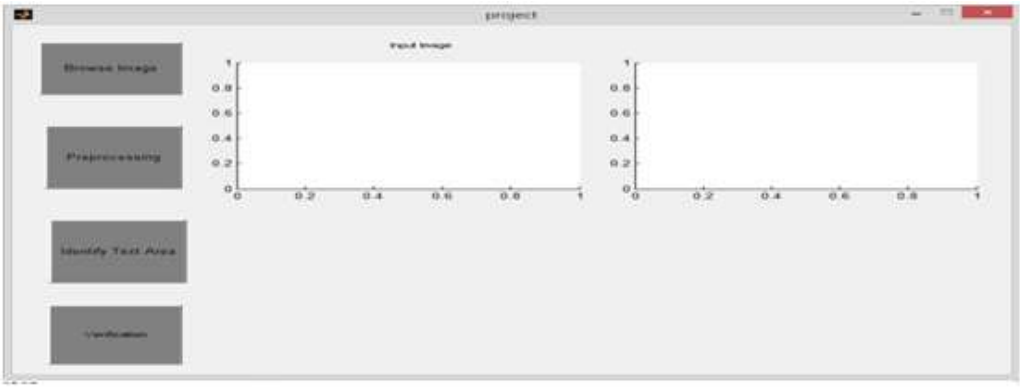


III. PROPOSED WORK

The use of signatures is one of the most employed mechanisms to verify the identity of individuals; the whole bank-check payment system is based on the use of signatures. In this context, computer-based signature verification is an active research area in biometry.[7] Lot of experiments and research work has done within last few years regarding off-line and on-line signature verification.[7] Though online verification provides better result than off-line system but off-line verification is also important in some situations where the person is not present physically.[7] The past experiments work fine to detect simple and random forgery. But have lesser success rate to detect skilled forgery. Keeping that thing in mind this system is developed, where some special properties and style of a genuine signature is detected for identification purpose. These properties are marked and compare it the test signature. [7]

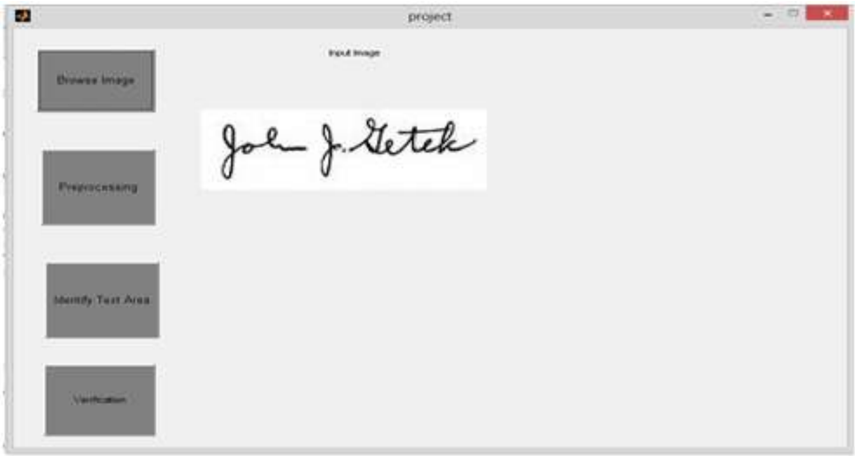
IV.IMPLEMENTATION WORK

The first task adopted according to the methodology is pre processing which carries out three main functions 1.)RGB to Gray conversion 2.)Resizing 3.)Median filter for noise removal.



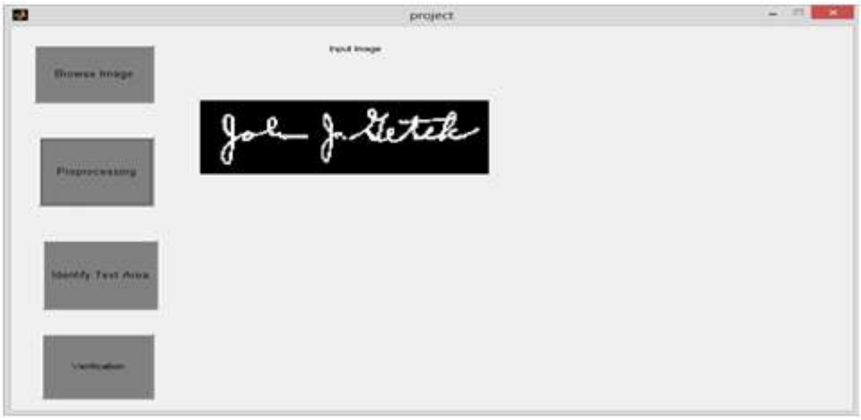
(a) Implementation Layout

According to the system designed the first task is to browse the image which is to be taken as input. Two basic boxes are taken one for the input image and the other with which the input image is verified. The input image is browsed from the user sample.



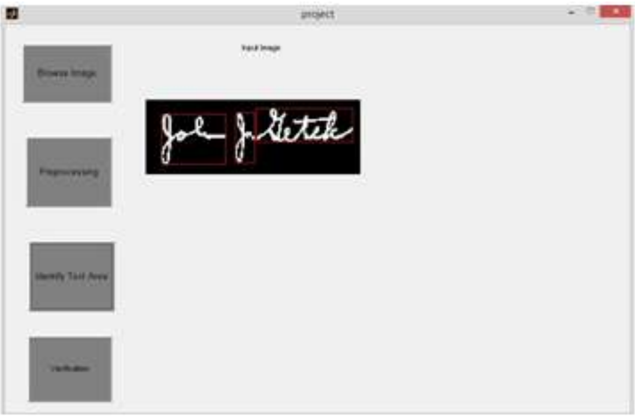
(b) Scanned Image

As per the first task of pre- processing signature of a user named John is taken by clicking the Browse image button. Signature is browsed to the input image box.



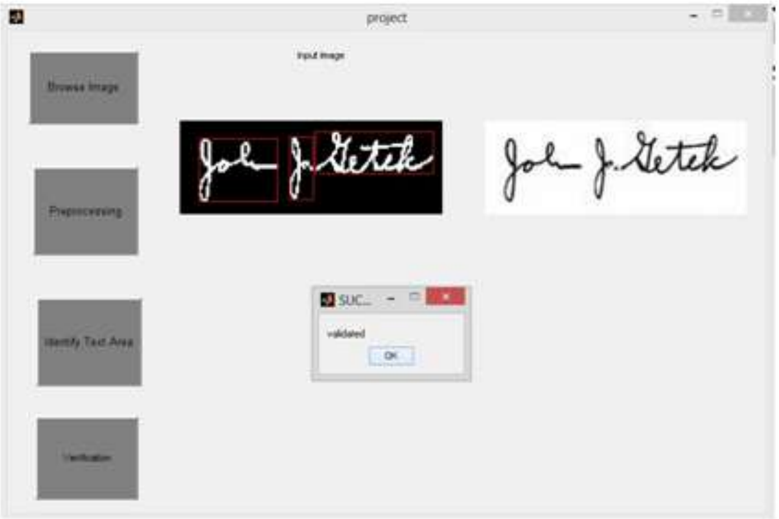
(c) Gray scale image

Once the input image is collected pre-processing task is initiated by clicking on pre-processing. First sub task of pre-processing RGB to Gray conversion is done and image is obtained as shown in the figure.



(d) Text Area Allocation

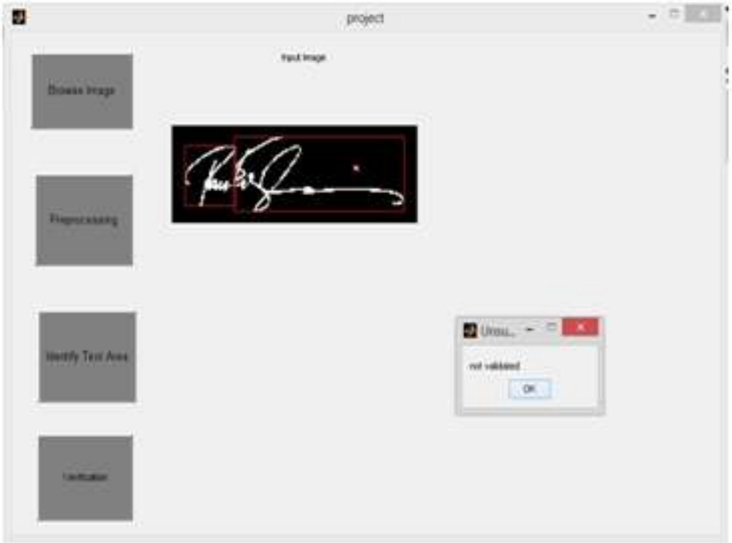
The other subtask in pre-processing of resizing the image and filtering for noise removal is performed in the background while processing the image. The next step is to only identify the area which is covered only by the signature i.e. text area recognition. By the Identify Text Area button the verification of image is contracted to only the text area covered in the image.



validated

(d) Verification

After the text area being classified, the main procedure is carried out that is comparison of the input image with the one stored in the database of the same intended user. For this particular features of the input signature are extracted. These features are compared with the already same extracted features of other two previously stored sample signature of same user. If the features are matched and it satisfies the Euclidean distance then the system accepts the signature. It delivers success by the message validated.



not validated

(e) Rejection

Similarly if the input image fails to achieve the error acceptance ratio then the system gives the message not validated and rejects the signature.

V. RESULT AND ANALYSIS

Table 1(a) Feature Measurement

Mean Values of Features	**Sample 1**	**Sample2**
Image Threshold	84	93.5
Slant Angle (SA)	15	20
Aspect Ratio (AR)	1.6500	2.8409
Normalized Area (NA)	.0803	.0608
Center Of Gravity (COG)	(482.2187,212.68)	(512.4289, 318.7370)
COG- Left half	(191.95,113.98)	(260.4076, 189.4470)
COG-Right half	(158.605,206.75)	(184.571, 133.5464)
Slope	-2.8715	0.7371
No. of Edge Points	10	28
No. of Cross Points	6	11

The expected results of our simulation for forged and genuine signatures are as shown in the table below. The system will be robust; it will reject all the casual forgeries. Out of the 25 genuine signatures that will be fed in, assume 4 will be rejected as forgeries. This will yield a False Rejection Rate (FRR) of 5.26%. Also out of 10 skilled forgeries fed into the system, 2 signatures will be accepted. This gave us a False Acceptance Rate (FAR).

VI. CONCLUSION

The proposed signature verification system is been based on some special features extraction. Global features included connected component, height width ratio, number of end points and type of end point line. It uses a compact and memory efficient storage of feature points, which reduces memory overhead and results in faster comparisons of the data to be verified. From intuition, the statistics on the positional variations of the features or strokes of signature samples should be useful for verification.[5] The present study was aimed at evaluating the usefulness of the method.[5] Although it is not the best among all existing methods, there is the possibility of combining it with other methods to achieve better results. Similar to other real world problems, no single approach may solve the signature verification problem perfectly, and practical solutions are often derived by combining different approaches. This technique can be added with any existing verification system for better result.[5]

VII. FUTURE WORK

The system needs to be modified in the section in which more features could be added as well as deleted if it is no more used for accuracy. The efficiency has to be achieved by adding features to the pre-specified database signatures due to which no genuine signature falls into category of forger attempt.

ACKNOWLEDGMENTS

This research paper was supported by Prof. BhagirathPrajapati and Prof. Priyanka Puvaras well as the institution A. D. Patel Institute of Technology, Gujarat, India.

REFERENCES

[1] DeepthiUppalapati, “Integration of Offline and Online Signature
Verification systems,” Department of Computer Science and Engineering, I.I.T., Kanpur, July.

[2] M.K kalera, S. Shrihari, "Offline Signature Verification And Identification Using Distance Statistics", *InternationalJournal of Pattern Recognition and Artificial Intelligence* Vol. **18**, No. 7 (2004) 1339-1360 ,World ScientificPublishing Company.

[3] MinalTomar&Pratibha Singh, "A Simpler Energy Density method for Off-line Signature Verification using Neural Network".

[4] https://homepages.cae.wisc.edu/~ece533/project/f05/ganesan_dhawanrpt.pdf

[5] http://www.erpublications.com/uploaded_files/download/download_08_07_2015_12_28_38.pdf.

[6] http://www.ijcsit.com/docs/Volume%205/vol5issue01/ijcsit20140501153.pdf

[7] http://www.erpublications.com/uploaded_files/download/download_25_06_2015_16_10_48.pdf