Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.827 – 834

RESEARCH ARTICLE

Result Analysis for LBP and Shape Context Methodologies used as Authentication Mechanisms of Digital Signatures used for Certification

Shraddha Kulkarni[1], Prof. Vikrant Chole[2]

[1]Department of Computer Science and Engineering, G. H. Raisoni Academy of Engineering and Technology, Nagpur, India

[2]Department of Computer Science and Engineering, G. H. Raisoni Academy of Engineering and Technology, Nagpur, India

[1] shraddha.kulkarni6@gmail.com; [2] vikrantchole@gmail.com

Abstract— Signature is very important attribute which is mostly used for financial document Certification and personal identification. So it is necessary to check authentication and genuineness of that signature. In literature most of the signature verification methods verifies that whether test signature is perfectly aligned to the specified axis or not. If not then that method rejects that signature even though it may be genuine. Here, implemented technique verifies the signature size and angle invariant. The invariance can be calculated by scaling and rotational manipulations on the test image. In this paper proposed methodology shape context involves, cropping signature image from cheque, gray scale image conversion, Edge detection of image, Binarization of image which is then localized and compared with the account holder's source of information then it authenticate that cheque and clarify.

Keywords— Feature Extraction; Genuineness; Authenticity; Accuracy; Digital Signature

I. Introduction

From quite few years signature is used as biometrics attribute for personal identification and authentication purpose by human being. Handwritten signature involves lots of variation because it varies from person to person. And it is also very easy to detect any alteration in signature. As compared to traditional signature authentication method such as pen and paper signature the digital authentication of signature is very easy, because in this method signature is cropped and checked (verified) electronically. In online signature recognition technique signature is directly cropped, taken on device and then process and in offline signature recognition technique written signature is scan and process further. Here Offline signature recognition technique is used. In this test signature is compared with signatures samples kept into database, if test signature image is matching with database image then it give result authenticate otherwise it give result not authenticate.

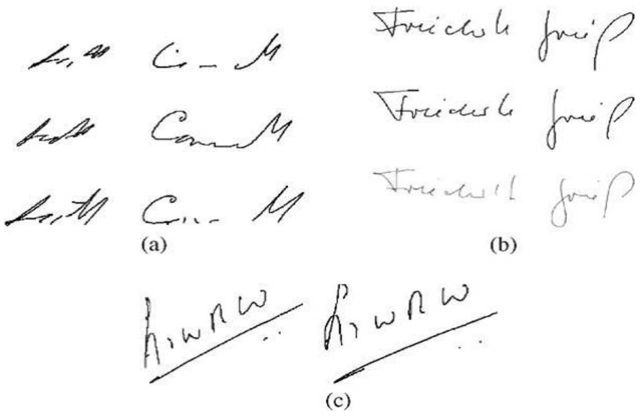


Fig. 1 Sample Signature Images.

II. **RELATED WORK**

A. Hidden Markov Models Approach.

Paper [5] talks about an offline signature verification system that is based on Hidden Markov Modelling (HMM) technique. Set of localized direction features are extracted from a scanned signature image and this technique is applied on them

In Paper [7] there is an elaboration on understanding HMM as stochastic models and their ability to determine distinctness and similarity of the patterns. Also speaks about how HMM states can be varied to analyse the state transition topology. Around samples of 100 users are used containing genuine and skilled random forged signature samples to do the testing.

B. Neural Network Approach.

Paper [8] speaks about the wide usability of neural network approach since it is very simple and powerful. There are 2 steps usually. In the first step features representing the signature are extracted. And a classification is performed on the samples. After the classification it is easily possible to determine if a signature is matching with any of the classes.

Paper [9] performs a study on two approaches. It is basically determination of a class the then match the signature. The 2 approaches are: 1) The Resilient Back propagation (RBP) neural network. 2) Radial Basic Function (RBF).

Around 2 thousand test signatures are available in the database which is mixture of genuine and forgeries with a ratio of 4:6. First classifier registers a 91% success rate and 88% is registered by the second classifier.

C. Support Vector Machine.

Paper [8] does a study on Support Vector Machine (SVM) algorithms. These are algorithms used in machine learning. It involves deriving unseen data by adjudging differences between classes using a high dimensional feature space of given data. Grid features and directional attributes of the signature are utilized to make a judgement.

D. Template Matching Approach.

Paper [10] claims template matching approach to be one of the simplest of approaches. It is mainly used for pattern recognition. It is not only a very simple and robust approach but also a very primitive one. It has a view disadvantages because of its robustness. This results in failure of recognition of distorted genuine patterns. Light distortion does get detected successfully but usually the intra class variations are large and hence it will not be advisable to use this for proficient ones. There are following forms in which this technique is used: Geometric feature extraction, Stroke analysis and Graphics matching.

E. Statistical Approach.

Paper [10] performs a study on statistical approach. Here patterns are considered as d features which is nothing; but a point in a Dimensional space. In a d-dimensional feature space the pattern vectors are kept in a close and disjoint regions hence categorizing the pattern vectors separately. A set of properly detached patters is considered as useful. A Hidden Markov Model (HMM) and Bayesian models used for pattern recognition are very popular examples of statistical approach. A Statistical approach is better than template matching approach in detecting even the adept forgeries.

III. PROPOSED METHODOLOGY

A. Objective:

Problem is divided into two stages. In first stage from scanned cheque, image signature image is cropped. Then that cropped signature image is pre-processed. After pre-processing that image is ready for feature extraction. Then from that pre-processed signature image all geometric features are extracted, which distinguishes signatures of different persons.

We propose a model in which appropriate classifier is used for verification. Signatures from database are pre-processed prior to feature extraction. Features are extracted from pre-processed signature image. These extracted features are then used to train a classifier. In verification stage, on test signatures pre-processing and feature extraction is performed. The classification is done between forged or genuine signature by applying the extracted features.

B. Algorithm:

A training stage consist of four major steps

- Retrieval of a signature image from a database
- Image pre-processing
- Feature extraction
- Training

A testing stage consists of five major steps

- Retrieval of a signature to be tested from a database
- Image pre-processing
- Feature extraction
- Application of extracted features to a trained classifier
- Checking output generated from a classifier.

C. Project Flow (Block Diagram):-

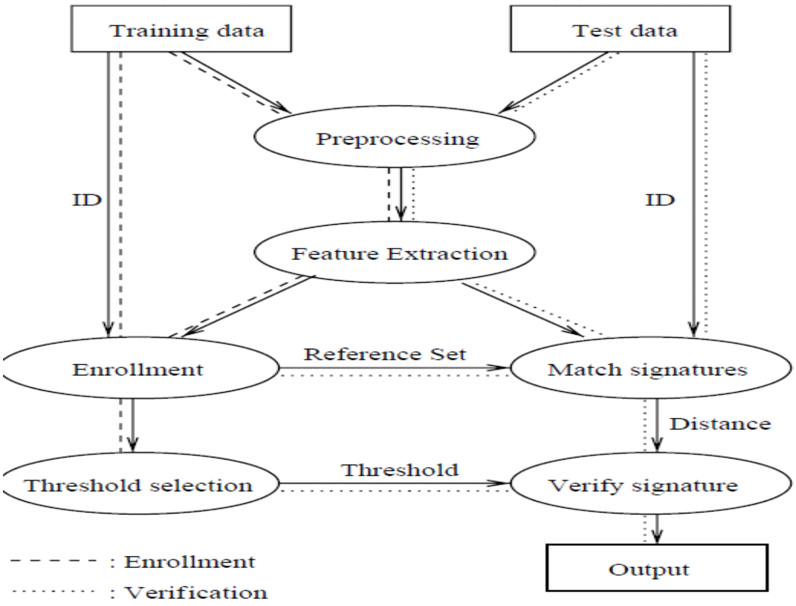


Fig. 2 Project Flow Diagram.

IV. RESULT AND ANALYSIS

This project is linked with Dropbox cloud (virtual cloud). The total project divided into two parts

A. Client Part (Main.m Form).

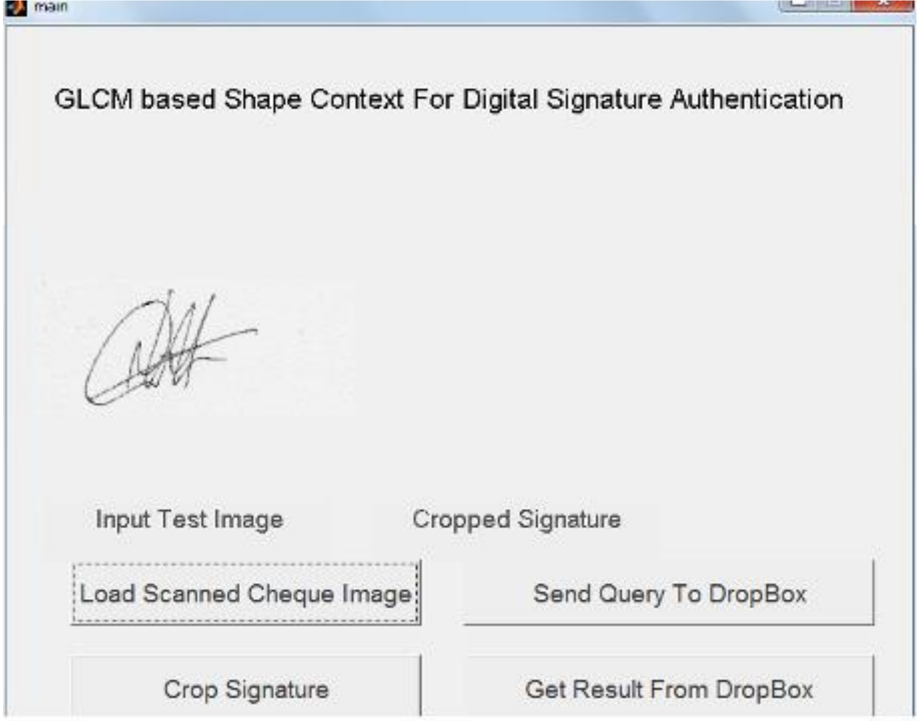


Fig. 3 Client Form

Figure 3 displays the form for the Client side. It contains following actions:

1. *Load Scanned Cheque Image:* The scanned cheque images will be loaded.
2. *Send Query To Drop Box:* The cropped image is sent to the server form for further processing.
3. *Get Result from Drop Box:* It obtains the result of image processing from the server.

B. Server Form (GUI.m) using LBP Methodology

In this Form LBP methodology is used i.e. Local Binary Pattern. The main purpose of Local Binary patterns is to classify the text.

Steps to create LBP feature vector:

- Examined window is divided into cells.
- Along a circle each pixel in a cell is compared with its 8 neighbors on right-top, left-middle etc.
- If the neighbor’s value is lesser than that of the center pixel’s value then output is “True” i.e. “1” else the output is False i.e. “0”.
- As an output eventually a decimal converted from 8-digut binary number is given.
- Based on the output pattern, i.e. frequency of each occurring “number” the histogram is computed.
- As a next step the histogram are normalized for better results.
- To obtain the feature vector now these normalized histograms are concatenated.

  For the recognition of signature, once the feature vector is obtained, it has to be processed to be used in various machine learning algorithms such as Support Vector Machines.

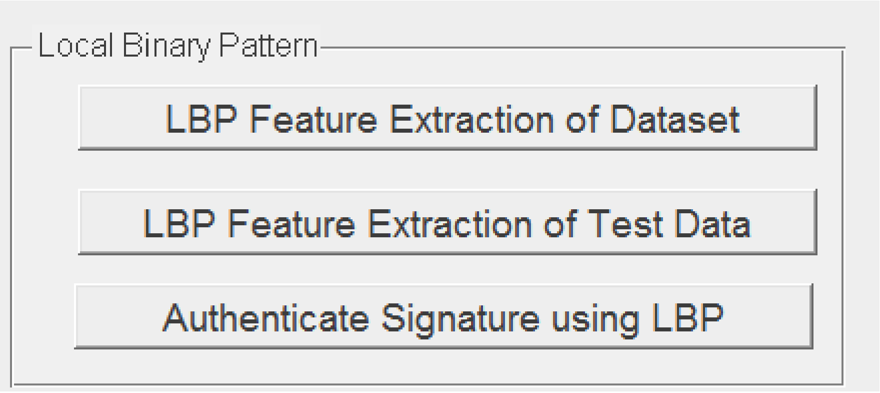
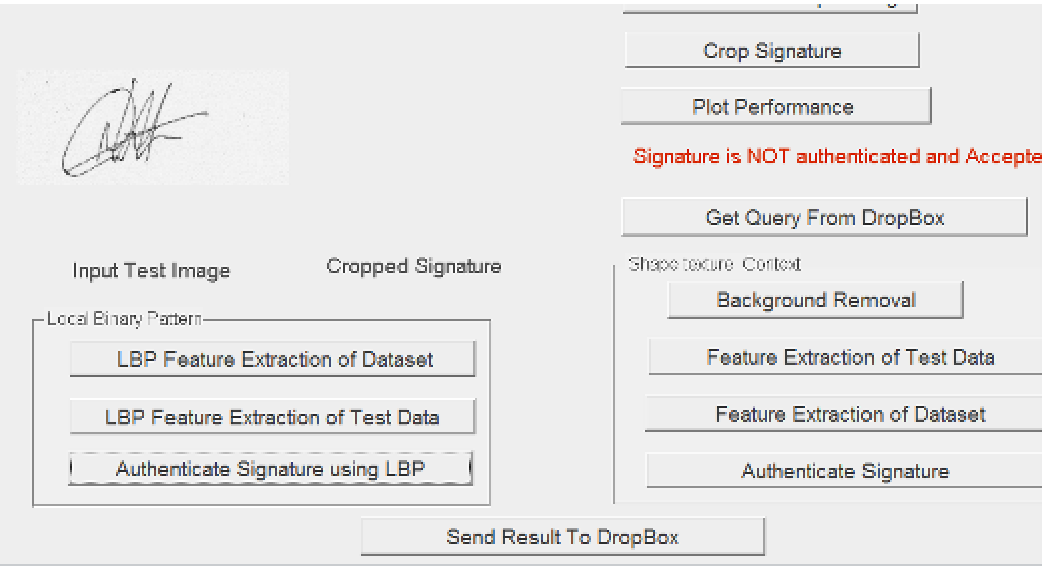

Local Binary Pattern
LBP Feature Extraction of Dataset
LBP Feature Extraction of Test Data
Authenticate Signature using LBP

Fig. 4 Actions to execute Local Binary Pattern

Figure 4 displays the form for the server side. It contains following actions for the Local Binary Pattern:

1. *Get query from the Drop Box:* The image sent from client is received for further processing.
2. *LBP feature extraction of dataset:* All features of signatures existing in the database are extracted.
3. *LBP feature extraction of dataset:* All features of test images are extracted.
4. *Authenticate using LBP:* Authentication result is obtained.



Signature is NOT authenticated and Accepte

Fig. 5 Authentication Result

5. *Send Result to Drop Box (Client):* The result is sent across to the client.

So in conclusion even for genuine signatures the LBP cannot generate 100% accurate result.

C. Server Form (GUI.m) using Shape Context Methodology:

Shape Context is used for object recognition as a feature descriptor.

The objective of Shape Context is to formulate point correspondences and enabling shape similarity measurement. On the contours of a shape set of n points are picked. Assume pi to be a point on the shape, it is then connected to all other points and hence obtaining n-1 vectors. It thus gives a detailed description of localization of all these vectors at that point.

The objective is to have a descriptor which is discriminative, compact and robust relative positions distribution. The formula to obtain the coarse histogram for the point pi:

h_i(k) = \#\{q \ne p_i : (q - p_i) \in \mbox{bin}(k)\}

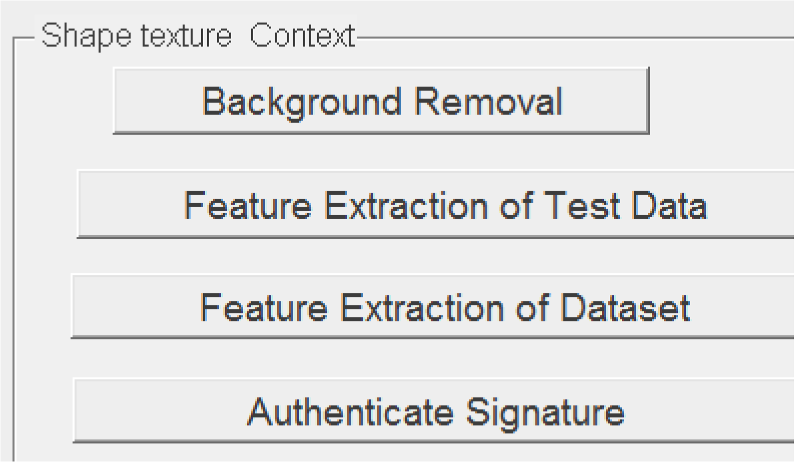


Fig. 6 Actions to execute Shape Texture Context

Figure 6 shows the actions available for the Shape Texture Context. Following actions are available:

1) *Background removal using Shape Context:* Here image is converted into grey level.

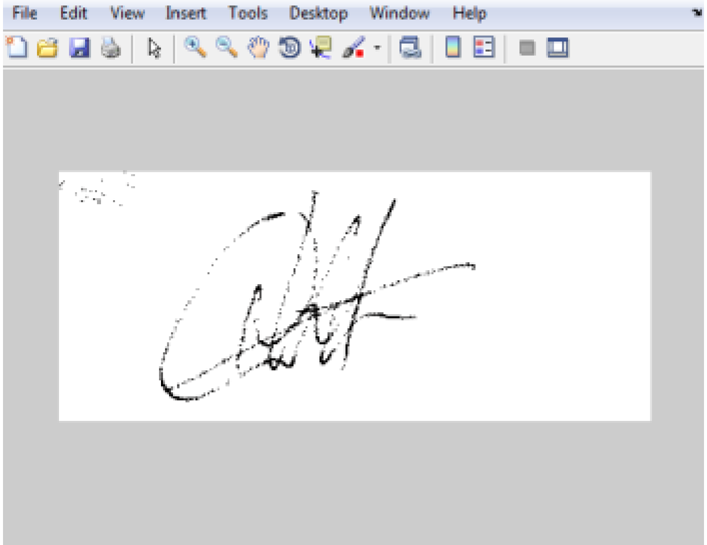
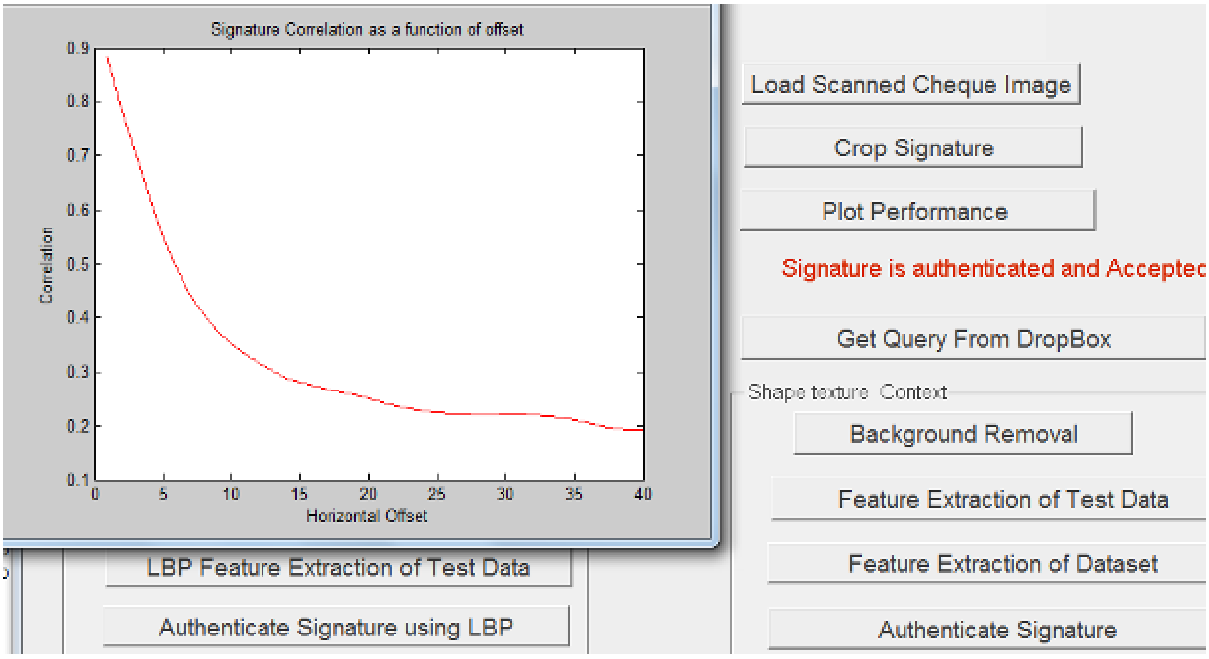


Fig. 7 Grey level image

2) *Feature extraction of test data:* Here all features of test image are extracted.
3) *Feature extraction dataset:* Here features of all signatures existing in database are extracted.
4) *Authenticate using shape context:* On this action authentication result is obtained.


Signature Correlation as a function of offset
Correlation
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
5
10
15
20
25
30
35
40
Horizontal Offset
Load Scanned Cheque Image
Crop Signature
Plot Performance
Get Query From DropBox
Shape texture Context
Background Removal
Feature Extraction of Test Data
Feature Extraction of Dataset
Authenticate Signature
LBP Feature Extraction of Test Data
Authenticate Signature using LBP

Signature is authenticated and Acceptec

Fig. 8 Authentication using Shape Context.

5) *Send result to Drop Box Client:* On this action the processed result is sent to the client form.

D. Graphical Result Analysis of LBP and Shape Context: Shape Context generates more accuracy than LBP.

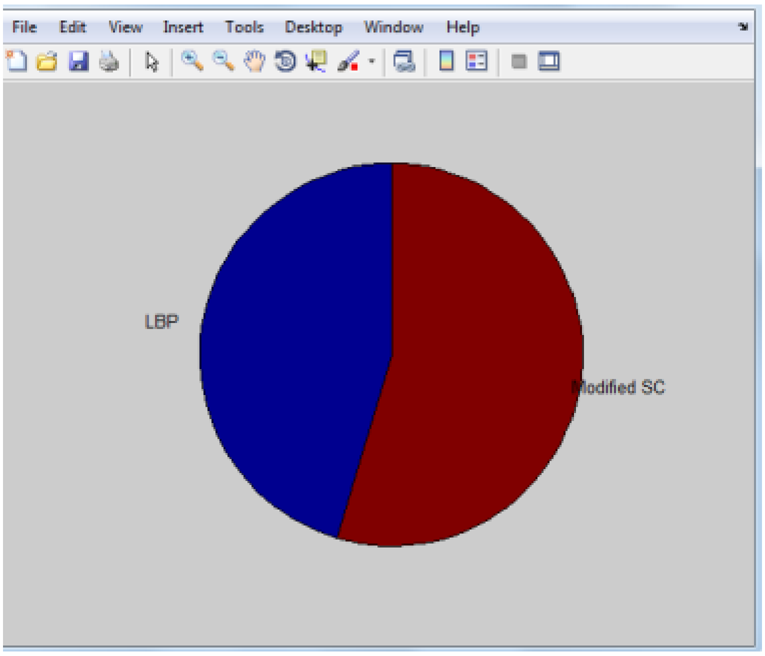


Fig. 9 Graphical Analysis.

V. CONCLUSION

In this paper we have built an application to enable a crisp comparison between two methods Local Binary Pattern (LBP) and Shape Context used for feature extraction and object recognition. Based on Multiple analysis performed with these two methods and on the results obtained, we conclude that Shape Context proves to be far more accurate in determining the genuineness of a signature and authenticating the same.

REFERENCES

[1] Velez, J.F., A. Sanchez and A.B. Moreno, 2003. Robust off-line signature verification using compression networks and positional cuttings. Proceedings of 2003 IEEE Signal Processing Society Workshop on Neural Networks, 17-19September, 2003, Toulouse, France, pp: 627-636.

[2] Blumenstein. S. Armand., Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural based Classification, International Joint Conference on Neural Networks, 2007.

[3] S.Srihari. K. M. Kalera. and A. XU, Offline Signature Verification and Identification Using Distance Statistics, International Journal of Pattern Recognition And Artificial Intelligence, 2008.

[4] S. Enturk. E. O¨ zgunduz. and E. Karshgil, “Handwritten Signature Verification Using Image Invariants and Dynamic Features,” Proceedings of the 13th European Signal Processing Conference EUSIPCO 2005,Antalya Turkey, 4th-8th September, 2000nr.

[5] Bakri, Nurhaniza B. T.; Syed Ahmsinatured, Sharifah Mumtaza h; Shak “Offline digital signature verification using hidden markov mode”l feb-march 2010.

[6] Miguel A. Ferrer, J. Francisco Vargas, Aythami Morales, and AarónOrdóñez “Robustness of Offline Signature Verification Based on grey level feature” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2012.

[7] Pradeep Kumar,Shekhar Singh “Hand Written Signature Recognition &Verificationusing Neural Network” march 2013.

[8] Ashwini Pansare, Shalini Bhatia “Handwritten Signature Verification using Neural Network” January 2012.

[9] H. S. Srihari and M. Beall, “Signature Verifcation Using Kolmogrov Smirnov Statistic” Proceedings of International Graphonomics Society, Salemo Italy, pp. 152–156, june,2005.

[10] HemantaSaikiaand Kanak Chandra Sarma “Approaches and Issues in Offline Signature verification System”, International Journal of Computer Applications (0975 – 8887)Volume 42– No.16, March 2012.

[11] Ramachandra A. C ,Jyoti shrinivas Rao ”Robust Offline signature verification based on global features” IEEE International Advance Computing Conference ,2009.

[12] Martinez, L.E., Travieso, C.M, Alonso, J.B., and Ferrer, M. Parameterization of a forgery Handwritten Signature Verification using SVM. IEEE 38thAnnual 2004 International Carnahan Conference on Security Technology ,2004 PP.193-196.

[13] C., Kertész: Texture-Based Foreground Detection, International Journal of Signal Processing, Image Processing and Pattern Recognition (IJSIP), Vol. 4, No. 4, 2012.

[14] S. Belongie, J. Malik, and J. Puzicha (2011). "Shape Context: A new descriptor for shape matching and object recognition". NIPS 2011