FRAUD DETECTION USING SIGNATURE VALIDATION

Hussain Manasawala[1] Yadnesh Mankame[2] Harshal Patil[3]
Pillai HOC College of Engineering & Technology, Rasayani
BE, Dept. Student of Computer Engineering, PHCET,
BE, Dept. Student of Computer Engineering, PHCET,
BE, Dept. Student of Computer Engineering, PHCET,

Abstract- Validation can be performed in many ways, the verifiable and most as often as possible accepted technique is a hand signatures. Detecting fraud in manually written signature is an intense job for any examiner. It is an essential job that has been utilized to resolve clashes for years. The current system just store the signature as a picture not under the most dependable conditions: With low resolutions, written in a small area, composed while moving, composed with the finger i.e. it is written in such a manner that it cannot be classified as fraud or authentic. Thusly there is a need of changing this information to allow an examiner to control it and gain the required results. Manipulation in the written signatures can be done by scaling, rotating, greying etc. So to get the required results based on several parameters can be achieved. After analysing the signature based on parameters now deciding the authenticity of a signature can be done. The principle objective is to find a way to deduce fraud signature. This paper depicts endeavours to create an application that prevents fraud signature and detects the same. This can be used in banking sectors, organisation or wherever there is a need of signature validation.

***Keywords*— dynamic, signature, KNN, cohen kappa cofficient**

I. INTRODUCTION

A signature is a pattern or mark made by a single person on piece of document or using electronic signature machine to signify acknowledgment, acceptance, authorization or commitment. The sign is considered as authorized validation proof on document that one has consented to agree to the terms & conditions written in the document and further that he has read all the contents and he has affixed his sign as token of correctness. In similar manner a person's signature is treated as "Trademark" and one's sign can be in any shape or in tangled manner and completely in a decipherable character's that can be separately called out as a person's name. In many cases there is no resemblance to the writer's name but are somehow identifying marks.

With the constant increase in the crime rates signature forgery has made its way through the list. Very important documents (land papers, affidavit, confidential etc) are signed in an unethical manner without the signer having the information of the document. Cash withdrawal using a blank cheque with forged sign of the actual account holder, and many such forgery cases take place every year. Handwritten signs have been very conflicted thing to be examined from the centuries as it's a very important task. With arrival of new technologies for being part of signing the document has come up with new challenges for this task. Unfortunately, the information that is collected cannot be compared with eyes. After capturing the relevant data, a framework can extract the significant features that can help in deciding the genuineness of a signature compared with the authentic signature. Authentication can be performed from various perspectives, yet the historical and most habitually utilized technique is a hand written signatures. This habit of hand written signature is being followed for ages and is consider being the best way of authentication. After various improvements in technology the use of electronic devices such as electronic pads and contact screen came in to usage to capture signature, for example, cell phones and tablets.

There are Four Major Benefits of Digital Signatures:

Efficiency: documents can be signed in an instant from anywhere in the World where there is an internet connection. All pages can be automatically initialed, and there is no need for witnesses. Its customer friendly allows for contracts to be signed sooner, booking revenue sooner. Authentication: the owner of the digital key is bound to a specific user, no need for a handwriting expert anymore. Integrity: the document and the signatory are linked, so that there can be no changes to the document post signature. Non-repudiation: an entity that signed digitally cannot deny that they have signed. The main objective is to provide the path for organizations to be able to analyze handwritten signatures acquired with dynamic information embedded. The major steps which would be required in for perfuming verification of signature are:- Input: The dataset Handwritten Signatures images are implemented as input image. The input images are taken in the format .jpg or .png. Pre-processing: The collected input images are subjected to pre-processing. In the Pre-processing step we can implement the image will be resize into no. of row = 256, no. of col = 256 and gray scale conversion is performed.

Segmentation: In this step segmentation is carried out using binary conversion method & thinning is also performed in this step.

Feature extraction: In this feature extraction, we can use the geometric features like, shape and edge will extract.

Classification: In the classification process, we can implement the KNN classifier to classify the input signature is real or fake. (RPF classification is used in the paper).

Performance Estimation: In this module, the performance metrics like Accuracy, Sensitivity & Specificity will be estimate.

II. Related work

A. Handwritten Signature Verification:

Author-Md. Jahid Faruki Syed Khaleel Ahmed. 2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA).

It is online verification using a fuzzy inference system. Verification: Online verification using a fuzzy inference system. A FIS-based method is used for signature verification. FIS is well suited for this task due to the similarity between individual signatures but has a low acceptance rate.

B. Offline Handwritten Signature Recogniztion using Histogram Orientation Gradient and Support Vector Machine:

Author- Nidaa Hasan Abbas, Khaled N. Yasen. JATIT 30th April 2018. Vol.96. No 8.

The objective of this paper is proposing an offline handwritten signature extraction namely Histogram Orientation Gradient, in order to be passed into Support Vector Machine (SVM) but due to its slower detection it consumed more time to recognize.

C. Static Handwritten Signature Recognition Based on Hogs Using K-NN Classifier:

Author- Panditkumar Patil, Geeta B, International Journal of Computer Engineering and Applications, Volume XII, Issue I, Jan. 18,

A study on static handwritten (offline) signature recognition using feature extraction methods. Only Extracting features doesn’t help to achieve accurate signature validation.

D. Signature Recognition and Authentication from Multishare Based Image Database:

Author-Sharayu S. Sangekar, Minal C. Toley. International Journal of Computer & Mathematical Sciences IJCMS ISSN 2347 – 8527 Volume 7, Issue 3 March 2018

How to improve security of biometric systems with the help of signatures using multilayer multishare approach of hierarchical visual cryptography. Hierarchical visual cryptography is defined on the basis of visual cryptography.

III. Existing system

With the expansion in utilization of signature as a parameter for verification there is a need of system which can recognize fake signatures. If it is possible that a device is able to store the signature done by hand signature and it is supplied as an attachment to the applicable document. In many of the devices signature is stored in an image format , much of the time not under appropriate conditions: with low resolutions, written in a compact space, written while moving, etc. In many system in which the signature procedure is like the conventional technique (i.e., with a pen, on an appropriate surface), the signature is represented as in the picture with lines of a similar width. Therefore just by comparing the images it becomes difficult to prove the uniqueness of the signature.

A. Problem Statement

Since long signatures have considered to be a unique form of authentication in many sectors. So it is not surprising that people use many different forms of their name as signature. Even today in Banking sector the signature validation are done by human eyes which cannot give an accurate result some banks scan the documents where signatures are verified using pixel matching technique. Very important documents (land papers, affidavit, confidential etc) are signed in an unethical manner without the signer having the information of the document. Today’s existing system are not so reliable, even a valid user is said to be a fraud customer or vice versa.

IV. Proposed System

The process is to detect the fake signature and recognize the authentication results. A image is collection of pixels values in rectangular pattern. Each pixel represents the measurement of some property of scene measured over a finite area. For accurate segmentation the most useful features are spatial frequency and an average grey level. Hence here we use GLCM algorithm for extracting features. In addition to these features shape and boundary of the signature will also be calculated using Fourier Descriptor, Edges using Canny Filter and thereafter calculating the distance and height of the signature and lastly calculating the standard deviation. In pattern recognition, the K-nearest neighbor classifier (K-NN) is a non-parametric method used for classification and regression. The output depends on whether the K-NN is used for classification or regression. Here we classify text based on extracting the feature from the image.

A. KNN Algorithm

The k-nearest neighbors algorithm(k-NN) which is a pattern recognition method that uses non-parametric for classification and regression. In both scenarios k closest consist of training examples in the feature space. If k-NN is used for classification or regression the output depends upon it.

B. GLCM as Gabor

The grey Level Co-occurrence Matrix1 (GLCM) and associated texture feature calculations are image analysis techniques. An image is composed of pixels having intensity (a specific grey level), the GLCM is a tabular manner of how often various combinations of grey levels co-occur in image section. Texture feature calculations use the contents of the GLCM to give a value of the variation in intensity (a.k.a. image texture) at the interested pixel.

C. Cohen Kappa’s Coefficient

CKC (k) is a statistic inter-calculated decision for categorical things (items). It is more accurate calculation then simple percent decision calculation, as *k* take into consideration of possibility of the decision occurring by chance.

D. Block Diagram

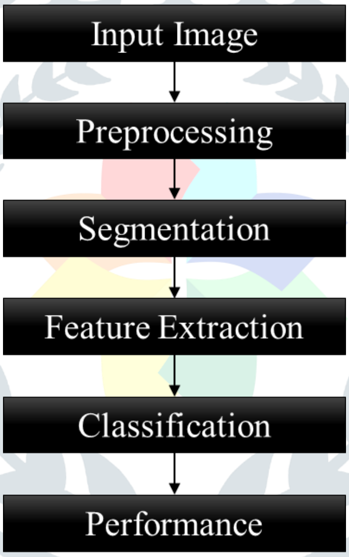


Figure 1: Block Diagram

E. System Architecture

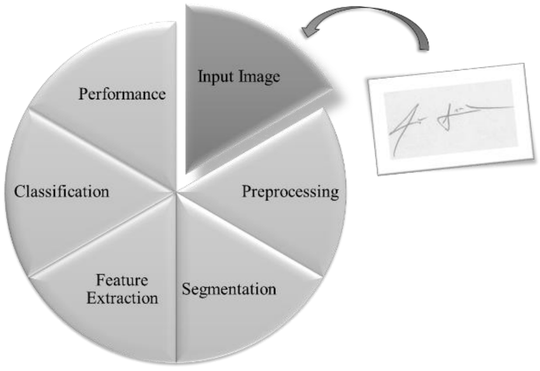


Figure 2: System Architecture

F. Requirement Analysis

- Hardware Requirement :
  - Processor – i3 2.4 Ghz
  - Ram – 4GB DDR
  - Hard Drive – 256 GB
- Software Requirement :
  - OS – Windows 7 and higher
  - Tool – Matlab R2015b

G. Dataflow Diagram

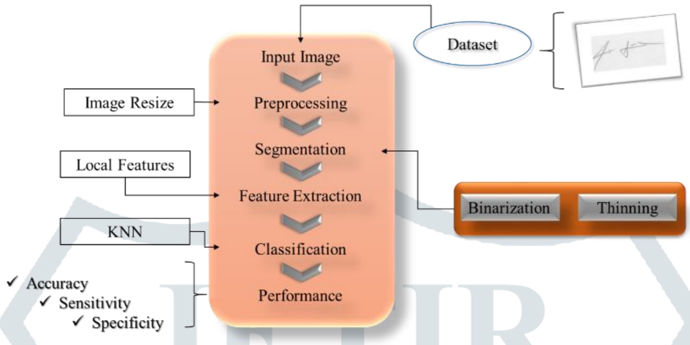


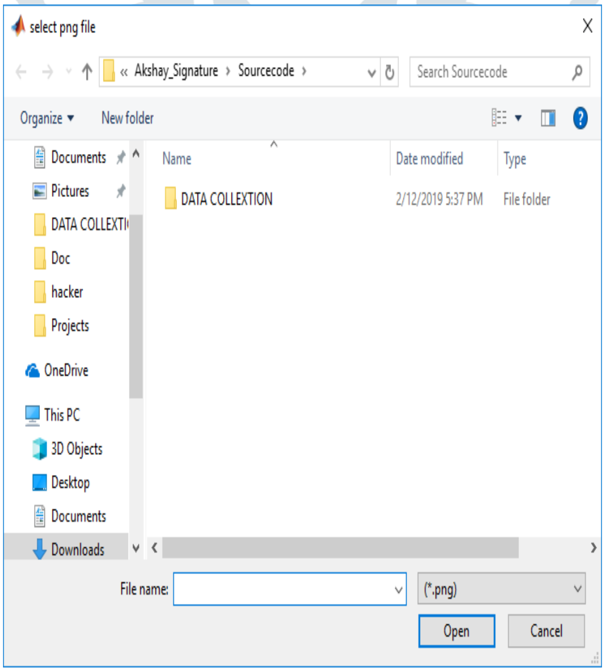
Figure 3: Dataflow Diagram

The diagrams are showing the flow of the signature verification system. This system is efficient to detect the fraud signature by taking the image as input in the system. Then by resizing the image and making its binary image. Later it will extract the image features in a table by comparing it with the database and showing the readings and Gabors. Finally letting we know whether the image is original or fake.

We have use the dataset's of signature's to make the system more efficient and accurate in the nature so that it will not give false positive results.

V. Images Illustrating the Flow of System

1. Input to the system



Name	Date modified	Type
DATA COLLEXTION	2/12/2019 5:37 PM	File folder

File name:
(*.png)

Figure 4: Input to the sytem

2. Inputed Image

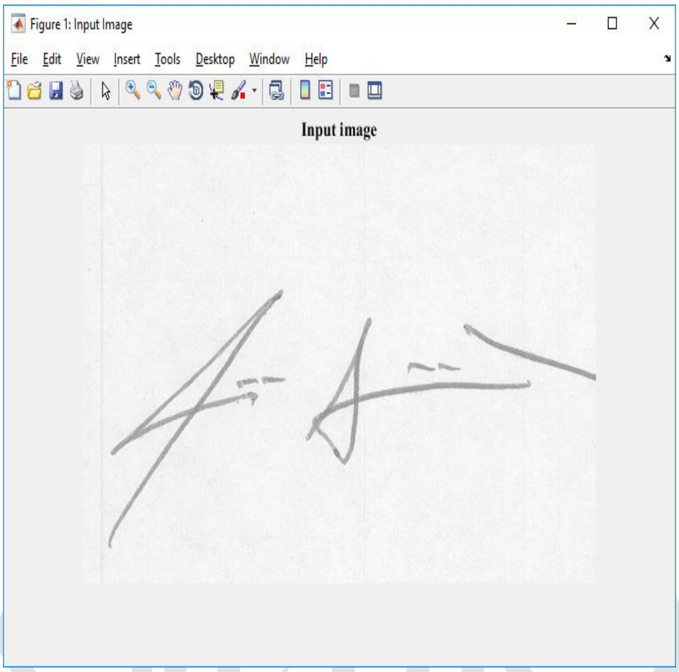


Figure 5: Inputed Image

3. Resized Image

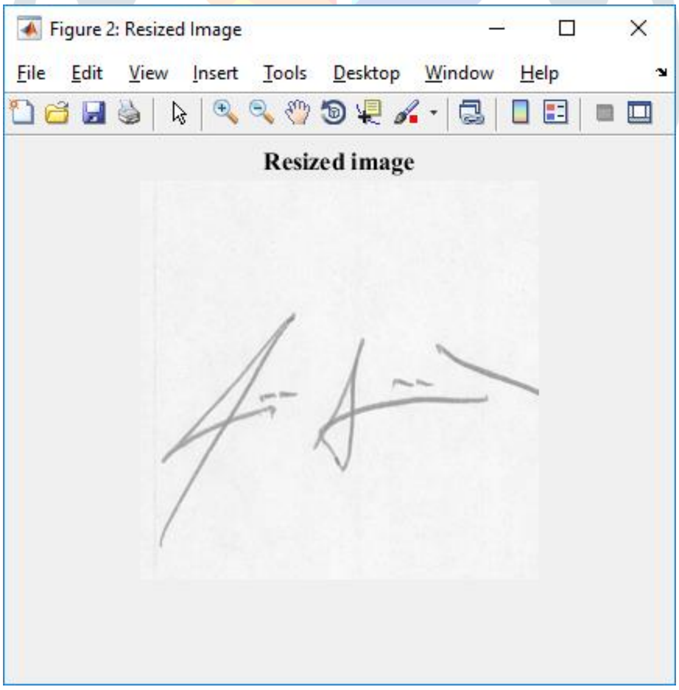


Figure 6: Resized Image

4. Binary Image

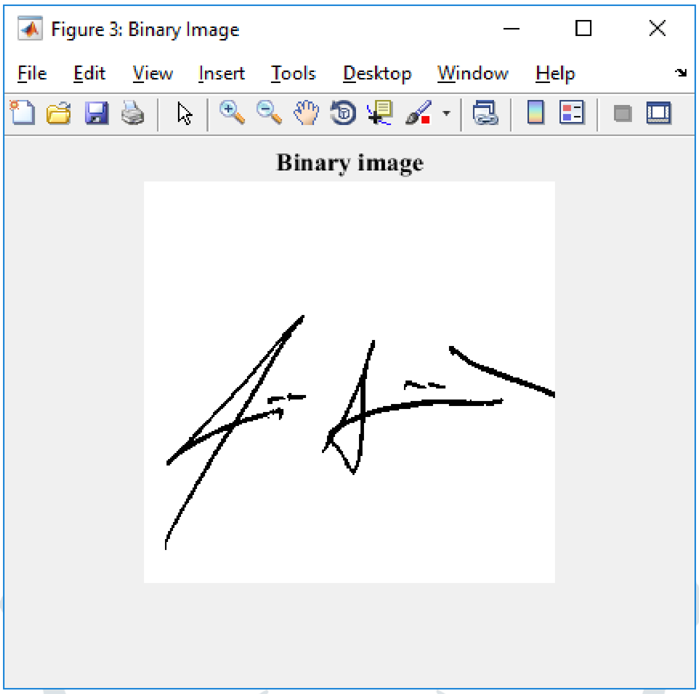
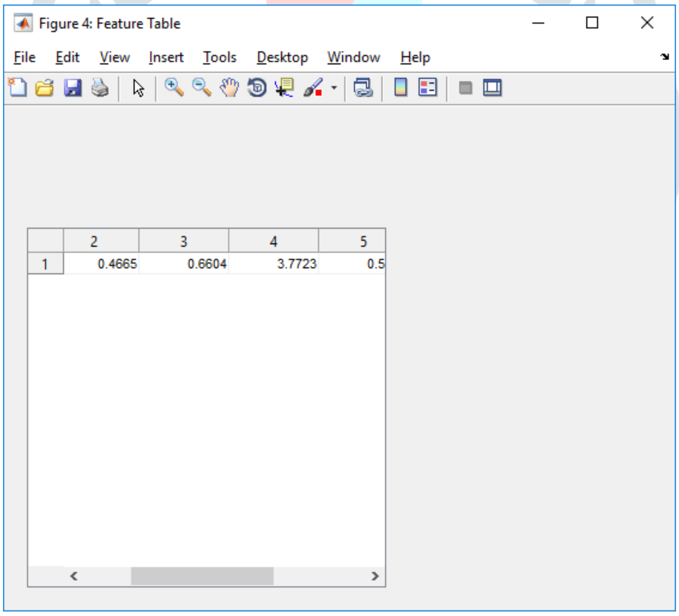


Figure 7: Binary Image

5. Feature Table



	2	3	4	5
1	0.4665	0.6604	3.7723	0.5

Figure 8: Feature Table

6. Performance Graph

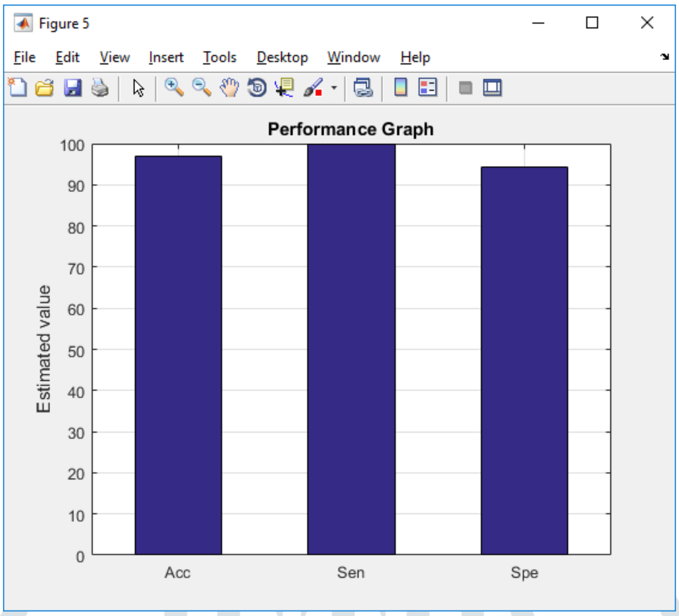


Figure 9: Performance Graph

7. Gabor

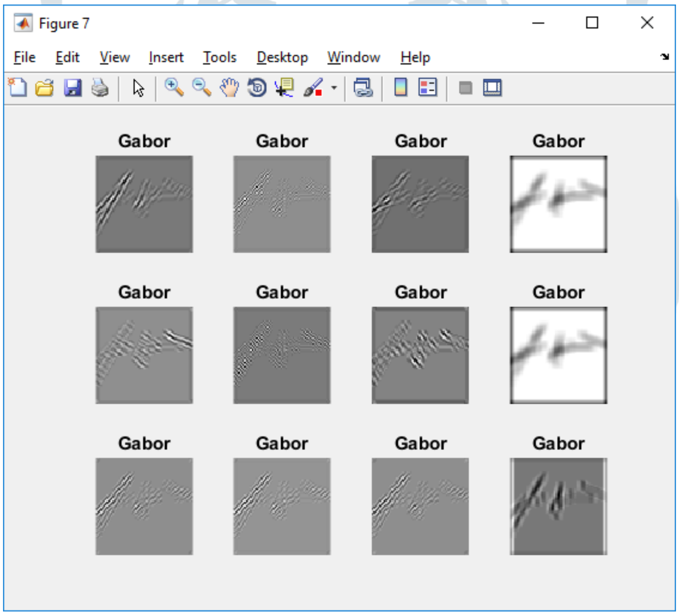


Figure 10. Gabor

8. Orginal or Fake

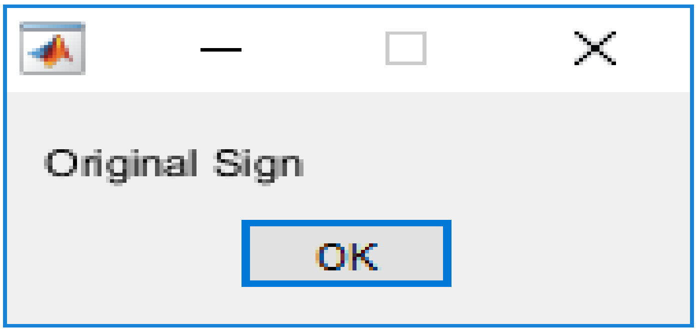

Original Sign

Figure 11: Orginal or Fake

VI. Results

The obtained results of the proposed technique are viewed in this section. The execution was done with Intel i3 processor, 2.4 Ghz and 4 GB of memory using Matlab v.R2015b tool. Test performed were done on various different sets of signatures. This signatures have been taking manually on the sheet of paper and then scanned on the scanner to make it digital signature.

The k-NN algorithm technique performed the obtained results with one-step method like as CKC (k) or Gabors. The mark reached by this technique is of 0.4256 with GLCM and 0.97 based on the Cohen Kappa's Coefficient, and it illustrate that the present technique is effective approach for fraud detection using signature.

VII. Conclusion

In this paper, we introduced a modified verification method for detection of fraud signatures. K-NN, CKC and GLCM method were combined for perfectly identify the shape and size of the signature. In the first step, CKC resizes the image and convert it into binary image. Then k-NN algorithm extracts the feature from the binary image and views it in the table. Later the GLCM method as Gabor helps to compare the image and feature with rest of the images in the database using the distortion and other techniques. In last if the image matches the feature extracted and the stored features and then gives the result whether the image is original or fake. The approach is vigorous to the shape change and do not require large dataset for the training purpose of initial system.

References

[1] D. Impedovo, G. Pirlo. "Automatic Signature Verification- The State of the Art". IEEE Transactions on Systems Man and Cybernetics, 38(5):609-635, 2008

[2] A.C. Ramachandra, J.S. Rao, K.B. Raja, K.R. Venugopla, L.M. Patnaik. "Robust Offline Signature Verification Based On Global Features". In Proceedings of the IEEE International Advance Computing Conference. Patiala, India, 2009

[3] J. Coetzer, B.M. Herbst, J.A. du Preez. "Offline Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model". EURASIP Journal on Applied Signal Processing, 2004(4):559–571, 2004

[4] W. Hou, X. Ye, K. Wang. "A Survey of Off-line Signature Verification". Proceedings of the 2004 International Conference on intelligent Mechatronics and Automation. Chengdu, China,2004

[5] S. Sayeed, N.S. Kamel, R. Besar. "A Sensor-Based Approach for Dynamic Signature.

[6] 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.

[7] 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.

[8] Migual A. Ferrer, Jesus B. Alonso and Carlos M. Travieso, "Off- line Geometric Parameters for Automatic SignatureVerification Using Fixed- Point Arithmetic", IEEE Tran. on Pattern Analysis and Machine Intelligence, vol.27, no.6, June 2013.

[9] Debasish Jena, Banshidhar Majhi, Saroj Kumar Panigrahy, Sanjay Kumar Jena "Improved Offline Signature Verification Scheme Using Feature Point Extraction Method".

[10] en.wikipedia.org/wiki/Sobel_operator