3rd International Conference on Latest Trends in Engineering, Science, Humanities and Management
(IFUNA) Indian Federation of United Nations Associations, New Delhi (India) (ICLTESHM-17)
8th April 2017, www.conferenceworld.in ISBN: 978-93-86171-23-8

OFFLINE SIGNATURES: IDENTIFICATION AND VERIFICATION USING STATISTICAL DESCRIPTORS AND SINGLE LEVEL THRESHOLDING

Devshri Satyarthi[1], Mohan Dhurvey[2] , Jaimala Jha[3]

[1]*CSE Deptt.,Dr.B.R.A. Polytechnic College Gwalior M.P. (INDIA)*

[2]*CSE Deptt,Dr.B.R.A. Polytechnic College Gwalior M.P. (INDIA)*

[3]*CSE,Itdeptt.,MITS College Gwalior M.P. (INDIA)*

ABSTRACT

Present a method of pixels values (the elements of a rectangular matrix) based on a pixels value data. In the proposed method focus is on the pixels value in order to improve the overall efficiency as individual pixels value lack in providing unique feature for different signature and provide generalized feature for minute change in signature of the same person. The proposed method is tested our own signature database contains 400 offline signature of individuals including, 1 test signature and the result are compare with other state of art of method sand prove that proposed methods is better in terms of efficiency.

Keyword: *Signature verification, Pixels value, Threshold, Euclidean distance, Forgeries.*

1. INTRODUCTION

Maximum works have done in this area, because of security, verification and identification of the person. Signature verification techniques elect vary according to assets or requirements.

Offline signatures are scanned from paper document, where they were written in easy way. Offline signature analysis can be carried out with a scanned image of the signature using camera or scanner. In offline verification system, only static features are considered absolutely on the signature's image but it less hardware required. Signature verification is most important identity of the person; it is used in paper work, documents, finical, check etc. On one know that signature is authentic person or is criminal. This paper supported to detect original signature.

Signature verification is different than the nature identification, because signature is frequently changed and it is just an image with some specific shape, language that represents the writing style and way. In special case of handwriting, it is symbol or picture is used. So it is common sense and necessary deal with a signature as a

ISBN: 978-93-86171-23-8

complete image with special distribution of pixel and representing a particular writing style and not as a collection of letters and word [1, 2].

In this paper based on only pixel value data. An image is a rectangular array of dots called pixels (picture elements). The number of rows M and number of columns N of dots in an image are specified. At each row-column intersection (m,n) there is a pixel, or picture element. The point (m,n) is the location of the pixel, while the pixel value at that location is designated by p(m,n), or sometimes by f(m,n) or f(x,y), where $0 < m < M-1$ and $0 < n < N-1$. The bottom vertical direction is x and y is the horizontal right direction. The origin is in upper left corner.

The pixel values in an image may be grayscale or color. We first deal with grayscale because it is simpler and even when we process color images we often process the intensity part, which is grayscale, and then put the color back into the processed image.

There are three types of signature:

1 Random: It is a signature done by a person, who does not know the shape and style of genuine signature.
2. Simple: It is written by a person who knows the shape of original signature without much practice.
3. Skilled: It is written by a person who knows the shape of original signature without much practice.

II. FORGERIES

There are four types of forgeries:

1. Genuine signature: Genuine signature is original signature.
2. Random forger: Random signature is something learns but not original signature.
3. Simulated simple forgery: simulated simple forgery is copy not know original shape of signature without any practice.
4. Simulated skilled forgery: Simulated skilled forgery is copy not know original shape of signature with need practice.

The rest of paper is structured as follows.

III. QUALITY PERFORMANCE MEASURES

The false rejection rate (FRR) of genuine signatures and the false acceptance rate (FAR) of forgery signatures and these two are inversely related.

Quality performance measures are classified into different way:

1. FAR: The FRR is the ratio of genuine test signatures rejected to the total number of genuine test signatures submitted. The FRR called the type I error and is defined as,

$$\text{FAR} = \frac{\text{Total number of genuine test pattern rejected}}{\text{Total number of genuine test pattern submitted}}$$

2. FRR: The FAR is the ratio of the number of forgeries accepted to the total number of forgeries submitted. The FAR is also called the type II error and is defined as,

ISBN: 978-93-86171-23-8

$$FRR = \frac{\text{Total number of forgeries accepted}}{\text{Total number of forgeries submitted}}$$

3. AER: The average of the FRR and FAR is called the AER.
4. EER: The EER is find the equal error rate between forgeries accepted and forgeries submitted number. The EER is also called the type III error.

IV. WORK DONE IN THE EXISTING FIELDS

E. Ozgunduz et al [1] proposed on global features (height-width proportion, middle point, corner points, etc.), and grid features as inputs. Tests are performed both by using simple MLP classifiers and by using SVMs. SVMs were tested with kernels with linear, polynomial, and radial basis function. The latter seemed to deliver the best results with an average error rate of 7-8% compared to the 16-22% error rates measured when using MLPs.

M. K. Kalera et al. [2] It utilizes CGS vectors (originally developed for character recognition) to extract global features. The main idea here is, to assign a 1024 bit long binary vector to each image and compare these vectors in the later phases. Images are divided into 4x8=32 segments, and information (like concavity, gradient, structural properties) is encoded into the vector for each segment. These vectors are then compared by several algorithms operating with vector distances. In this scenario, the SVM based solution performs poorly, with an average error rate of 46% while a Naïve Bayes classifier achieved error rates between 20% and 25%.

B. Kovari et al. [3] proposed on problems occurring during feature based off-line signature verification and delivered solutions for the special questions of this problem class. We have shown that the behavior of a feature based off-line signature verification system can be effectively simulated with a statistical approach. The resulting equations allow the prediction of the performance limit of a verification system on a given database and more importantly, can help in the calibration of the system. We have also demonstrated.

R.Planmandon [4] proposed on 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.

M. Ammar et al. [5] have worked on the detection of skilled forgeries. They have calculated the statistics of dark pixels and used them to identify changes in the global flow of the writing.

M. Ammar et al. [6] is based on reference patterns, namely the horizontal and vertical positions of the signature image. The projections of the questioned signature and the reference are compared using Euclidean distance.

J. K. Guo et al. [7] have presented an algorithm for the detection of skilled forgeries based on a local correspondence between a questioned signature and a model obtained a priori.

R. B. Dubey et al. [8] introduced a procedure to extract features from handwritten signature images and computed feature is used for verification. A novel off-line signature verification algorithm has been presented which uses the soft-computing clustering technique. The equi-spaced features are adjusted or updated using the cluster update algorithm and these centres or feature points are trained using the training signatures in the database to avoid interpersonal and intrapersonal errors as much as possible. Despite our best efforts still there are some loop holes in the algorithm, due to which there are some errors in the result. The algorithm has its pre-

ISBN: 978-93-86171-23-8

specified threshold of max error = 155, pre-specified step size in the clustering that is 0.005 etc. All these parameters can be made adaptive, that will adjust them according to the input given to them.

A. C. Ramachandra et al. [9] proposed a Cross-validation for Graph Matching based offline Signature Verification (CGMOSV) algorithm. The dissimilarity measure between two signatures in the database was determined by (i) constructing a bipartite graph (ii) obtaining complete matching in and (iii) finding minimum Euclidean distance by Hungarian method. Using Cross-validation principle reference signatures were selected and an optimum decision threshold value was determined. The threshold value was used to compare and authenticate the test signature. They observed that FRR, FAR and EER values were improved compared to the existing algorithm.

A. Bansal et al. [10] proposed a contour matching algorithm. They used the geometrical properties of the signature and considered the inevitable intrapersonal variations for the user set A. The system was trained with 8 original signatures and given a test sample. Verification was done by a triangle matching algorithm. FAR in case of Random Forgery was found to be 0.08% and in case of Simple and Skilled forgery it was 13.02%. FRR was 2.64%.

J. F. Vargas et al. [11] proposed an offline signature verification system based on grey level information using texture features. They analyzed the co-occurrence matrix and local binary pattern and used as features. Genuine samples and random forgeries were used to train an SVM model. Random and skilled forgeries were used for testing. For skilled forgeries, they were able to achieve an EER of 12.82%.

S. Armand et al. [12] proposed a method for off-line signature verification and identification. In their method, the contour of the signature was determined from its binary representation. Using combination of the Modified Direction Feature (MDF) (this technique employs a hybrid of two other feature extraction techniques - Direction Feature and the Transition Feature) some unique structural features were extracted from the signature-contour. They employed Neural Network based classifiers. A Resilient Back Propagation neural network and a Radial Basis Function neural network were compared. Obtained verification rate was 91.12%.

A. C. Ramachandra et al. [13] proposed Robust Off-line Signature Verification based on Global Features (ROSVGF) for skilled and random forgeries. The model extracts the features which are pre-processed by normalization, binarization and thinning. The feature extraction technique consists of global features such as aspect ratio, maximum horizontal histogram and maximum vertical histogram, horizontal and vertical centre of signature and signature area.

R. Sabourinand et al. [14] proposed Automatic Handwritten Signature Verification System (AHVS), which can cope up with all types of forgeries. In order to eliminate rapidly gross forgery directional Probability Density Function (PDF) is chosen as a global feature vector. The comparison of features is based on Neural Network using classical back propagation algorithm.

V. Proposed Methodology

Euclidean distance model

Let A (a_1, a_2…..a_n) and B (b_1, b_2….b_n) are two vectors of size n. We can calculate distance (d) by using equation 1.

ISBN: 978-93-86171-23-8

$$distance(d) = \sqrt{\sum_{i=1}^{n}(a_i - b_i)^2} \quad .. (1)$$

In our application, vectors are feature points on plane. So d is the simple distance between two points.

VI. THRESHOLD

Threshold converts each pixel into black, white or unchanged depending on whether the original colour value is within the threshold range. Threshold is a very important command that is often used to prepare scanned RGB or RGB images for vectorization or use as guide layers in the creation of drawings. It can be used with raster data images to set off ranges of values that may then be used for subsequent analysis or as selection masks.

Distance measure to every test signature, where a distance of zero is attributed to a perfect match (genuine signature or positive class) and a distance of inanity to a complete mismatch (forgery or negative class). A typical threshold-based on confidence to every test patterns. A confidence is calculated in such a way that it is inversely proportional to the distance measure. A confidence of one is attributed to a perfect match (genuine signature or positive class) and a confidence of zero is attributed to a complete mismatch (forgery or negative class).

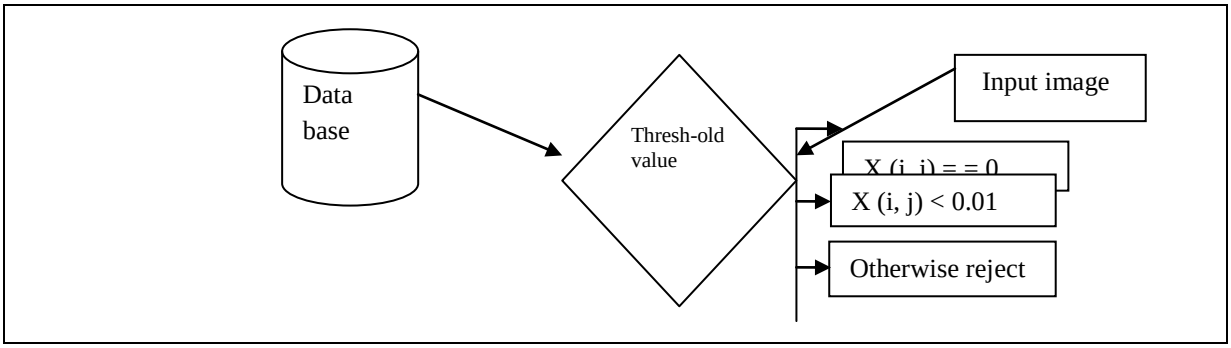


Fig.1 Flow chart of Threshold value.

VII. VERIFICATION

The comparison between the database signatures and test signature is made by computing the difference between four statistical features (mean, entropy, standard deviation, and variance) obtained for both the signatures. A threshold is set which decides the Authenticity of the signature. The threshold value of 0.01 radians is considered for verification purpose. The absolute difference between database and input signature is compared with the threshold value.

Pseudo code

1. Input the 400 samples of signature images and 10 signatures for test.
2. Calculate GCF.
3. Calculate X-axis right hand.
4. Calculate Y-axis bottom.
5. Store these values in database (step2, step3 and step4).
6. Match the database signature value to test signature value.
7. Apply Euclidean distance for finding absolute difference on Step6.
8. Set the threshold value.

ISBN: 978-93-86171-23-8

9. Verify signature is FAR and FRR.

Proposed Algorithm

```
1. Input the 400 samples of signature images and 10    signatures for test.

2. Signature verify
3. while signature(s)=True
4.  do
5.     for i=1:100
6.       for j=1:4
7.            if GCF(i,j)<0.01
8.                                    display ('FAR')
9.                          otherwise
10.                                   display('FRR')
11.    end if
12.           if X-axis(i,j)<0.01
13.                                   display ('FAR')
14.                        otherwise
15.                                   display('FRR')
16.      end if
17.            if Y-axis(i,j)<0.01
18.                                            display ('FAR')
19.                        otherwise
20.                                           display('FRR')
21.         end if
22.     end
23. end
24.end
```

ISBN: 978-93-86171-23-8

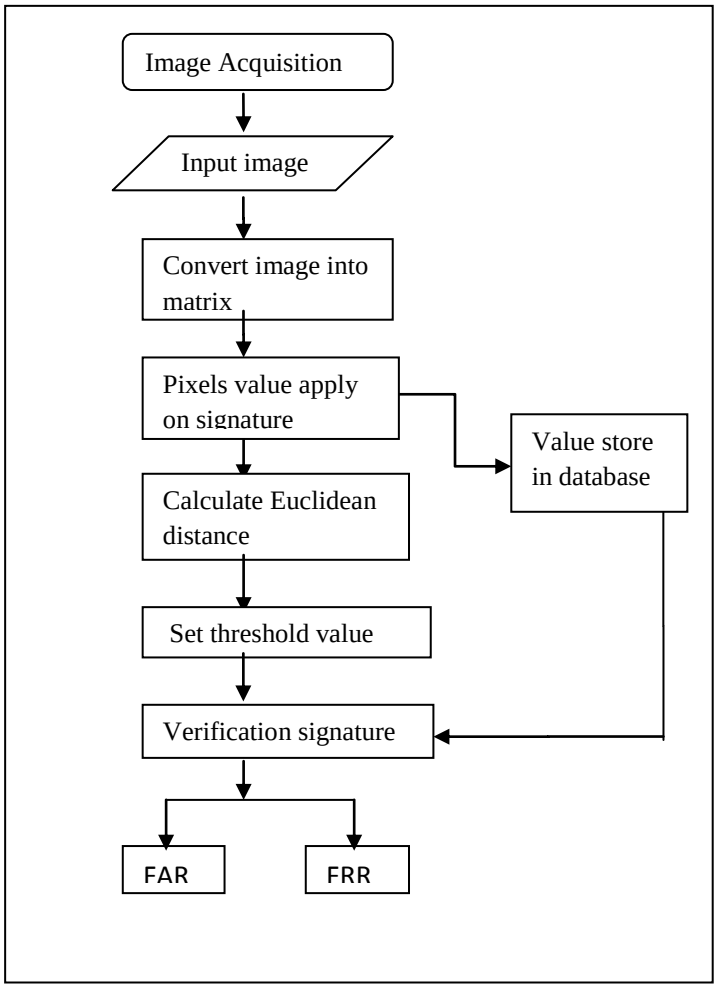


Fig.2 Flowchart of signature identification.

VIII. IMPLEMENTATION

We have not used the exiting database, instead we created the database from MITS (Madhav Institute Of Technology And Science) College Gwalior.

For analysis, the database consisting of 400 signature images and 10 test signature images are considered. Among them, 100 signature samples are genuine and 300 signature samples are forged.

All signatures stores in database, than the test signature match with each and every signature in database individually. It used different size of image, different style and also considers the art of signature are used for analyze. Firstly apply on database signature images to find out gcd, X axis in right and Y axis in bottom signature cover the pixels of image, after calculating these pixels data values store in database and also find these pixels data value apply on test signature at testing time it calculate pixels data values, then apply Euclidean distance to find the absolute difference between test image and database images and set the threshold value 0.01 and verify signature is genuine and forgery in form of FAR is 0.2% and FRR is 99.8% according to Threshold value increase efficiency and it give almost better efficiency. The verification perform is evaluated using different threshold value as present in table 1, table2 and table3.

ISBN: 978-93-86171-23-8

Table1. GCF variation of FAR and FRR with Threshold.

S. no	Threshold value	%FAR	%FRR
1	0.01	0.2	99.8
2	0.10	6.42	93.6
3	0.20	0	100
4	0.25	0	100
5	0.50	0	100

Table2. X-axis on Right-hand (RH) variation of FAR and FRR Threshold.

S. no	Threshold value	%FAR	%FRR
1	0.01	0.6	99.4
2	0.10	0.6	99.4
3	0.20	0.6	99.4
4	0.25	0.6	99.4
5	0.50	0.6	99.4

Table3. Y-axis on bottom variation of FAR and FRR with Threshold.

S. no	Threshold value	%FAR	%FRR
1	0.01	0.6	99.4
2	0.10	0.6	99.4
3	0.20	0.6	99.4
4	0.25	0.6	99.4
5	0.50	0.6	99.4

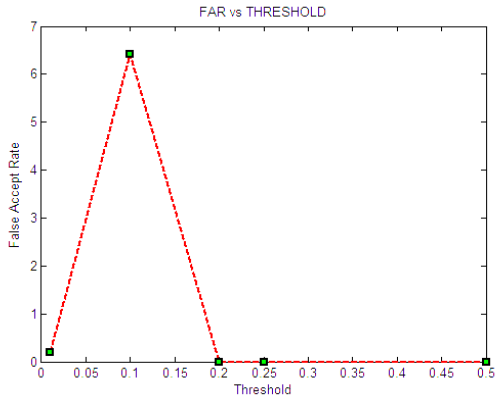


Fig3. GCF FAR against Threshold.

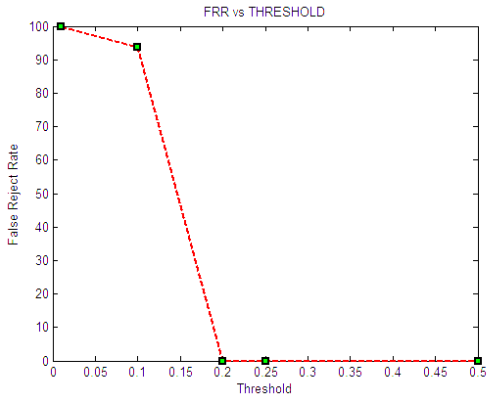


Fig4. GCF FRR against Threshold.

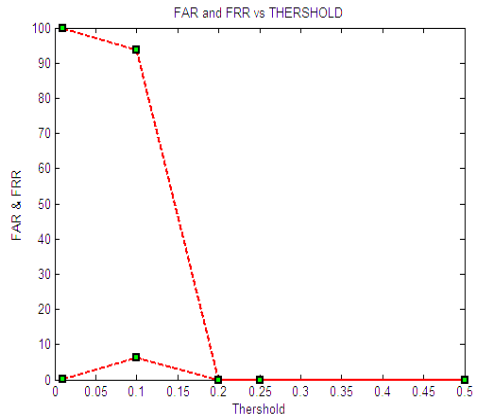


Fig5. GCF FAR and FRR against Threshold.

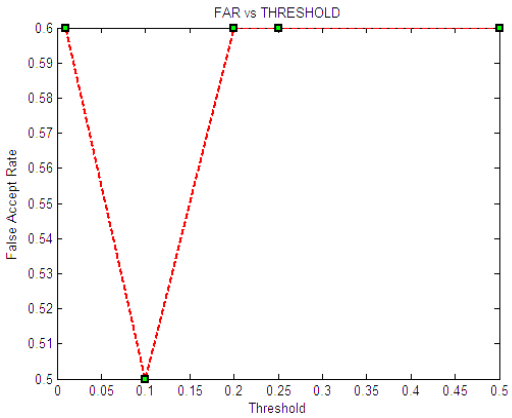


Fig6. X-axis on RH FAR against Threshold.

ISBN: 978-93-86171-23-8

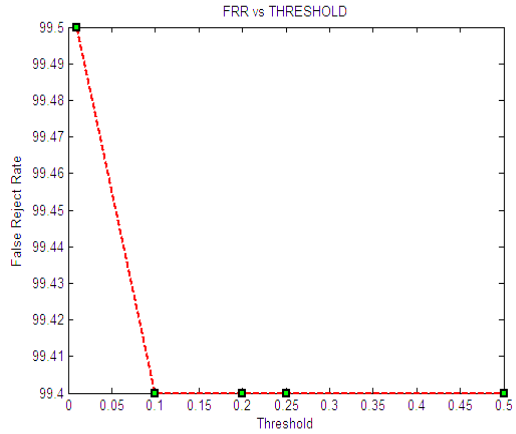


Fig7. X-axis on RH FRR against Threshold.

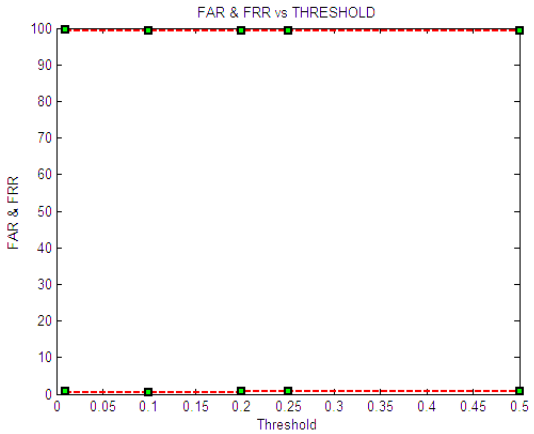


Fig8. X-axis on RH FAR and FRR against Threshold.

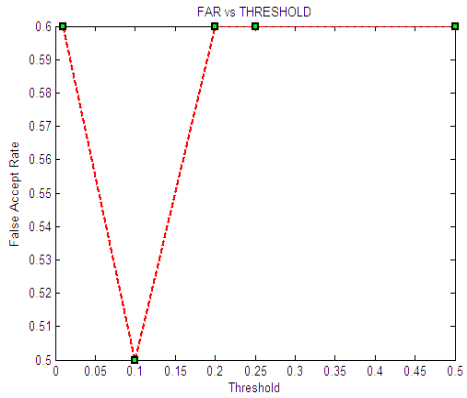


Fig9. Y-axis on Bottom FAR against Threshold.

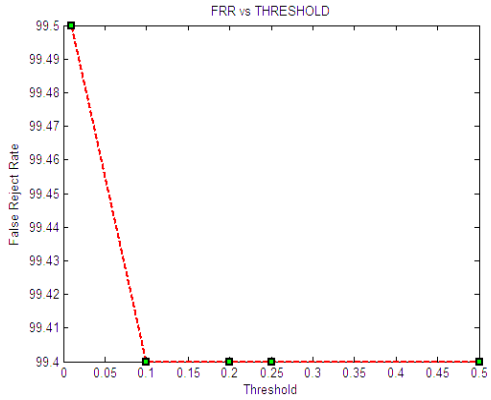


Fig.10 Y-axis on Bottom FRR against Threshold.

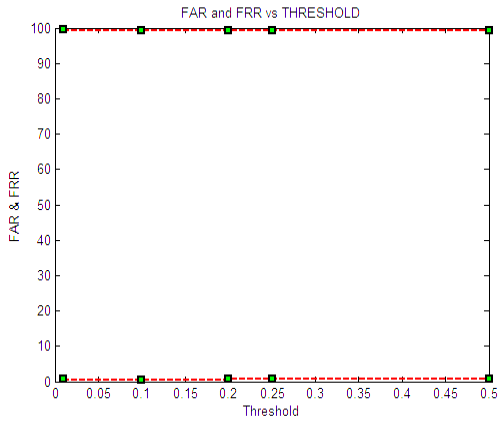


Fig11. Y-axis on Bottom FAR and FRR against Threshold.

IX. CONCLUSION

We proposed and presented an offline signature verification which is based on pixels value. The pixels value is very important is signature image to verify signature is original and forgery. The results show that using a threshold outperforms for false acceptance rate is 0.2% and false rejection rate is 99.8%.

ISBN: 978-93-86171-23-8

REFERENCE

[1] E. Ozgunduz, T. Senturk, and M. Karsligil, "Off-line Signature Verification and Recognition by Support Vector Machine", Proceedings of the Thirteenth European Signal Processing Conference, 2005.

[2] M. K. Kalera, S. Srihari, and A. Xu, "Offline Signature Verification and Identification Using Distance Statistics" , Proceedings of the International Journal of Pattern Recognition and Artificial Intelligence, vol. 18, no. 7, pp. 1339-1360, 2004.

[3] B. Kovari, H. Charaf, "Statistical Analysis of Signature Features with Respect to Applicability in Off-line Signature Verification", Proceedings of the Latest trends on computers (Volume II), pp. 473-478.

[4] R. Plamondon, "The design of an on-line signature verification system: from theory to practice", Proceedings of the International journal Pattern Recognize Artificial Intelligence, vol. 8, pp. 795-811, 1994.

[5] M. Ammar, Y. Yoshida and T. Fukumura, "A new effective approach for off-line verification of signatures by using pressure features", Proceedings of the International Conference on Pattern Recognize, pp. 566-569, 1986.

[6] M. Ammar, "Progress in verification of skilfully simulated handwritten signatures", Proceedings of the International Journal Pattern Recognize and Artificial Intelligence, vol. 5, pp. 337-351, 1991.

[7] J. K. Guo and D. Doermann, A. Rosenfeld, "Off-line skilled forgery detection using stroke and sub-stroke properties", Proceedings of the International Conference on Pattern Recognize, pp. 355-358, 2000.

[8] R. B. Dubey, S. Sachdeva, "Offline signature verification", Proceedings of the Webmed Central, pp.1-10, id. WMC001919, 2011.

[9] A. C. Ramachandra, K. Pavithra, K. Yashasvini, K. B. Raja, K. R. Venugopal and L. M. Patnaik, "Cross-Validation for Graph Matching based Offline Signature Verification", Proceedings of the India Conference INDICON 2008.[10] A. Bansal, D. Garg, and A. Gupta, "A Pattern Matching Classifier for Offline Signature Verification", Proceedings of the First International Conference on Emerging Trends in Engineering and Technology (IEEE Computer Society) 2008.

[11] J. F. Vargas, M. A. Ferrer, C. M. Travieso and J. B. Alonso, "Off-line signature verification based on grey level information using texture features", Proceedings of the Pattern Recognition 44, pp. 375–385, 2011.

[12] S. Armand, M. Blumenstein and V. Muthukkumarasamy, "Off-line Signature Verification based on the Modified Direction Feature", Proceedings of the 18th IEEE International Conference on Pattern Recognition (ICPR'06), 2011.

[13] A. C. Ramachandra, J. Srinivasa Rao, K. B. Raja, K. R. Venugopal and L. M. Patnaik, "Robust Off-line Signature Verification based on Global Features" , Proceedings of the IEEE International Advance Computing Conference**,** pp. 1173-1178, March 2009.

[14] R. Sabourin and Jean-Pierre Drouhard, "Impact of Signature Legibility and Signature Type in Off-line Signature Verification", Proceedings of the IEEE International Conference on Pattern Recognition, pp. 321-325, 1992.

[15] C. R. Prashanth, K. B. Raja, K. R. Venugoupal and L. M. Patnaik, "DWT based offline signature verification using Angular feature", Proceedings of the International Journal of computer Application, vol. 52, no. 15, 2012.

[16] H. Saikia and K. C. Sarma, "Approaches and Issues in Offline signature verification system", Proceedings of the International Journal of computer Application, vol. 42, no. 16, 2012.

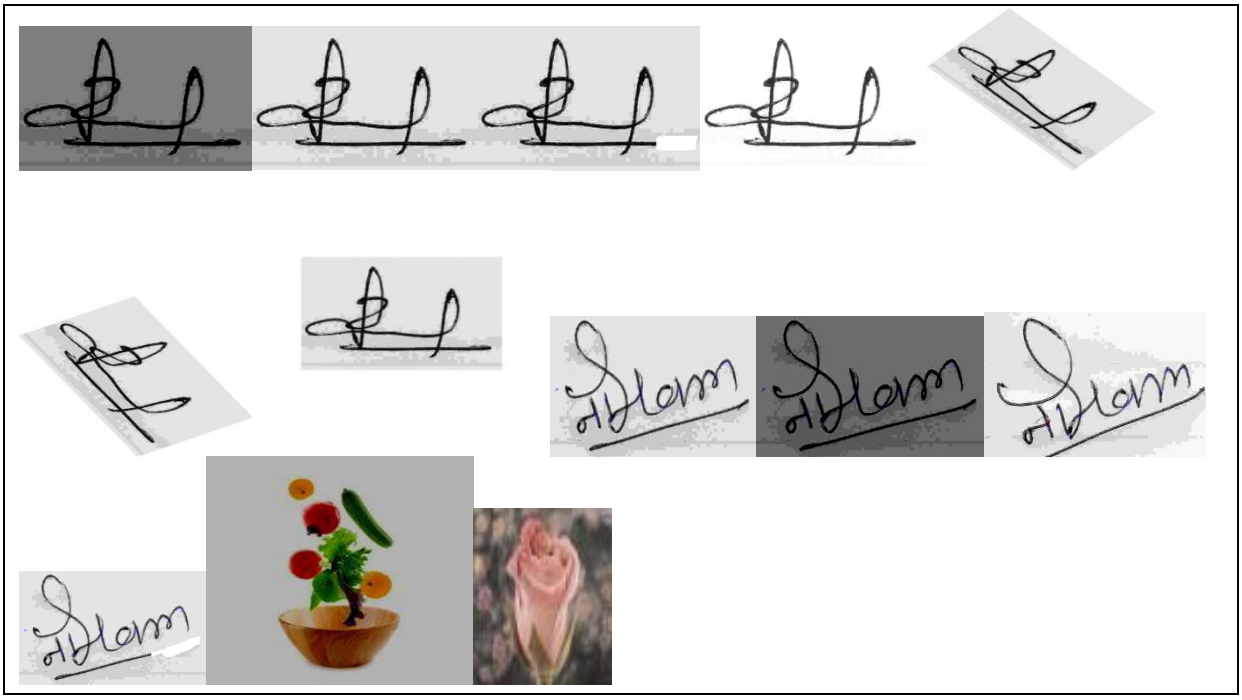
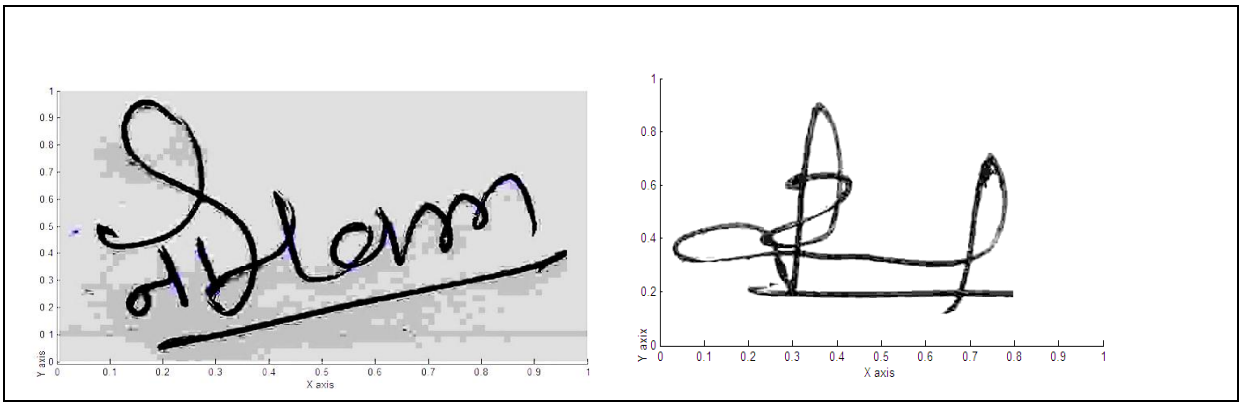
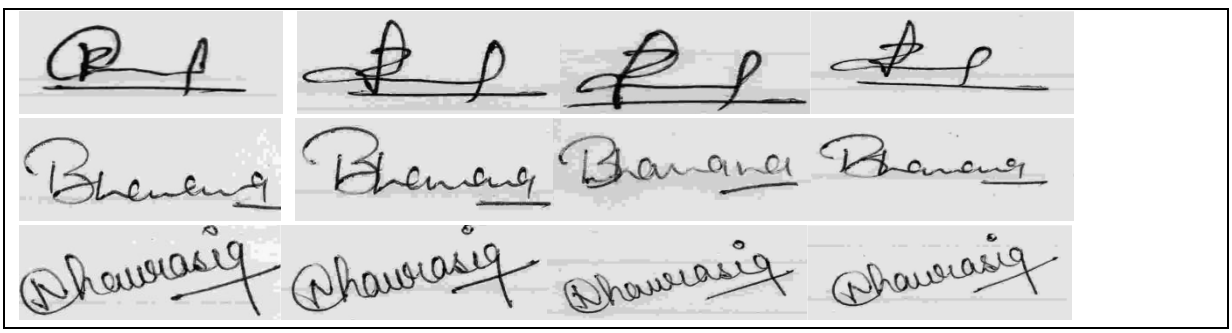


Fig12. Test image.





ISBN: 978-93-86171-23-8

Fig13. Database